



Manual do usuário

AWS Transfer Family



AWS Transfer Family: Manual do usuário

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é AWS Transfer Family?	1
Como AWS Transfer Family funciona	4
Publicações de blog relevantes para o Transfer Family	5
Pré-requisitos	9
Regiões, endpoints e cotas	9
Inscreva-se para AWS	10
Configurar armazenamento	10
Configurar um bucket do Amazon S3	11
Configurar um sistema de arquivos Amazon EFS	16
Criar uma política e um perfil do IAM	20
Criação de um perfil de usuário	21
Como funcionam as políticas de sessão	24
Exemplo de política de read/write acesso	28
Tutoriais do Transfer Family	32
Introdução a endpoints do servidor	33
Pré-requisitos	33
Etapa 1: faça login no AWS Transfer Family console	34
Etapa 2: criar um SFTP-enabled servidor	34
Etapa 3: Adicionar um usuário gerenciado de serviço	36
Etapa 4: Transferir um arquivo usando um cliente	37
Crie um fluxo de trabalho de descritografia	39
Etapa 1: Configure uma função de execução	40
Etapa 2: Crie um fluxo de trabalho gerenciado	41
Etapa 3: Adicione o fluxo de trabalho a um servidor e crie um usuário	42
Etapa 4: Crie um par de chaves PGP	44
Etapa 5: Armazene a chave privada PGP em AWS Secrets Manager	45
Etapa 6: Criptografe um arquivo	46
Etapa 7: Execute o fluxo de trabalho e visualize os resultados	47
Crie e use conectores SFTP	48
Tipos de saída do conector	49
Etapa 1: criar os recursos de suporte necessários	49
Etapa 2: criar e testar um conector SFTP	56
Etapa 3: Enviar e recuperar arquivos usando o conector SFTP	61

Procedimentos para criar um servidor Transfer Family para usar como seu servidor SFTP remoto	65
Use um provedor de identidade personalizada	68
Pré-requisitos	69
Etapa 1: criar uma CloudFormation pilha	69
Etapa 2: Conferir a configuração do método do API Gateway para seu servidor	70
Etapa 3: Visualizar os detalhes do servidor do Transfer Family	71
Etapa 4: Testar se o usuário consegue se conectar ao servidor	73
Etapa 5: Testar a conexão SFTP e a transferência de arquivos	73
Etapa 6: Limitar o acesso ao bucket	74
Atualize o Lambda se estiver usando o Amazon EFS	76
Configurar uma configuração AS2	77
Etapa 1: Criar os certificados para AS2	79
Etapa 2: Importar certificados como recursos de certificados do Transfer Family	83
Etapa 3: Crie perfis para você e seu parceiro comercial	84
Etapa 4: Criar um servidor Transfer Family que usa o protocolo AS2	85
Etapa 5: criar um acordo entre você e seu parceiro	88
Etapa 6: criar um conector entre você e seu parceiro	90
Etapa 7: Teste a troca de arquivos pelo AS2 usando Transfer Family	91
Configurar um aplicativo web básico	93
Pré-requisitos	93
Etapa 1: criar os recursos de suporte necessários	94
Etapa 2: criar um aplicativo web Transfer Family	95
Etapa 3: configurar o compartilhamento Cross-origin de recursos (CORS) para seu bucket	96
Etapa 4: adicionar um usuário ao seu aplicativo web Transfer Family	97
Etapa 5: registrar um local no Amazon S3 e criar uma concessão de acesso	99
Etapa 6: Acesse seu aplicativo web Transfer Family como usuário	101
Próximas etapas	102
Integre o Okta como seu provedor de identidade para aplicativos da web	102
Configure o aplicativo web com acesso seletivo a vários buckets	105
Pré-requisitos	105
Etapa 1: criar um aplicativo web Transfer Family	106
Etapa 2: configurar funções do IAM para acesso ao S3	107
Etapa 3: configurar o S3 Access Grants	109
Etapa 4: registrar os locais dos buckets do S3	110

Etapa 5: criar concessões de acesso	110
Etapa 6: Configurar a política CORS para buckets S3	111
Etapa 7: testar a configuração	112
Conclusão	112
Transfer Family para SFTP, FTPS, FTP	113
Opções do provedor de identidade	113
AWS Transfer Family matriz de tipo de endpoint	115
Configurar um endpoint do servidor Transfer Family	119
Crie um SFTP-enabled servidor	121
Crie um FTPS-enabled servidor	130
Crie um FTP-enabled servidor	139
Crie um servidor em uma VPC	148
Trabalhar com nomes de host personalizados	173
FTP/FTPS Considerações sobre o NLB	177
Transferir arquivos pelo endpoint do servidor	178
SFTP/FTPS/FTP Comandos disponíveis	181
Encontre seu endpoint da Amazon VPC	182
Evitar erros setstat	184
Usar OpenSSH	38
Usar o WinSCP	186
Usar o Cyberduck	37
Use FileZilla	189
Usar um cliente Perl	191
Use o LFTP	191
Processamento pós upload	191
Mensagens SFTP	193
Gerenciar usuários	195
Amazon EFS versus Amazon S3	196
Diretórios lógicos	197
Cotas de grupo do Active Directory	198
Service-managed usuários	199
Provedor de identidades personalizado	208
Serviço de diretório para MS AD	248
Serviço de diretório para Entra ID	259
Use diretórios lógicos	266
Entendendo o chroot e a estrutura de diretórios	267

Regras para usar diretórios lógicos	267
Implementando diretórios lógicos	269
Configurar exemplos de diretórios lógicos	273
Configure diretórios lógicos para o Amazon EFS	274
AWS Lambda Resposta personalizada	275
Access FSx para sistemas de arquivos NetApp ONTAP	276
Visão geral do	277
Pré-requisitos	277
Como o armazenamento FSx funciona com o Transfer Family	278
Criando um ponto de acesso S3 para FSx	279
Usando aliases de ponto de acesso S3 com FSx	282
Configurando o Transfer Family para armazenamento FSx	284
Gerenciando usuários para armazenamento FSx	285
Configurando clientes de transferência de arquivos	287
Solução de problemas de armazenamento FSx	288
Aplicativos web Transfer Family	290
Regiões da AWS para aplicativos web Transfer Family	291
Compatibilidade do navegador para aplicativos AWS Transfer Family da web	291
Como criar um aplicativo web Transfer Family	291
Configure seu provedor de identidade	294
Configurar perfis do IAM	296
Configurar um aplicativo web Transfer Family	299
Crie um aplicativo web Transfer Family	299
Endereçamento IP	301
Crie um aplicativo web Transfer Family em uma VPC	302
Crie um aplicativo web Transfer Family	303
Post-creation etapas	305
Cross-origin política de compartilhamento de recursos (CORS)	305
Restringir o acesso a um VPC endpoint específico	306
Atribuir ou adicionar usuários ou grupos a um aplicativo web Transfer Family	307
Configure o compartilhamento de Cross-origin recursos (CORS) para seu bucket	310
Configurar concessões de acesso ao Amazon S3	312
Use um URL personalizado	318
Registro para aplicativos web da Transfer Family	321
Habilitando eventos de dados do Amazon S3	322
Exemplos de registros de autenticação	324

Visualizando entradas de registro	331
Solução de problemas em seus aplicativos da web	332
Solucionar erros de rede	333
Solucione o problema de que o bucket configurado não aparece	333
Solucionar erros de URL personalizados	334
Solucionar erros diversos	334
Buckets S3 duplicados que aparecem no aplicativo web	335
Instruções para o usuário final	336
Cotas de aplicativos web	336
Usuários do Centro de Identidade do IAM	336
Third-party usuários finais	338
Interface de usuário final do Transfer Family	338
Ações disponíveis	339
Conectores SFTP	342
Criação de conectores SFTP	342
Escolhendo o tipo de saída do conector SFTP	343
Escolhendo o modo de endereçamento IP	344
Armazene as credenciais no Secrets Manager.	345
Crie um conector SFTP com saída gerenciada por serviços	347
Crie um conector SFTP com saída VPC-based	357
Testar um conector SFTP	369
Conectividade da VPC	371
Usando conectores SFTP	372
Transferir arquivos	372
Listar conteúdo de diretórios remotos	374
Mover e excluir arquivos no servidor remoto	376
Monitorando conectores SFTP	378
Use a API do conector para consultar o status das solicitações de transferência de arquivos	378
Veja eventos do conector SFTP na Amazon EventBridge	379
Veja os registros do conector SFTP na Amazon CloudWatch	379
Monitorando conectores do tipo de saída VPC	379
Gerenciando conectores SFTP	381
Atualizar conectores SFTP	382
Exibir detalhes do conector SFTP	383
Cotas da para conectores SFTP	384

Cotas da para conectores SFTP	384
Dimensionando seus conectores SFTP	385
Arquiteturas de referência	386
Publicações no blog	387
Workshops	387
Soluções	387
Arquiteturas de referência de VPC	388
Transfer Family para AS2	390
Casos de uso do AS2	391
Modelos AS2 CloudFormation	396
Personalizando modelos AS2	396
Testando sua implantação do AS2	397
Práticas recomendadas para implantação do modelo AS2	397
Configurar AS2	398
Configurações AS2	399
Cotas AS2	401
Recursos e capacidades AS2	404
Gerenciar certificados AS2	406
Importar certificados AS2	406
Alternância de certificados AS2	409
Crie perfis AS2	411
Crie um servidor AS2	412
Crie um servidor AS2 usando o console Transfer Family	412
Crie um servidor AS2 usando um modelo	415
Crie um contrato AS2	419
Configurar conectores AS2	420
Crie um conector AS2	421
Algoritmos de conector AS2	424
Autenticação básica para conectores AS2	425
Habilitar a autenticação básica para conectores AS2	427
Visualizar detalhes do conector	430
Transferir mensagens AS2	432
Receba mensagens AS2	433
Configurar o HTTPS para AS2	434
Transferir arquivos com conectores AS2	440
Nomes e localizações dos arquivos	442

Códigos de status	445
Arquivos JSON de amostra	446
Cabeçalhos HTTP personalizados para AS2	448
Visão geral do modelo	449
Como funciona	449
Recursos principais	449
Detalhes da implantação	449
Implantação e uso	451
Monitor AS2	452
Códigos de status AS2	453
Códigos de erro AS2	454
Monitoramento da expiração do certificado	467
DaysUntilExpiry métrica	467
Práticas recomendadas para monitoramento de certificados	468
Exemplo de configurações de alarme	469
Gerenciando fluxos de trabalho de processamento de arquivos	470
Criar um fluxo de trabalho	472
Configurar e executar um fluxo de trabalho	474
Visualizar detalhes do fluxo de trabalho	476
Usar etapas predefinidas	479
Copiar arquivo	479
Descriptografar arquivo	484
Arquivo de marcação	490
Excluir arquivo	491
Variáveis nomeadas para fluxos de trabalho	492
Exemplo para marcar e excluir fluxo de trabalho	492
Use etapas personalizadas de processamento de arquivos	497
Usando várias funções do Lambda consecutivamente	499
Acessar um arquivo após o processamento personalizado	499
Exemplos de eventos enviados para AWS Lambda após o upload do arquivo	500
Exemplo de função do Lambda para uma etapa de fluxo de trabalho personalizada	501
Permissões do IAM para a etapa de personalizar	502
Políticas do IAM para fluxos de trabalho	503
relação de confiança no fluxo de trabalho	505
Exemplo de função de execução: descriptografar, copiar e marcar	505
Exemplo de função de execução: executar função e excluir	507

Tratamento de exceções para um fluxo de trabalho	508
Monitore a execução do fluxo	509
CloudWatch registro para um fluxo de trabalho	509
CloudWatch métricas para fluxos de trabalho	512
Criar fluxo de trabalho a partir de modelo	512
Remover um fluxo de trabalho de um servidor Transfer Family	516
Restrições e limites	517
Gerenciamento de servidores	520
Exibir uma lista de servidores	520
Excluir um servidor	521
Exibir detalhes do servidor SFTP	522
Exibir detalhes do servidor AS2	523
Suporte a IPv6	525
Limitações do IPv6	526
Configurando o IPv6 para servidores	526
Use o ALB para servidor público AS2 de pilha dupla	527
Editar detalhes do servidor	529
Edite os protocolos de transferência de arquivo	532
Edite o endpoint do servidor	534
Editar registro em log	535
Edite a política de segurança	536
Altere o fluxo de trabalho gerenciado	538
Altere os banners de exibição do seu servidor	539
Coloque seu servidor online ou offline	539
Editar a configuração do provedor de identidade	540
Mudando para provedor de identidade gerenciado por serviços	541
Mudando para AWS Directory Service	541
Mudando para um provedor de identidade personalizado	541
Preservação do usuário durante as transições do provedor de identidade	547
Considerações importantes ao alterar os provedores de identidade	547
Gerencie chaves de host do servidor	547
Quando importar chaves de host	549
Adicionar uma chave de host do servidor adicional	549
Excluir uma chave de host do servidor	551
Altere as chaves do host do servidor	552
Informações adicionais sobre a chave do host do servidor	554

Monitore o uso no console	554
Gerenciar controles de acesso	561
Como criar uma política de acesso ao bucket do S3	562
Criar uma política de sessão	563
Exemplo de política de sessão	564
Substituições aninhadas para políticas de sessão	567
Gerenciamento dinâmico de permissões	567
Entendendo a arquitetura de permissão do Transfer Family	567
Duas abordagens para o gerenciamento de permissões	568
Implementando políticas de sessão	569
Implementação por tipo de usuário	570
Exemplo: simplificação do gerenciamento de funções com políticas de sessão	570
CloudTrail registro	574
Ativando CloudTrail o registro	576
Habilitando eventos de dados do Amazon S3	576
Exemplo de entrada de registro para criar um servidor	577
Registros de acesso a dados	578
Exemplo de entrada de registro para acesso bem-sucedido aos dados	578
Operações comuns de acesso a dados	581
CloudWatch registro	582
Tipos de CloudWatch registro para Transfer Family	582
Criação de registros para servidores	584
Criação de registros para servidores	587
Atualizando registro em logs de um servidor	588
Como visualizar a configuração do servidor	591
Gerenciando registros para fluxos de trabalho	593
Configurando uma função para CloudWatch	596
Visualizando fluxos de registros do Transfer Family	598
Criação de CloudWatch alarmes na Amazon	602
Registrar chamadas de API S3 em logs de acesso S3	603
Exemplos para limitar o problema de "confused deputy"	603
CloudWatch estrutura de log para Transfer Family	605
Registros estruturados JSON para Transfer Family	605
Registros legados para Transfer Family	608
Exemplo de entradas CloudWatch de registro	611
Exemplo de entradas de registro de sessões de transferência	612

Exemplo de entradas de registro para conectores SFTP	613
Exemplo de entradas de registro para conectores VPC Lattice	615
Exemplo de entradas de registro para falhas no algoritmo de troca de chaves	616
Usando CloudWatch métricas	617
Dimensões do Transfer Family	622
Notificações ao usuário	622
CloudWatch consultas	623
Gerenciando eventos usando EventBridge	626
Transfer Family eventos	627
Eventos de servidor SFTP, FTPS e FTP	627
Eventos do conector SFTP	630
Eventos AS2	631
Enviar eventos do Transfer Family	632
Como criar padrões de eventos	634
Testando padrões de Transfer Family eventos para eventos	635
Permissões	635
Recursos adicionais do	636
Referência detalhada de eventos	636
Eventos do servidor	637
Eventos do Connector	644
Eventos AS2	652
Segurança	658
Benefícios da segurança da conectividade VPC	659
Modelo de segurança VPC Lattice	659
Práticas recomendadas de segurança para conectividade VPC	660
Políticas de segurança para servidores	660
Algoritmos criptográficos	662
Detalhes da política de segurança	673
Políticas de segurança para conectores SFTP	691
Algoritmos criptográficos	691
Detalhes da política de segurança do conector SFTP	692
Post-Quantum políticas de segurança	694
Sobre a troca de chaves híbrida pós-quântica híbrida no SSH	695
Como usar	696
Como testá-la	697
Proteção de dados	700

Criptografia de dados no Transfer Family	701
Criptografia em repouso	703
Gerenciamento de chaves	704
Visão geral do algoritmo	704
Autenticação SSH	705
Algoritmos PGP	706
Gerar Chaves SSH	708
Alterar chaves SSH	713
Gerar chaves PGP	716
Gerenciar chaves PGP	717
Clientes PGP compatíveis	722
Gerenciamento de identidade e acesso	723
Público	724
Autenticação com identidades	724
Gerenciar o acesso usando políticas	726
Como AWS Transfer Family funciona com o IAM	728
Identity-based exemplos de políticas	732
Tag-based exemplos de políticas	735
Solução de problemas de identidade e acesso	738
Chaves de condição do IAM	741
Validação de conformidade	743
Resiliência	743
VPC endpoints para APIs	744
Controle do acesso usando políticas de VPC endpoint	745
Criar endpoint da VPC	746
Segurança da infraestrutura	746
Considerações sobre NLB e NAT	747
Segurança da infraestrutura de conectividade VPC	748
Firewall da aplicação web	749
Cross-service prevenção delegada confusa	750
Alterar funções de usuário do Transfer Family	752
Funções do fluxo de trabalho do Transfer Family	754
Funções do conector Transfer Family	755
Transferir logging/invoction funções da Transfer Family	757
AWS políticas gerenciadas	758
AWSTransferConsoleFullAccess	759

AWSTransferFullAccess	759
AWSTransferLoggingAccess	759
AWSTransferReadOnlyAccess	759
Atualizações da política	760
Módulos Transfer Family Terraform	761
Servidores SFTP	761
Conectores SFTP	761
COMO 2	762
B2B Data Interchange	762
Solução de problemas do Transfer Family	763
Problemas de autenticação	763
Falhas de autenticação— SSH/SFTP	764
Problema de realm incompatíveis do AD gerenciado	764
Limites de grupos do Active Directory excedidos	765
Problemas de autenticação diversos	765
Solução de problemas do Amazon API Gateway	766
Solução de problemas ao testar seu provedor de identidade	768
Buckets duplicados do Amazon S3 em um aplicativo web	335
Problemas com o conector SFTP	769
Solução de problemas ao adicionar chaves de host confiáveis para seu conector SFTP	769
Falha na negociação chave	770
Limitação do conector SFTP	770
Otimizando o desempenho do conector SFTP	771
Solucionar problemas de conectividade da VPC	772
Problemas diversos do conector SFTP	775
Problemas de conectividade SFTP	775
Solucionar problemas de conectividade SFTP	776
Solucionar problemas do cliente SFTP	776
Solução de problemas de upload de arquivos	776
Solucionar problemas do conector SFTP do tipo de saída VPC	778
Problemas com provedores de identidade personalizados	780
Solucionar erros de integração do API Gateway	780
Solucionar problemas de tempo limite da função Lambda	781
Solucione problemas consistentes de tempo limite do Lambda	782
Solucionar problemas de exceções KeyError	783
Problemas de fluxo de trabalho	783

Solução de problemas de fluxos de trabalho gerenciados	783
Solução de problemas de decodificação do fluxo de trabalho	786
Problemas com o EFS	790
Solução de problemas do Amazon EFS	790
Problemas de armazenamento e criptografia	793
Solução de problemas de políticas para buckets criptografados do Amazon S3	793
Solução de problemas de exceção ResourceNotFound	794
Problemas de monitoramento e alerta	794
Solucionar problemas de métricas ausentes ou incompletas CloudWatch	795
Solucionar problemas de eventos ausentes EventBridge	795
Cross-region problemas de transferência	797
Solucionar problemas de permissão de transferência entre regiões	797
Solucionar problemas de desempenho de transferência entre regiões	799
Problemas de implantação do Terraform	800
Solucionar problemas de falha na criação de recursos do Terraform	800
Solucionar problemas de gerenciamento de estado do Terraform	801
Problemas de integração do WAF	802
Solucionar problemas de bloqueio de tráfego legítimo pelo WAF	802
Solucione problemas de integração do WAF com provedores de identidade personalizados	803
Service-managed problemas do usuário	804
Solução de problemas de usuários gerenciados por serviços	804
Problemas do AS2	805
Solução de problemas do AS2	805
Problemas com o certificado AS2	806
Problemas de recebimento do AS2 MDN	806
Problemas de monitoramento da expiração do certificado	807
Referência da API	808
Como fazer solicitações de API	809
Cabeçalhos de solicitação obrigatórios do Transfer Family	810
Entradas e assinaturas de solicitações do Transfer Family	810
Respostas de erro	811
Bibliotecas disponíveis	813
Provedores de identidade	813
Convenções	815
Formatos de identificação	815

Formatos ARN	815
DNS e endpoints	816
Endpoints da API	817
Endpoints do servidor	817
Histórico do documento	819
.....	dccccxxvi

O que é AWS Transfer Family?

AWS Transfer Family é um serviço de transferência segura que permite transferir arquivos para dentro e para fora dos serviços de AWS armazenamento. O Transfer Family faz parte da Nuvem AWS plataforma. AWS Transfer Family oferece suporte totalmente gerenciado para a transferência de arquivos via SFTP, AS2, FTPS, FTP e transferências baseadas em navegador da Web diretamente para dentro e para fora dos serviços de armazenamento. AWS Você pode migrar, automatizar e monitorar facilmente seus fluxos de trabalho de transferência de arquivos mantendo as configurações existentes do lado do cliente para autenticação, acesso e firewalls, para que nada mude para seus clientes, parceiros e equipes internas ou seus aplicativos. Consulte [Introdução AWS](#) para saber mais e começar a criar aplicativos em nuvem com a Amazon Web Services.

AWS Transfer Family suporta a transferência de dados de ou para os seguintes serviços AWS de armazenamento.

- Armazenamento do Amazon Simple Storage Service (Amazon S3). Para obter mais informações sobre o Amazon S3, consulte [Conceitos básicos do Amazon Simple Storage Service](#).
- Sistemas de arquivos Network File System (NFS) do Amazon Elastic File System (Amazon EFS). Para obter mais informações sobre o Amazon EFS, consulte [O que é o Sistema de arquivos elásticos da Amazon?](#)

AWS Transfer Family suporta a transferência de dados pelos seguintes protocolos:

- Protocolo de transferência segura de arquivos (SFTP): versão 3

O documento oficial do IETF está aqui: [SSH File Transfer](#) Protocol draft-ietf-secsh-filexfer-02.txt.

- Protocolo de Transferência de Arquivos Seguro (FTPS)
- Protocolo de Transferência de Arquivos (FTP)
- Declaração de Aplicabilidade 2 (AS2)
- Browser-based transferências

Note

Para conexões de dados FTP e FTPS, o intervalo de portas que o Transfer Family usa para estabelecer o canal de dados é 8192-8200.

Os protocolos de transferência de arquivos são usados em fluxos de trabalho de intercâmbio de dados em diferentes setores, como serviços financeiros, saúde, publicidade e varejo, entre outros. O Transfer Family simplifica a migração dos fluxos de trabalho de transferência de arquivos para o AWS

Veja a seguir alguns casos de uso comuns do uso do Transfer Family com o Amazon S3:

- Reservas de dados AWS para uploads de terceiros, como fornecedores e parceiros.
- Subscription-based distribuição de dados com seus clientes.
- Transferências internas dentro da organização.

Veja a seguir alguns casos de uso comuns do Transfer Family com o Amazon EFS:

- Distribuição de dados
- Cadeia de suprimentos
- Gerenciamento de conteúdo
- Aplicativos de atendimento na Web

Veja a seguir alguns casos de uso comuns do Transfer Family com o AS2:

- Fluxos de trabalho com requisitos de conformidade que dependem de recursos de proteção e segurança de dados incorporados ao protocolo
- Logística da cadeia de suprimentos
- Fluxos de trabalho de pagamentos
- Business-to-business Transações (B2B)
- Integrações com sistemas de planejamento de recursos corporativos (ERP) e gerenciamento de relacionamento com o cliente (CRM)

A seguir estão alguns casos de uso comuns para usar os aplicativos web Transfer Family:

- Acesso simplificado aos dados no Amazon S3 para uma gama mais ampla e diversificada de usuários corporativos
- Gerenciamento centralizado de acesso a dados para sua força de trabalho
- Visualização dos Amazon S3 Access Grants por meio de uma interface gerenciada

Com o Transfer Family, você tem acesso a um servidor habilitado para o protocolo de transferência de arquivos AWS (ou a uma interface web de transferência de arquivos gerenciada), sem a necessidade de executar nenhuma infraestrutura de servidor. Você pode usar esse serviço para migrar seus fluxos de trabalho baseados em transferência de arquivos e, ao AWS mesmo tempo, manter os clientes e as configurações dos usuários finais como estão. Para servidores, primeiro você associa seu nome de host ao endpoint do servidor, depois adiciona seus usuários e fornece a eles o nível certo de acesso. Depois de fazer isso, suas solicitações de transferência de usuários serão atendidas diretamente pelo endpoint do servidor do Transfer Family.

Para aplicativos web Transfer Family, determine suas configurações e aplique personalizações opcionais. Depois de fazer isso, seus usuários podem fazer login e transferir dados diretamente de e para o Amazon S3.

O Transfer Family oferece os seguintes benefícios:

- Um serviço totalmente gerenciado que pode ser dimensionado em tempo real para atender às suas necessidades.
- Você não precisa modificar seus aplicativos nem executar nenhuma infraestrutura de protocolo de transferência de arquivos.
- Com seus dados no armazenamento durável do Amazon S3, você pode usar o nativo Serviços da AWS para processamento, análise, emissão de relatórios, auditoria e funções de arquivamento.
- Com o Amazon EFS como seu armazenamento de dados, você obtém um sistema de arquivos elástico totalmente gerenciado para uso com Nuvem AWS serviços e recursos locais. O Amazon EFS foi criado para escalar sob demanda para petabytes sem interromper os aplicativos, podendo aumentar ou diminuir à medida que arquivos são adicionados e removidos. Isso ajuda a eliminar a necessidade de provisionar e gerenciar a capacidade para acomodar o crescimento.
- Um serviço de fluxo de trabalho de transferência de arquivos totalmente gerenciado e com tecnologia sem servidor que facilita a configuração, a execução, a automação e o monitoramento do processamento de arquivos enviados usando o AWS Transfer Family.
- Não há custos adiantados, e você paga apenas pelo uso do serviço.

Nas seções a seguir, você encontrará uma descrição dos diferentes recursos do Transfer Family, um tutorial de introdução, instruções detalhadas sobre como configurar os diferentes servidores habilitados para protocolos, como usar diferentes tipos de provedores de identidade e a referência da API do serviço.

Para aprender os conceitos básicos do Transfer Family, consulte:

- [Como AWS Transfer Family funciona](#)
- [Pré-requisitos](#)
- [Introdução aos endpoints de AWS Transfer Family servidor](#)
- [Aplicativos web Transfer Family](#)

Como AWS Transfer Family funciona

AWS Transfer Family é um AWS serviço totalmente gerenciado que você pode usar para transferir arquivos para dentro e para fora do armazenamento do Amazon Simple Storage Service (Amazon S3) ou dos sistemas de arquivos do Amazon Elastic File System (Amazon EFS) por meio dos seguintes protocolos ou navegadores da web:

- Protocolo de transferência segura de arquivos (SFTP): versão 3

O documento oficial do IETF está aqui: [SSH File Transfer](#) Protocol draft-ietf-secsh-filexfer-02.txt.

- Protocolo de Transferência de Arquivos Seguro (FTPS)
- Protocolo de Transferência de Arquivos (FTP)
- Declaração de Aplicabilidade 2 (AS2)
- Browser-based transferências

AWS Transfer Family suporta até 3 zonas de disponibilidade e é apoiado por uma frota redundante e de escalonamento automático para suas solicitações de conexão e transferência. Para obter um exemplo de como criar maior redundância e minimizar a latência da rede usando o Latency-based roteamento, consulte a postagem do blog [Minimize a latência da rede com sua AWS](#) transferência para servidores SFTP.

O Transfer Family Managed File Transfer Workflows (MFTW) é um serviço de fluxo de trabalho de transferência de arquivos totalmente gerenciado e de tecnologia sem servidor que facilita a configuração, a execução, a automação e o monitoramento do processamento de arquivos enviados usando AWS Transfer Family. Os clientes podem usar o MFTW para automatizar várias etapas de processamento, como cópia, marcação, digitalização compressing/decompressing, filtragem e os dados que são transferidos usando encrypting/decrypting o Transfer Family. Isso fornece visibilidade de ponta a ponta para rastreamento e auditabilidade. Consulte mais detalhes em [AWS Transfer Family fluxos de trabalho gerenciados](#).

AWS Transfer Family suporta qualquer cliente de protocolo de transferência de arquivos padrão.

Alguns clientes comumente usados são:

- [OpenSSH](#) - Um utilitário de linha de comando da Macintosh e Linux.
- [WinSCP](#) — Windows-only Um cliente gráfico.
- [Cyberduck](#) - Um cliente gráfico Linux, Macintosh e Microsoft Windows.
- [FileZilla](#)— Um cliente gráfico Linux, Macintosh e Windows.

AWS oferece os seguintes workshops do Transfer Family.

- Crie uma solução de transferência de arquivos que utilize SFTP/FTPS endpoints gerenciados e Amazon Cognito e DynamoDB para gerenciamento de usuários. AWS Transfer Family É possível ver os detalhes desse workshop [aqui](#).
- [Crie um endpoint Transfer Family com AS2 habilitado e um conector Transfer Family AS2. Você pode ver os detalhes deste workshop aqui.](#)
- Crie uma solução que forneça orientação prescritiva e um laboratório prático sobre como você pode criar uma arquitetura de transferência de arquivos escalável e segura AWS sem precisar modificar os aplicativos existentes ou gerenciar a infraestrutura do servidor. É possível ver os detalhes desse workshop [aqui](#).

Publicações de blog relevantes para o Transfer Family

A tabela a seguir lista as publicações do blog que contêm informações úteis para clientes do Transfer Family. A tabela está em ordem cronológica inversa, de forma que as postagens mais recentes estejam no início da tabela.

Título e link da publicação do blog	Data
Implante o Okta como um provedor de identidade personalizado para AWS Transfer Family	11 de agosto de 2025
Automatizando o processamento de solicitações de saúde de papel para eletrônico com AWS	29 de maio de 2025

Título e link da publicação do blog	Data
Como usar AWS Transfer Family e GuardDuty para proteção contra malware	30 de abril de 2025
Como a FICO moderniza as transferências de arquivos com a automação ETL usando AWS Transfer Family	24 de abril de 2025
Anunciando aplicativos AWS Transfer Family web para transferências de arquivos totalmente gerenciadas do Amazon S3	1.º de dezembro de 2024
Seis dicas para melhorar a segurança do seu AWS Transfer Family servidor	24 de setembro de 2024
Simplifique a autenticação do Active Directory com um provedor de identidade personalizado para AWS Transfer Family	12 de agosto de 2024
Arquitetando transferências de arquivos gerenciadas seguras e compatíveis com conectores AWS Transfer Family SFTP e criptografia PGP	16 de maio de 2024
Usando o Amazon Cognito como provedor de identidade com o Amazon AWS Transfer Family S3	14 de maio de 2024
Como a Transfer Family pode ajudar você a criar uma solução de transferência gerenciada de arquivos segura e compatível	3 de janeiro de 2024
Detecte ameaças de malware usando AWS Transfer Family	20 de julho de 2023
Estendendo as cargas de trabalho do SAP com AWS Transfer Family	13 de julho de 2023

Título e link da publicação do blog	Data
Criptografe e descriptografe arquivos com PGP e AWS Transfer Family	21 de junho de 2023
Autenticando AWS Transfer Family com o Azure Active Directory e AWS Lambda	15 de dezembro de 2022
Personalize as notificações de entrega de arquivos usando fluxos de trabalho AWS Transfer Family gerenciados	14 de outubro de 2022
Construir uma plataforma de transferência de arquivos nativa de nuvem usando fluxos de trabalho do AWS Transfer Family	5 de janeiro de 2022
Habilitando o gerenciamento de chaves de autoatendimento do usuário com A AWS Transfer Family e AWS Lambda	17 de dezembro de 2021
Melhore o controle de acesso aos dados com AWS Transfer Family o Amazon S3	5 de outubro de 2021
Melhore a produtividade de transferências de arquivos, usos AWS Global Accelerator e AWS Transfer Family serviços voltados para a Internet	7 de junho de 2021
Protegendo AWS Transfer Family com o AWS Web Application Firewall e o Amazon API Gateway	5 de maio de 2021
Protegendo AWS Transfer Family com o AWS Web Application Firewall e o Amazon API Gateway	15 de janeiro de 2021
AWS Transfer Family suporte para Amazon Elastic File System	7 de janeiro de 2021

Título e link da publicação do blog	Data
Ativar a autenticação por senha para AWS Transfer Family usar AWS Secrets Manager	5 de novembro de 2020
Centralize o acesso aos dados usando AWS Transfer Family e AWS Storage Gateway	22 de junho de 2020
Usando o Amazon EFS AWS Lambda em seus aplicativos sem servidor	18 de junho de 2020
Use a lista de permissões de IP para proteger seus AWS Transfer Family servidores	8 de abril de 2020
Minimize a latência da rede com sua AWS transferência para servidores SFTP	19 de fevereiro de 2020
Migração Lift and Shift de servidores SFTP para AWS	12 de fevereiro de 2020
Simplifique sua estrutura AWS SFTP com chroot e diretórios lógicos	26 de setembro de 2019
Usando o Okta como provedor de identidade com AWS Transfer Family	30 de maio de 2019

Pré-requisitos

As seções a seguir descrevem os pré-requisitos necessários para usar o serviço. AWS Transfer Family No mínimo, você precisa criar um bucket do Amazon Simple Storage Service (Amazon S3) e fornecer acesso a esse bucket por meio de AWS Identity and Access Management uma função (IAM). Sua função também precisa estabelecer uma relação de confiança. Essa relação de confiança permite ao Transfer Family assumir ao perfil do IAM para acessar seu bucket para que ele possa atender às solicitações de transferência de arquivos.

Para obter informações sobre o suporte a IPv6 para AWS Transfer Family servidores, consulte o [Suporte IPv6 para servidores Transfer Family](#) capítulo Gerenciando servidores.

Tópicos

- [AWS Regiões, endpoints e cotas compatíveis com servidores Transfer Family](#)
- [Inscreva-se para AWS](#)
- [Configurar o armazenamento para uso com AWS Transfer Family servidores](#)
- [Criar uma política e um perfil do IAM](#)

AWS Regiões, endpoints e cotas compatíveis com servidores Transfer Family

Para se conectar programaticamente a um AWS serviço, você usa um endpoint. Por exemplo, o endpoint para clientes na região Leste dos EUA (Ohio) (us-east-2), é `transfer.us-east-2.amazonaws.com`. As cotas de serviço, também chamadas de limites, correspondem ao número máximo de recursos ou operações de serviço para sua Conta da AWS. Neste guia, você pode encontrar cotas em [Cotas AS2](#) e [Cotas da para conectores SFTP](#)

Para obter mais informações sobre AWS regiões, endpoints e cotas de serviço compatíveis, consulte [AWS Transfer Family endpoints e cotas](#) no. Referência geral da Amazon Web Services

Para aplicativos web Transfer Family, as regiões suportadas estão listadas em [Regiões da AWS para aplicativos web Transfer Family](#). Para cotas relacionadas aos aplicativos web Transfer Family, consulte. [Cotas de aplicativos web](#)

Inscreva-se para AWS

Quando você se inscreve no Amazon Web Services (AWS), sua AWS conta é automaticamente cadastrada em todos os serviços em AWS, inclusive AWS Transfer Family. A cobrança incorrerá apenas pelos serviços utilizados.

Se você já tiver uma AWS conta, vá para a próxima tarefa. Se ainda não possuir uma conta da AWS, use o procedimento a seguir para criar uma.

Se você não tiver uma Conta da AWS, conclua as etapas a seguir para criar uma.

Para se inscrever em uma Conta da AWS

1. Abra o <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções online.

Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo teclado do telefone.

Quando você se inscreve em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar [tarefas que exigem acesso de usuário-raiz](#).

Para obter informações sobre preços e como usar AWS Calculadora de Preços para obter uma estimativa do custo de uso do Transfer Family, consulte [AWS Transfer Family preços](#).

Para obter informações sobre a disponibilidade AWS da região, consulte os [AWS Transfer Family endpoints e as cotas](#) no. Referência geral da AWS

Configurar o armazenamento para uso com AWS Transfer Family servidores

Este tópico descreve as opções de armazenamento que você pode usar com AWS Transfer Family. Você pode usar o Amazon S3 ou o Amazon EFS como armazenamento para seus servidores Transfer Family.

Sumário

- [Configurar um bucket do Amazon S3](#)
 - [Pontos de acesso Amazon S3](#)
 - [Comportamento do Amazon S3 HeadObject](#)
 - [Conceder a capacidade de somente gravar e listar arquivos](#)
 - [Grande número de objetos de zero byte causando problemas de latência](#)
- [Configurar um sistema de arquivos Amazon EFS](#)
 - [Propriedade do arquivo do Amazon EFS](#)
 - [Configurar usuários do Amazon EFS para Transfer Family](#)
 - [Configurar usuários do Transfer Family no Amazon EFS](#)
 - [Crie um usuário raiz do Amazon EFS](#)
 - [Comandos do Amazon EFS compatíveis](#)

Configurar um bucket do Amazon S3

AWS Transfer Family acessa seu bucket do Amazon S3 para atender às solicitações de transferência de seus usuários, então você precisa fornecer um bucket do Amazon S3 como parte da configuração do seu servidor habilitado para o protocolo de transferência de arquivos. Você pode usar um bucket existente ou criar um novo.

Note

Você não precisa usar um servidor e o bucket do Amazon S3 que estão na mesma região da AWS, mas essa é uma prática recomendada.

Ao configurar seus usuários, você atribui um perfil do IAM a cada um. Essa função determina o nível de acesso que eles têm no bucket do Amazon S3.

Para obter mais informações sobre como criar um novo bucket, consulte [Como criar um bucket S3?](#), no Guia do usuário do Amazon Simple Storage Service.

Note

Você pode usar o bloqueio de objetos do Amazon S3 para evitar que um objeto seja excluído ou substituído por um período fixo ou indefinidamente. Isso funciona da mesma forma com o

Transfer Family e com outros serviços. Se um objeto existe e está protegido, não é permitido gravar nesse arquivo nem excluí-lo. Para obter mais detalhes sobre o bloqueio de objetos do Amazon S3, consulte [Usar o bloqueio de objetos do Amazon S3](#) no Guia do usuário do Amazon Simple Storage Service.

Pontos de acesso Amazon S3

AWS Transfer Family oferece suporte [aos pontos de acesso do Amazon S3](#), um recurso do Amazon S3 que permite gerenciar facilmente o acesso granular a conjuntos de dados compartilhados. É possível usar aliases de ponto de acesso do S3 em qualquer lugar em que você use nomes de bucket do S3. Você pode criar centenas de pontos de acesso no Amazon S3 para usuários que têm permissões diferentes para acessar dados compartilhados em um bucket do Amazon S3.

Por exemplo, você pode usar pontos de acesso para permitir que três equipes diferentes tenham acesso ao mesmo conjunto de dados compartilhado, em que uma equipe pode ler dados do S3, uma segunda equipe pode gravar dados no S3 e a terceira equipe pode ler, gravar e excluir dados do S3. Para implementar um controle de acesso granular, conforme mencionado acima, você pode criar um ponto de acesso S3 que contenha uma política que dê acesso assimétrico a diferentes equipes. Você pode usar pontos de acesso do S3 com seu servidor do Transfer Family para obter um controle de acesso refinado, sem criar uma política complexa de bucket do S3 que abranja centenas de casos de uso. Para saber mais sobre como usar os pontos de acesso do S3 com um servidor Transfer Family, consulte a postagem do [blog Enhance data access control with AWS Transfer Family on Amazon S3](#).

Note

AWS Transfer Family atualmente não oferece suporte aos pontos de Multi-Region acesso do Amazon S3.

Comportamento do Amazon S3 HeadObject

Note

Ao criar ou atualizar um servidor Transfer Family, você pode otimizar o desempenho dos diretórios do Amazon S3, o que elimina chamadas. `HeadObject`

Nos buckets e objetos do Amazon S3 estão os recursos primários e os objetos são armazenados em buckets. O Amazon S3 pode imitar um sistema de arquivos hierárquico, mas às vezes pode se comportar de modo diferente de um sistema de arquivos típico. Por exemplo, os diretórios não são um conceito de primeira classe no Amazon S3, mas são baseados em chaves de objeto. AWS Transfer Family infere um caminho de diretório dividindo a chave de um objeto pelo caractere de barra (/), tratando o último elemento como o nome do arquivo e agrupando os nomes dos arquivos que têm o mesmo prefixo no mesmo caminho. Zero-byte objetos são criados para representar o caminho de uma pasta quando você cria um diretório vazio usando `mkdir` ou usando o console Amazon S3. A chave para esses objetos termina em uma barra lateral. Esses objetos de zero bytes são descritos em [Organização de objetos no console do Amazon S3 usando pastas](#) no Guia do usuário do Amazon S3.

Quando você executa um `ls` comando e alguns resultados são objetos de zero bytes do Amazon S3 (esses objetos têm chaves que terminam na barra), o Transfer Family `HeadObject` emite uma solicitação para cada um desses objetos (consulte a Referência da API [HeadObject](#) do Amazon Simple Storage Service para obter detalhes). Isso pode resultar nos seguintes problemas ao usar o Amazon S3 como seu armazenamento com o Transfer Family.

Conceder a capacidade de somente gravar e listar arquivos

Em alguns casos, talvez você queira oferecer somente acesso de gravação aos seus objetos do Amazon S3. Por exemplo, talvez você queira fornecer acesso para escrever (ou fazer upload) e listar objetos em um bucket, mas não para ler (baixar) objetos. Para executar `ls mkdir` comandos usando clientes de transferência de arquivos, você deve ter o Amazon S3 `ListObjects` e `PutObject` as permissões. No entanto, quando a Transfer Family precisa fazer uma `HeadObject` chamada para gravar ou listar arquivos, a chamada falha com um erro de Acesso negado, pois essa chamada requer a `GetObject` permissão.

Note

Ao criar ou atualizar um servidor Transfer Family, você pode otimizar o desempenho dos diretórios do Amazon S3, o que elimina chamadas. `HeadObject`

Nesse caso, você pode conceder acesso adicionando uma condição de política AWS Identity and Access Management (IAM) que adiciona a `GetObject` permissão somente para objetos que terminam em uma barra (/). Essa condição impede `GetObject` chamadas em arquivos (para que eles não possam ser lidos), mas permite que o usuário liste e percorra pastas. O exemplo de política

a seguir oferece somente acesso de gravação e lista aos seus buckets do Amazon S3. Para usar essa política, *amzn-s3-demo-bucket* substitua pelo nome do seu bucket.

 Note

Para abordar o comportamento de upload do WinSCP, certifique-se de adicionar a "arn:aws:s3:::amzn-s3-demo-bucket/*.*filepart" linha conforme listado no exemplo de política a seguir. Essa linha garante o manuseio adequado dos objetos.filepart para evitar falhas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListing",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "AllowReadWrite",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Sid": "DenyIfNotFolder",
      "Effect": "Deny",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "NotResource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*/*",
        "arn:aws:s3:::amzn-s3-demo-bucket/*.*filepart"
      ]
    }
  ]
}
```

```
    ]
  }
]
}
```

Note

Essa política não permite o acesso dos usuários a arquivos. Em outras palavras, um usuário designado a essa política não pode abrir arquivos para adicionar conteúdo a eles ou modificá-los. Além disso, se seu caso de uso exigir uma chamada do `HeadObject` antes de fazer o upload de um arquivo, essa política não funcionará para você.

Grande número de objetos de zero byte causando problemas de latência

Se seus buckets do Amazon S3 contiverem um grande número desses objetos de zero bytes, o Transfer Family emitirá muitas chamadas, o que pode resultar em `HeadObject` atrasos no processamento. A solução recomendada para esse problema é permitir que os diretórios otimizados reduzam a latência.

Por exemplo, suponha que você acesse seu diretório inicial e tenha 10.000 subdiretórios. Em outras palavras, seu bucket do Amazon S3 tem 10.000 pastas. Nesse cenário, se você executar o comando `ls` (`list`), a operação de lista levará entre seis e oito minutos. No entanto, se você otimizar seus diretórios, essa operação levará apenas alguns segundos. Você define essa opção na tela Configurar detalhes adicionais durante o procedimento de criação ou atualização do servidor. Esses procedimentos são detalhados no [Configurando um endpoint de servidor SFTP, FTPS ou FTP](#) tópico.

Note

Os clientes da GUI podem emitir um `ls` comando fora do seu controle, portanto, é importante habilitar essa configuração, se possível.

Se você não otimiza ou não consegue otimizar seus diretórios, uma solução alternativa para esse problema é excluir todos os objetos de zero bytes. Observe o seguinte:

- Os diretórios vazios não existirão mais. Os diretórios só existem porque seus nomes estão na chave de um objeto.

- Não impede que alguém ligue para `mkdir` e quebre tudo de novo. Você pode mitigar isso criando uma política que impeça a criação de diretórios.
- Alguns cenários usam esses objetos de 0 byte. Por exemplo, você tem uma estrutura como `inboxes/customer1000` e o diretório da caixa de entrada é limpo todos os dias.

Por fim, mais uma solução possível é limitar o número de objetos visíveis por meio de uma condição de política para reduzir o número de `HeadObject` chamadas. Para que essa seja uma solução viável, você precisa aceitar que talvez só consiga visualizar um conjunto limitado de todos os seus subdiretórios.

Configurar um sistema de arquivos Amazon EFS

AWS Transfer Family acessa o Amazon Elastic File System (Amazon EFS) para atender às solicitações de transferência de seus usuários. Portanto, você deve fornecer um sistema de arquivos do Amazon EFS como parte da configuração do seu servidor habilitado para o protocolo de transferência de arquivos. Você pode usar um sistema de arquivo existente ou criar um novo.

Observe o seguinte:

- Quando você usa um servidor Transfer Family e um sistema de arquivos Amazon EFS, o servidor e o sistema de arquivos devem estar na mesma Região da AWS.
- O servidor e o sistema de arquivos não precisam estar na mesma conta. Se o servidor e o sistema de arquivos não estiverem na mesma conta, a política do sistema de arquivos deverá dar permissão explícita à função do usuário.

Para obter informações sobre como configurar várias contas, consulte [Gerenciando as AWS contas em sua organização](#) no Guia do AWS Organizations usuário.

- Ao configurar seus usuários, você atribui um perfil do IAM a cada um. Essa função determina o nível de acesso que eles têm ao seu sistema de arquivos Amazon EFS.
- Para obter detalhes sobre a montagem de um sistema de arquivos Amazon EFS, consulte [Montagem de sistemas de arquivos Amazon EFS](#).

Para obter mais detalhes sobre como o Amazon EFS AWS Transfer Family e o Amazon EFS trabalham juntos, consulte [Uso AWS Transfer Family para acessar arquivos em seu sistema de arquivos Amazon EFS](#) no Guia do usuário do Amazon Elastic File System.

Propriedade do arquivo do Amazon EFS

O Amazon EFS usa o modelo de permissão de arquivo da Portable Operating System Interface (POSIX) para representar a propriedade do arquivo.

No POSIX, os usuários do sistema são categorizados em três classes de permissão distintas: Quando você permite que um usuário acesse arquivos armazenados em um sistema de arquivos Amazon EFS usando AWS Transfer Family, você deve atribuir a ele um “perfil POSIX”. Esse perfil é usado para determinar seu acesso aos arquivos e diretórios no sistema de arquivos do Amazon EFS.

- Usuário (u): Proprietário do arquivo ou diretório. Normalmente, o criador de um arquivo ou diretório também é o proprietário.
- Grupo (g): conjunto de usuários que precisam de acesso idêntico aos arquivos e diretórios que compartilham.
- Outros (o): todos os outros usuários que têm acesso ao sistema, exceto o proprietário e os membros do grupo. Essa classe de permissão também é conhecida como “Pública”.

No modelo de permissão POSIX, cada objeto do sistema de arquivos (arquivos, diretórios, links simbólicos, canais nomeados e soquetes) está associado aos três conjuntos de permissões já mencionados. Os objetos do Amazon EFS têm um Unix-style modo associado a eles. Esse valor de modo define as permissões para executar ações nesse objeto.

Além disso, em Unix-style sistemas, usuários e grupos são mapeados para identificadores numéricos, que o Amazon EFS usa para representar a propriedade do arquivo. Para Amazon EFS, os objetos são de propriedade de um único proprietário e um único grupo. O Amazon EFS utiliza esses IDs numéricos para verificar as permissões quando um usuário tenta acessar um objeto do sistema de arquivos.

Configurar usuários do Amazon EFS para Transfer Family

Antes de configurar os usuários do Amazon EFS, você pode executar uma das seguintes ações:

- Você pode criar usuários e configurar suas pastas pessoais no Amazon EFS. Para mais detalhes, consulte [Configurar usuários do Transfer Family no Amazon EFS](#).
- Se você se sentir confortável em adicionar um usuário raiz, poderá [Criar um usuário raiz do Amazon EFS](#).

 Note

Os servidores do Transfer Family não oferecem suporte aos pontos de acesso do Amazon EFS para definir permissões POSIX. Os perfis POSIX dos usuários do Transfer Family (descritos na seção anterior) permitem definir permissões POSIX. Essas permissões são definidas no nível do usuário, para acesso granular, com base em UID, no GID e em GIDs secundários.

Configurar usuários do Transfer Family no Amazon EFS

Transfer Family mapeia os usuários para os diretórios UID/GID e diretórios que você especificar. Se ainda UID/GID/directories não existirem no EFS, você deverá criá-los antes de atribuí-los em Transferir para um usuário. As informações para criação de usuários do Amazon EFS são descritas em [Working with users, groups, and permissions at the Network File System \(NFS\) Level](#) (Trabalhar com usuários, grupos e permissões no nível do Network File System (NFS)) no Guia do usuário do Amazon Elastic File System.

Etapas para configurar usuários do Amazon EFS para Transfer Family

1. Mapeie o UID e o GID do EFS do seu usuário no Transfer Family usando os campos [PosixProfile](#).
2. Se quiser que o usuário inicie em uma pasta específica após o login, especifique o diretório EFS no campo [HomeDirectory](#).

Você pode automatizar o processo usando uma CloudWatch regra e uma função Lambda. Para ver um exemplo da função Lambda que interage com o EFS, consulte Como usar o [Amazon EFS AWS Lambda em seus aplicativos](#) sem servidor.

Além disso, você pode configurar diretórios lógicos para os usuários do Transfer Family. Para obter detalhes, consulte a seção [Configure diretórios lógicos para o Amazon EFS](#) no tópico [Como usar diretórios lógicos para simplificar suas estruturas de diretórios do Transfer Family](#).

Crie um usuário raiz do Amazon EFS

Se sua organização quiser que você habilite o acesso do usuário root SFTP/FTPS por meio da configuração de seus usuários, você pode criar um usuário com UID e GID 0 (usuário raiz) e, em seguida, usar esse usuário raiz para criar pastas e atribuir proprietários de ID POSIX para o restante

dos usuários. A vantagem dessa opção é que não há necessidade de montar o sistema de arquivos do Amazon EFS.

Execute as etapas descritas em [Adicionar usuários gerenciados por serviços do Amazon EFS](#) e, para a ID do usuário e a ID do grupo, insira 0 (zero).

 Tip

Não deixe essa conta de superusuário existir por mais tempo do que o necessário. Ou, se você mantiver a conta de usuário root, certifique-se de mantê-la bem protegida.

Comandos do Amazon EFS compatíveis

Os comandos a seguir são compatíveis com Amazon EFS para AWS Transfer Family

- `cd`
- `ls/dir`
- `pwd`
- `put`
- `get`
- `rename`
- `chown`: apenas raiz (ou seja, usuários com `uid=0`) pode alterar a propriedade e as permissões dos arquivos e diretórios.
- `chmod`: apenas raiz pode alterar a propriedade e as permissões dos arquivos e diretórios.
- `chgrp`: há suporte para raiz e para o proprietário do arquivo que só pode alterar um grupo de arquivos para ser um dos grupos secundários.
- `ln -s/symlink`
- `mkdir`
- `rm/delete`
- `rmdir`
- `chmtime`

Criar uma política e um perfil do IAM

Este tópico descreve os tipos de políticas e funções que podem ser usadas e explica o processo de criação de uma função de usuário. AWS Transfer Family também descreve como as políticas de sessão funcionam e dá um exemplo de função de usuário.

AWS Transfer Family usa os seguintes tipos de funções:

- **Função de usuário** — Permite que usuários gerenciados pelo serviço acessem os recursos necessários do Transfer Family. AWS Transfer Family assume essa função no contexto de um ARN de usuário do Transfer Family.
- **Função de acesso**: fornece acesso apenas aos arquivos do Amazon S3 que estão sendo transferidos. Para transferências do AS2 de entrada, a função de acesso usa o nome do recurso da Amazon (ARN) para o contrato. Para transferências do AS2 de saída, a função de acesso usa o ARN para o conector.
- **Função de invocação**: para uso com o Amazon API Gateway como provedor de identidade personalizada do servidor. O Transfer Family assume essa função no contexto de um ARN do servidor do Transfer Family.
- **Função de registro** — usada para registrar entradas na Amazon CloudWatch. O Transfer Family usa essa função para registrar em log os detalhes de sucesso e falha com informações sobre transferências de arquivos. O Transfer Family assume essa função no contexto de um ARN do servidor do Transfer Family. Para transferências do AS2 de saída, a função de acesso usa o conector ARN.
- **Função de execução**: permite que um usuário do Transfer Family chame e inicie fluxos de trabalho. O Transfer Family assume essa função no contexto de um ARN de fluxo de trabalho do Transfer Family.

Além dessas funções, você também pode usar políticas de sessão. Uma política de sessão é usada para limitar o acesso quando necessário. Observe que essas políticas são independentes: ou seja, você não as adiciona a uma função. Em vez disso, você adiciona uma política de sessão diretamente a um usuário do Transfer Family.

Note

Ao criar um usuário do Transfer Family gerenciado pelo serviço, você pode selecionar a Auto-generate política com base na pasta inicial. Esse é um atalho útil se você quer limitar o acesso do usuário às suas próprias pastas. Além disso, você pode ver detalhes sobre

políticas de sessão e um exemplo em [Como funcionam as políticas de sessão](#). Você também pode encontrar mais informações sobre políticas de sessão em [Políticas de sessão](#) no Guia do usuário do IAM.

Tópicos

- [Criação de um perfil de usuário](#)
- [Como funcionam as políticas de sessão](#)
- [Exemplo de política de read/write acesso](#)

Criação de um perfil de usuário

Ao criar um usuário, você toma uma série de decisões sobre o acesso do usuário. Essas decisões incluem quais buckets do Amazon S3 ou sistemas de arquivos do Amazon EFS o usuário pode acessar, quais partes de cada bucket do Amazon S3 e quais arquivos no sistema de arquivos estão acessíveis e quais permissões o usuário tem (por exemplo, PUT ou GET).

Para definir o acesso, você cria uma política e uma função baseadas em identidade AWS Identity and Access Management (IAM) que fornecem essas informações de acesso. Como parte desse processo, você fornece acesso para o Amazon S3 bucket ou sistema de arquivos Amazon EFS que é o destino ou origem para operações de arquivo. Para isso, siga as etapas de alto nível a seguir, descritas em detalhes posteriormente:

Criação de um perfil de usuário

1. Crie uma política do IAM para AWS Transfer Family. Isso está descrito em [Para criar uma política do IAM para AWS Transfer Family](#).
2. Criar um perfil do IAM e associar a ela a nova política. Para ver um exemplo, consulte [Exemplo de política de read/write acesso](#).
3. Estabeleça uma relação de confiança entre AWS Transfer Family e a função do IAM. Isso está descrito em [Estabelecer um relacionamento de confiança](#).

Os procedimentos a seguir descrevem como criar uma política e um perfil do IAM.

Para criar uma política do IAM para AWS Transfer Family

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.

2. No painel de navegação, selecione Políticas e, em seguida, Criar política.
3. Na página Create Policy (Criar política), escolha a guia JSON.
4. No editor que é exibido, substitua o conteúdo do editor pelo perfil do IAM que você deseja anexar ao perfil do IAM.

Você pode conceder read/write acesso ou restringir os usuários ao diretório inicial. Para obter mais informações, consulte [Exemplo de política de read/write acesso](#).

5. Escolha Revisar política, forneça um nome e uma descrição para a sua política e em seguida selecione Criar política.

Em seguida, crie um perfil do IAM e anexe a nova política do IAM à ela.

Para criar uma função do IAM para AWS Transfer Family

1. No painel de navegação, escolha Roles (Funções) e Criar função.

Na página Criar função, certifique-se de que AWS Serviço foi escolhido.

2. Selecione Transferir na lista de serviço, e Próximo: Permissões. Isso estabelece uma relação de confiança entre AWS Transfer Family e AWS.
3. Na seção Anexar política de permissões, localize e selecione a política que você acabou de criar e selecione Próximo: Tags.
4. (Opcional) Insira uma chave e um valor para a tag e selecione Próximo: análise.
5. Na página Análise, insira um nome e uma descrição para a sua nova função, e escolha Criar função.

Em seguida, você estabelece uma relação de confiança entre AWS Transfer Family e AWS.

Estabelecer um relacionamento de confiança

Note

Em nossos exemplos, usamos tanto `ArnLike` quanto `ArnEquals`. Eles são funcionalmente idênticos, portanto, é possível usá-los ao criar suas políticas. A documentação do Transfer Family usa `ArnLike` quando a condição contém um caractere curinga, e `ArnEquals` para indicar uma condição de correspondência exata.

1. No console do IAM, selecione a função que você acabou de criar.
2. Na página Resumo, selecione Relacionamentos de confiança e selecione Editar relacionamento de confiança.
3. No editor Editar relacionamento de confiança, verifique se o serviço é "transfer.amazonaws.com". A política de acesso editada é mostrada a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Recomendamos o uso das chaves de condição `aws:SourceAccount` e `aws:SourceArn` para se proteger contra o problema confused deputy. A conta de origem é o proprietário do domínio e o ARN de origem é o ARN do usuário. Por exemplo:

```
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "account_id"
  },
  "ArnLike": {
    "aws:SourceArn": "arn:aws:transfer:region:account_id:user/*"
  }
}
```

Você também pode usar a condição `ArnLike` se quiser restringir a um servidor específico em vez de a qualquer servidor na conta do usuário. Por exemplo:

```
"Condition": {
  "ArnLike": {
    "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-id/*"
  }
}
```

```
}  
}
```

Note

Nos exemplos acima, substitua cada um *user input placeholder* por suas próprias informações.

Para obter detalhes sobre o problema do confused deputy e mais exemplos, consulte [Cross-service prevenção delegada confusa](#).

4. Selecione Atualizar política de confiança para atualizar a política de acesso.

Agora você criou uma função do IAM que permite AWS Transfer Family chamar AWS serviços em seu nome. Você anexou o perfil do IAM que você criou à função para conceder acesso ao seu usuário. Na seção [Introdução aos endpoints de AWS Transfer Family servidor](#), essa função e política são designadas ao(s) seu(s) usuário(s).

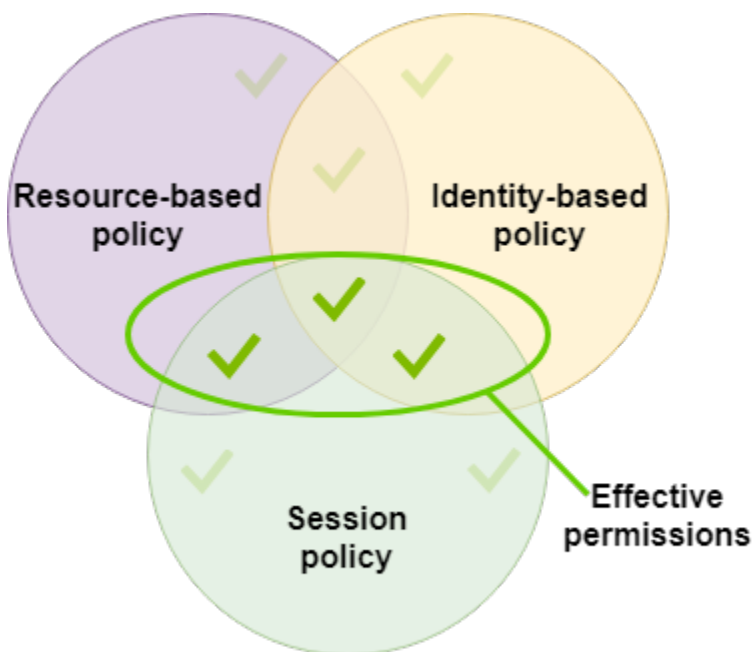
Consulte também

- Para obter mais informações gerais sobre as funções do IAM, consulte [Como criar uma função para delegar permissões a um AWS serviço](#) no Guia do usuário do IAM.
- Para saber mais sobre políticas baseada em identidade para recursos do Amazon S3, consulte o [Gerenciamento de identidade e acesso no Amazon S3](#) no Guia do Usuário do Amazon Simple Storage Service.
- Para saber mais sobre políticas baseadas em identidade para recursos do Amazon EFS, consulte [Como usar o IAM para controlar o acesso aos dados do sistema de arquivos](#) no Guia do usuário do Amazon Elastic File System.

Como funcionam as políticas de sessão

Quando um administrador cria uma função, a função geralmente inclui amplas permissões para cobrir vários casos de uso ou membros da equipe. Se um administrador configurar um [URL do console](#), poderá reduzir as permissões para a sessão resultante usando uma política de sessão. Por exemplo, se você criar uma função com [read/write acesso](#), poderá configurar uma URL que limite o acesso dos usuários somente aos diretórios pessoais.

As políticas de sessão são políticas avançadas que você transmite como um parâmetro quando você cria de forma programática uma sessão temporária para uma função ou usuário. As políticas de sessão são úteis para bloquear usuários para que eles tenham acesso apenas às partes do seu bucket em que os prefixos de objeto contêm seus nomes de usuário. O diagrama a seguir mostra que as permissões da sessão resultante são a interseção das políticas de sessão e das políticas baseadas em recurso, mais a interseção das políticas de sessão e das políticas baseadas em identidade.



Para obter mais informações, consulte [Políticas de sessão](#) no Guia do usuário do IAM.

Em AWS Transfer Family, uma política de sessão é suportada somente quando você está transferindo para ou do Amazon S3. A política de exemplo a seguir é uma política de sessão que limita o acesso dos usuários somente aos seus diretórios home. Observe o seguinte:

- As declarações de `GetObjectACL` e `PutObjectACL` só são necessárias se você precisar habilitar o acesso entre contas. Ou seja, seu servidor Transfer Family precisa acessar um bucket em uma conta diferente.
- O tamanho máximo de uma política de sessão é 2.048 caracteres. Para obter mais detalhes, consulte o [parâmetro de solicitação de política](#) para a `CreateUser` ação na referência da API.
- Se seu bucket do Amazon S3 for criptografado usando AWS Key Management Service (AWS KMS), você deverá especificar permissões adicionais em sua política. Para obter detalhes, consulte [Proteção e criptografia de dados](#).

- Para usar políticas de sessão para criar permissões de acesso com base nos atributos do usuário sem criar funções do IAM separadas para cada usuário, consulte [Abordagens dinâmicas de gerenciamento de permissões](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::${transfer:HomeBucket}"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "${transfer:HomeFolder}/*",
            "${transfer:HomeFolder}"
          ]
        }
      }
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
    }
  ]
}
```

 Note

O exemplo de política anterior pressupõe que os usuários tenham seus diretórios pessoais configurados para incluir uma barra final, para indicar que é um diretório. Se, por outro lado, você definir um `HomeDirectory` de usuário sem a barra final, então deve incluí-lo como parte de sua política.

No exemplo anterior da política, observe o uso dos parâmetros de política `transfer:HomeFolder`, `transfer:HomeBucket`, e `transfer:HomeDirectory`. Esses parâmetros são definidos para o `HomeDirectory` que está configurado para o usuário, conforme descrito em [HomeDirectoryImplementar seu método do API Gateway](#). Esses parâmetros têm as seguintes definições:

- O parâmetro `transfer:HomeBucket` é substituído pelo primeiro componente do `HomeDirectory`.
- O parâmetro `transfer:HomeFolder` é substituído pelas partes restantes do parâmetro `HomeDirectory`.
- O parâmetro `transfer:HomeDirectory` tem a barra inicial (/) removida para que possa ser usado como parte do nome do recurso da Amazon (ARN) do S3 em uma instrução `Resource`.

 Note

Se você estiver usando diretórios lógicos, ou seja, o `homeDirectoryType` do usuário é `LOGICAL`, esses parâmetros de política (`HomeBucket`, `HomeDirectory`, e `HomeFolder`) não serão compatíveis.

Por exemplo, suponha que o parâmetro `HomeDirectory` configurado para o usuário do Transfer Family seja `/home/bob/amazon/stuff/`.

- `transfer:HomeBucket` está definido como `/home`.
- `transfer:HomeFolder` está definido como `/bob/amazon/stuff/`.
- `transfer:HomeDirectory` se torna `home/bob/amazon/stuff/`.

O primeiro "Sid" permite que o usuário liste todos os diretórios a partir de `/home/bob/amazon/stuff/`.

O segundo "Sid" limita o acesso put e get do usuário ao mesmo caminho, `/home/bob/amazon/stuff/`.

Exemplo de política de read/write acesso

Conceda read/write acesso ao bucket do Amazon S3

O exemplo de política a seguir AWS Transfer Family concede read/write acesso a objetos em seu bucket do Amazon S3.

Observe o seguinte:

- Substitua `amzn-s3-demo-bucket` pelo nome do bucket do Amazon S3.
- As declarações de `GetObjectACL` e `PutObjectACL` só são necessárias se você precisar habilitar o acesso entre contas. Ou seja, seu servidor Transfer Family precisa acessar um bucket em uma conta diferente.
- As instruções `GetObjectVersion` e `DeleteObjectVersion` só serão necessárias se o versionamento estiver habilitado no bucket do Amazon S3 que está sendo acessado.

Note

Se você já habilitou o versionamento para seu bucket, precisará dessas permissões, pois você só pode suspender o versionamento no Amazon S3 e não desativá-lo completamente. Para obter detalhes, consulte Buckets [sem versão, com versionamento ativado e com versionamento suspenso](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```



```

    ],
    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
  },
  {
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
  }
]
}

```

Conceder acesso ao sistema de arquivos aos arquivos no sistema de arquivos do Amazon EFS

Note

Além da política, você também deve garantir que suas permissões de arquivo POSIX estejam concedendo o acesso apropriado. Para obter mais informações, consulte [Working with users, groups, and permissions at the Network File System \(NFS\) Level](#) (Trabalhar com usuários, grupos e permissões no nível do Network File System (NFS)) no Guia do usuário do Amazon Elastic File System.

O exemplo de política a seguir concede ao sistema de arquivos raiz acesso aos arquivos em seu sistema de arquivos do Amazon EFS.

 Note

Nos exemplos a seguir, *region* substitua pela sua região, *account-id* pela conta em que o arquivo está e *file-system-id* pelo ID do seu Amazon Elastic File System (Amazon EFS).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RootFileSystemAccess",
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Resource": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/file-system-id"
    }
  ]
}
```

O exemplo de política a seguir concede ao sistema de arquivos raiz acesso aos arquivos em seu sistema de arquivos do Amazon EFS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UserFileSystemAccess",
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Resource": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/file-system-id"
    }
  ]
}
```

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

Tutoriais do Transfer Family

O guia AWS Transfer Family do usuário fornece orientações detalhadas para vários casos de uso.

- [Introdução aos endpoints de AWS Transfer Family servidor](#)- Crie um servidor SFTP Transfer Family com um usuário gerenciado pelo serviço e transfira arquivos usando um cliente.
- [Configurando e usando conectores SFTP](#)- Configure um conector SFTP para transferir arquivos entre o armazenamento Amazon S3 e um servidor SFTP.
- [Configurando um método Amazon API Gateway como um provedor de identidade personalizado](#)- Configure um método Amazon API Gateway como um provedor de identidade personalizado para carregar arquivos em um AWS Transfer Family servidor.
- [Configurando um fluxo de trabalho gerenciado para descriptografar um arquivo](#)- Crie um fluxo de trabalho gerenciado para descriptografar arquivos, fazer upload de arquivos criptografados para o Amazon S3 e visualizar o conteúdo descriptografado.
- [Configurando uma configuração AS2](#)- Configure um servidor AS2 Transfer Family, incluindo importação de certificados, criação de perfil e contrato, configuração opcional do conector AS2 e testes.
- Os tutoriais a seguir orientam você na criação e configuração dos aplicativos web Transfer Family. Escolha o tutorial que melhor se adapta às suas necessidades:

[Tutorial: Configurando um aplicativo web básico do Transfer Family](#)- Aprenda a criar e configurar um aplicativo web Transfer Family.

[Tutorial: Configurando um aplicativo AWS Transfer Family web com acesso seletivo a vários buckets](#)- Configure um aplicativo web Transfer Family com permissões granulares de bucket do Amazon S3 para um único usuário.

Tópicos

- [Introdução aos endpoints de AWS Transfer Family servidor](#)
- [Configurando um fluxo de trabalho gerenciado para descriptografar um arquivo](#)
- [Configurando e usando conectores SFTP](#)
- [Configurando um método Amazon API Gateway como um provedor de identidade personalizado](#)
- [Configurando uma configuração AS2](#)
- [Tutorial: Configurando um aplicativo web básico do Transfer Family](#)

- [Tutorial: Configurando um aplicativo AWS Transfer Family web com acesso seletivo a vários buckets](#)

Introdução aos endpoints de AWS Transfer Family servidor

Use este tutorial para começar com AWS Transfer Family (Transfer Family). Você aprenderá a criar um SFTP-enabled servidor com endpoint acessível ao público usando o armazenamento Amazon S3, adicionar um usuário com autenticação gerenciada por serviços e transferir um arquivo com o Cyberduck.

Tópicos

- [Pré-requisitos](#)
- [Etapa 1: faça login no AWS Transfer Family console](#)
- [Etapa 2: criar um SFTP-enabled servidor](#)
- [Etapa 3: Adicionar um usuário gerenciado de serviço](#)
- [Etapa 4: Transferir um arquivo usando um cliente](#)

Pré-requisitos

Antes de começar, conclua os requisitos em [Pré-requisitos](#). Como parte dessa configuração, você cria um bucket do Amazon Simple Storage Service (Amazon S3) e AWS Identity and Access Management uma função de usuário (IAM).

Há permissões necessárias para usar o AWS Transfer Family console e há permissões necessárias para configurar outros AWS serviços que a Transfer Family usa, como Amazon Simple Storage Service AWS Certificate Manager, Amazon Elastic File System e Amazon Route 53. Por exemplo, para usuários que estão transferindo arquivos para dentro e para fora do AWS uso do Transfer Family, `AmazonS3FullAccess` concede permissões para configurar e usar um bucket do Amazon S3. Algumas das permissões dessa política são necessárias para criar buckets do Amazon S3.

Para usar o console do Transfer Family, você precisa do seguinte:

- `AWSTransferConsoleFullAccess` concede permissões para que seu usuário do SFTP crie recursos do Transfer Family.
- `IAMFullAccess` (ou, especificamente, uma política que permita a criação de funções do IAM) só é necessária se você quiser que a Transfer Family crie automaticamente uma função de registro

para seu servidor no Amazon CloudWatch Logs ou uma função de usuário para um usuário fazendo login em um servidor.

- Para criar e excluir tipos de servidor VPC, você precisa adicionar as ações `ec2:CreateVpcEndpoint` e `ec2:DeleteVpcEndpoints` à sua política. Para obter informações sobre como limitar o acesso ao VPC endpoint para fins de segurança, consulte [Limitando o acesso ao VPC endpoint para servidores Transfer Family](#)

Note

As `IAMFullAccess` políticas `AmazonS3FullAccess`, por si só, não são necessárias para o uso geral do AWS Transfer Family. Elas são apresentadas aqui como uma forma simples de garantir que todas as permissões necessárias sejam cobertas. Além disso, essas são políticas gerenciadas AWS, que são políticas padrão que estão disponíveis para todos os clientes AWS. É possível visualizar as permissões individuais nessas políticas e determinar um conjunto mínimo necessário para seus propósitos.

Etapa 1: faça login no AWS Transfer Family console

Para entrar no Transfer Family

1. Faça login no Console de gerenciamento da AWS e abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. Para ID da conta ou alias, insira o ID da sua Conta da AWS.
3. Para Nome de usuário do IAM, insira o nome da função de usuário que você criou para o Transfer Family.
4. Em Senha, insira a senha AWS da sua conta.
5. Escolha Logon.

Etapa 2: criar um SFTP-enabled servidor

O File Transfer Protocol (SFTP) do Secure Shell (SSH) é um protocolo de rede usado para transferência segura de dados pela internet. O protocolo suporta toda a funcionalidade de segurança e autenticação do SSH. Ele é amplamente usado para trocar dados, incluindo informações

confidenciais entre parceiros de negócios em diversos setores, como serviços financeiros, saúde, varejo e publicidade.

Para criar um SFTP-enabled servidor

1. Selecione Servidores no painel de Navegação e escolha Criar servidor.
2. Em Escolher protocolos, selecione SFTP e escolha Avançar.
3. Em Escolher um provedor de identidade, escolha Serviço gerenciado para armazenar identidades e chaves no Transfer Family e, em seguida, escolha Avançar.
4. Em Escolha um endpoint, faça o seguinte:
 - a. Em Tipo de endpoint, escolha o tipo de endpoint Acessível publicamente.
 - b. (Opcional) Em Nome de host personalizado, escolha Nenhum.
 - c. Escolha Próximo.
5. Em Escolher um domínio, escolha Amazon S3.
6. Em Configurar detalhes adicionais, para opções de algoritmo criptográfico, escolha uma política de segurança que contenha os algoritmos criptográficos habilitados para uso pelo seu servidor. Nossa política de segurança mais recente é a padrão: para obter detalhes, consulte [Políticas de segurança para AWS Transfer Family servidores](#).

 Note

Somente se você estiver adicionando um fluxo de trabalho gerenciado ao seu servidor, escolha Criar uma nova função para CloudWatchregistro. Para registrar eventos do servidor, você não precisa criar uma função do IAM.

7. Em Revisar e criar, escolha Criar servidor. Você é direcionado para a página Servidores.

Pode levar alguns minutos até que o status de seu novo servidor mude para Online. Nesse ponto, seu servidor pode realizar operações com arquivos, mas primeiro você precisa criar um usuário. Para obter detalhes sobre a criação de usuários, consulte [Gerenciando usuários para endpoints de servidor](#).

Etapa 3: Adicionar um usuário gerenciado de serviço

Para adicionar um usuário ao SFTP-enabled servidor

1. Na página Servidores, selecione o servidor ao qual você deseja adicionar um usuário.
2. Escolha Adicionar usuário.
3. Na seção Configuração do usuário, em Nome de usuário, insira o nome de usuário. Esse nome de usuário deve ter, no mínimo, 3 e, no máximo 100 caracteres. Você pode usar os seguintes caracteres no nome de usuário: a—z, 0—9 A-Z, sublinhado '_', hífen '-', ponto '.' e sinal de arroba '@'. O nome de usuário não pode começar com um hífen '-', ponto '.' ou com o sinal '@'.
4. Para Access, escolha a função do IAM que você criou em [Criar uma política e um perfil do IAM](#). Essa função do IAM inclui uma política do IAM que contém permissões para acessar seu bucket do Amazon S3, bem como uma relação de confiança com o AWS Transfer Family serviço. O procedimento descrito em [Estabelecer um relacionamento de confiança](#) mostra como estabelecer a relação de confiança adequada.
5. Em Política, selecione Nenhum.
6. Para o diretório inicial, escolha o bucket do Amazon S3 em que você deseja armazenar os dados que você transfere usando. AWS Transfer Family Insira o caminho para o home diretório. Esse é o diretório que seus usuários veem quando fazem login usando o cliente.

Recomendamos usar um caminho de diretório que contenha o nome de usuário para que você tenha a opção de usar uma política de sessão. Uma política de sessão limita o acesso de um usuário no bucket do Amazon S3 ao diretório desse usuáriohome. Para obter mais informações sobre o uso de políticas de sessão, consulte [Como funcionam as políticas de sessão](#).

Se preferir, você pode manter esse parâmetro em branco para usar o diretório do bucket do root Amazon S3. Se você escolher essa opção, certifique-se de que sua função do IAM forneça acesso ao root diretório.

7. Marque a caixa de seleção Restrito para impedir que seus usuários acessem qualquer coisa fora do home diretório. Isso também impede que os usuários vejam o nome do bucket ou da pasta do Amazon S3.
8. Para chave pública SSH, insira a parte da chave SSH pública do par de chaves SSH no formato. `ssh-rsa <string>`

Sua chave deve ser validada pelo serviço antes que você possa adicionar seu novo usuário. Para obter mais informações sobre como gerar um par de chaves SSH, consulte [Gere chaves SSH para usuários gerenciados por serviços](#).

9. (Opcional) Em Chave e Valor, insira uma ou mais tags como pares de chave/valor e escolha Adicionar tag.
10. Escolha Adicionar para adicionar o novo usuário ao servidor que você escolheu.

O novo usuário será exibido na seção Usuários da página Detalhes do servidor.

Etapa 4: Transferir um arquivo usando um cliente

Você transfere arquivos pelo AWS Transfer Family serviço especificando a operação de transferência em um cliente. AWS Transfer Family suporta vários clientes. Para obter detalhes, consulte [Transferindo arquivos em um endpoint de servidor usando um cliente](#)

Esta seção contém procedimentos para usar o Cyberduck e o OpenSSH.

Tópicos

- [Usar o Cyberduck](#)
- [Usar OpenSSH](#)

Usar o Cyberduck

Para transferir arquivos AWS Transfer Family usando o Cyberduck

1. Abra o cliente [Cyberduck](#).
2. Escolha Abrir conexão.
3. Na caixa de diálogo Abrir conexão, escolha SFTP (SSH File Transfer Protocol).
4. Para Servidor, insira o endpoint do seu servidor. O endpoint do servidor está localizado na página Detalhes do servidor, consulte [Exibir detalhes do servidor SFTP, FTPS e FTP](#).
5. Em Número da porta, insira **22** para SFTP.
6. Em Nome do usuário, insira o nome do usuário que você criou no [Gerenciando usuários para endpoints de servidor](#).
7. Em Chave privada SSH, escolha a chave privada SSH.
8. Selecione Conectar.

9. Realize a transferência do seu arquivo.

Dependendo de onde estão seus arquivos, siga um destes procedimentos:

- Em seu diretório local (a origem), escolha os arquivos que você deseja transferir e arraste e solte-os no diretório do Amazon S3 (o destino).
- No diretório do Amazon S3 (a origem), escolha os arquivos que você deseja transferir e arraste e solte-os no seu diretório local (o destino).

Usar OpenSSH

Use as instruções a seguir para transferir arquivos a partir da linha de comando usando o OpenSSH.

Note

Esse cliente funciona somente com um SFTP-enabled servidor.

Para transferir arquivos AWS Transfer Family usando o utilitário de linha de comando OpenSSH

1. No Linux ou Macintosh, abra um terminal de comando.
2. No prompt, insira o seguinte comando: `% sftp -i transfer-key sftp_user@service_endpoint`

No comando anterior, `sftp_user` é o nome do usuário e `transfer-key` é a chave privada SSH. Aqui `service_endpoint` está o endpoint do servidor, conforme mostrado no AWS Transfer Family console do servidor selecionado.

Um prompt `sftp` deve ser exibido.

3. (Opcional) Para visualizar o diretório inicial do usuário, digite o seguinte comando no `sftp` prompt: `sftp> pwd`
4. Na próxima linha, insira o seguinte texto: `sftp> cd /amzn-s3-demo-bucket/home/sftp_user`

Neste exercício de conceitos básicos, esse bucket do Amazon S3 é o destino da transferência de arquivos.

5. Na próxima linha, insira o seguinte comando: `sftp> put filename.txt`

O comando `put` transfere o arquivo para o bucket do Amazon S3.

Uma mensagem semelhante à seguinte será exibida, indicando que a transferência de arquivos está em andamento ou concluída.

```
Uploading filename.txt to /amzn-s3-demo-bucket/home/sftp_user/  
filename.txt
```

```
some-file.txt 100% 127 0.1KB/s 00:00
```

Configurando um fluxo de trabalho gerenciado para descriptografar um arquivo

Este tutorial ilustra como configurar um fluxo de trabalho gerenciado que contenha uma etapa de descriptografia. O tutorial também mostra como fazer upload de um arquivo criptografado para um bucket do Amazon S3 e, em seguida, ver o arquivo descriptografado nesse mesmo bucket.

Note

O blog AWS de armazenamento tem uma postagem que descreve como simplesmente descriptografar arquivos sem escrever nenhum código usando fluxos de trabalho do Transfer Family Managed, [criptografar e descriptografar](#) arquivos com PGP e AWS Transfer Family

Tópicos

- [Etapa 1: Configure uma função de execução](#)
- [Etapa 2: Crie um fluxo de trabalho gerenciado](#)
- [Etapa 3: Adicione o fluxo de trabalho a um servidor e crie um usuário](#)
- [Etapa 4: Crie um par de chaves PGP](#)
- [Etapa 5: Armazene a chave privada PGP em AWS Secrets Manager](#)
- [Etapa 6: Criptografe um arquivo](#)
- [Etapa 7: Execute o fluxo de trabalho e visualize os resultados](#)

Etapa 1: Configure uma função de execução

Crie uma função de execução AWS Identity and Access Management (IAM) que a Transfer Family possa usar para iniciar um fluxo de trabalho. O processo de criação de uma função de execução está descrito em [Políticas do IAM para fluxos de trabalho](#).

Note

Como parte da criação de uma função de execução, certifique-se de estabelecer uma relação de confiança entre a função de execução e o Transfer Family, conforme descrito em [Estabelecer um relacionamento de confiança](#).

A política de função de execução a seguir contém todas as permissões necessárias para iniciar o fluxo de trabalho que você cria neste tutorial. Para usar esse exemplo de política, substitua os *user input placeholders* por suas próprias informações. `amzn-s3-demo-bucket` Substitua pelo nome do bucket do Amazon S3 em que você carrega seus arquivos criptografados.

Note

Nem todo fluxo de trabalho exige todas as permissões listadas neste exemplo. Você pode restringir as permissões com base nos tipos de etapas em seu fluxo de trabalho específico. As permissões necessárias para cada tipo de etapa predefinido estão descritas em [Usar etapas predefinidas](#). As permissões necessárias para cada uma etapa personalizada estão descritas em [Permissões do IAM para a etapa de personalizar](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkflowsS3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject",
```

```

        "s3:PutObjectTagging",
        "s3:ListBucket",
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
},
{
    "Sid": "DecryptSecret",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/transfer/*"
}
]
}

```

Etapa 2: Crie um fluxo de trabalho gerenciado

Agora você precisa criar um fluxo de trabalho que contenha uma etapa de descriptografia.

Para criar um fluxo de trabalho que contenha uma etapa de descriptografia

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, escolha Fluxos de trabalho e, em seguida, Criar fluxo de trabalho.
3. Insira os detalhes a seguir:
 - Insira uma descrição, por exemplo **Decrypt workflow example**.
 - Na seção Etapas nominais, escolha Adicionar etapa.
4. Em Escolher tipo de etapa, escolha Descriptografar arquivo e, em seguida, escolha Próximo.
5. Na caixa de diálogo Configurar parâmetros, especifique o seguinte:

- Insira um nome descritivo da etapa, por exemplo, **decrypt-step**. Não são permitidos espaços nos nomes das etapas.
- Em Destino para arquivos descriptografados, escolha Amazon S3.
- Em Nome do bucket de destino, escolha o mesmo bucket do Amazon S3 que você especificou como `amzn-s3-demo-bucket` na política do IAM criado na Etapa 1.
- Em Prefixo de chave de destino, insira o nome do prefixo (pasta) em que você deseja armazenar seus arquivos descriptografados no bucket de destino, por exemplo, **decrypted-files/**.

 Note

Certifique-se de adicionar uma barra final (/) ao seu prefixo.

- Para este tutorial, deixe Substituir existente desmarcado. Quando esta configuração estiver desmarcada, se você tentar descriptografar um arquivo com o mesmo nome de um arquivo existente, o processamento do fluxo de trabalho será interrompido, e o novo arquivo não será processado.

Escolha Próximo para ir para a tela de revisão.

6. Revise os detalhes da etapa. Se tudo estiver correto, escolha Criar etapa.
7. Como seu fluxo de trabalho precisa apenas de uma única etapa de descriptografia, não há etapas adicionais a serem configuradas. Escolha Criar fluxo de trabalho para criar o novo fluxo de trabalho.

Anote a ID do fluxo de trabalho do seu novo fluxo de trabalho. Você precisará dessa ID na próxima etapa. Este tutorial usa `w-1234abcd5678efghi` como exemplo da ID do fluxo de trabalho.

Etapa 3: Adicione o fluxo de trabalho a um servidor e crie um usuário

Agora que você tem um fluxo de trabalho com uma etapa de descriptografia, você deve associá-lo a um servidor do Transfer Family. Este tutorial mostra como anexar o fluxo de trabalho a um servidor do Transfer Family existente. Você também pode criar um novo servidor para usar com seu fluxo de trabalho.

Depois de anexar o fluxo de trabalho a um servidor, você deve criar um usuário que possa usar o SFTP no servidor e acionar a execução do fluxo de trabalho.

Para configurar um servidor do Transfer Family para executar um fluxo de trabalho

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, selecione Servidores e em seguida escolha um servidor da lista. Verifique se esse servidor é compatível com o protocolo SFTP.
3. Na página de detalhes do servidor, role para baixo até a seção Detalhes adicionais e escolha Editar.
4. Na página Editar detalhes adicionais, na seção Fluxos de trabalho gerenciados, escolha seu fluxo de trabalho e escolha uma função de execução correspondente.
 - Em Fluxo de trabalho para carregamentos de arquivos completos, escolha o fluxo de trabalho que você criou em [Etapa 2: Crie um fluxo de trabalho gerenciado](#), por exemplo, **w-1234abcd5678efghi**.
 - Para a função de execução de fluxos de trabalho gerenciados, escolha perfil do IAM que você criou em [Etapa 1: Configure uma função de execução](#).
5. Navegue até a parte inferior da página e escolha Salvar para salvar suas alterações.

Anote a ID do servidor que você está usando. O nome do AWS Secrets Manager segredo que você usa para armazenar suas chaves PGP é baseado em parte na ID do servidor.

Para adicionar um usuário que possa acionar o fluxo de trabalho

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, selecione Servidores e selecione o servidor que você está usando para o fluxo de trabalho de descryptografia.
3. Na página de detalhes do servidor, role para baixo até a seção Usuários e escolha Adicionar usuário.
4. Para seu novo usuário, insira os seguintes detalhes:
 - Em Nome do usuário, insira **decrypt-user**.
 - Em Função, escolha uma função do usuário que possa acessar seu servidor.
 - Para o Diretório inicial, escolha o bucket do Amazon S3 que você usou anteriormente, por exemplo, **amzn-s3-demo-bucket**.
 - Para chaves públicas SSH, cole uma chave pública que corresponda a uma chave privada que você tem. Para obter detalhes, consulte [Gere chaves SSH para usuários gerenciados por serviços](#).

5. Escolha Adicionar para salvar seu novo usuário.

Anote o nome do usuário do Transfer Family para esse servidor. O segredo é parcialmente baseado no nome do usuário. Para simplificar, este tutorial usa um segredo padrão que pode ser usado por qualquer usuário do servidor.

Etapa 4: Crie um par de chaves PGP

Use um dos [clientes PGP compatíveis](#) para gerar um par de chaves PGP. Este processo está descrito em detalhes em [Gerar chaves PGP](#).

Para gerar um par de chaves PGP

1. Neste tutorial, é possível usar o cliente gpg (GnuPG) versão 2.0.22 para gerar um par de chaves PGP que usa RSA como algoritmo de criptografia. Para esse cliente, execute o seguinte comando e forneça um endereço de e-mail e uma senha. É possível usar qualquer nome ou endereço de e-mail que desejar. Lembre-se dos valores que usar, pois você precisará inseri-los posteriormente no tutorial.

```
gpg --gen-key
```

Note

Se você estiver usando o GnuPG versão 2.3.0 ou mais recente, deverá executar `gpg --full-gen-key`. Quando solicitado sobre o tipo de chave a ser criada, escolha RSA ou ECC. Se você escolher ECC, poderá escolher NIST entre BrainPool e Curve25519 para a curva elíptica.

2. Exporte a chave privada executando o seguinte comando. Substitua *user@example.com* pelo endereço de e-mail que você usou quando gerou a chave.

```
gpg --output workflow-tutorial-key.pgp --armor --export-secret-key user@example.com
```

Este comando exporta a chave privada para o arquivo **workflow-tutorial-key.pgp**. É possível nomear o arquivo de saída como quiser. Você também pode excluir o arquivo de chave privada depois de adicioná-lo ao AWS Secrets Manager.

Etapa 5: Armazene a chave privada PGP em AWS Secrets Manager

Você precisa armazenar a chave privada no Secrets Manager de uma forma muito específica para que o fluxo de trabalho possa encontrar a chave privada quando o fluxo de trabalho executar uma etapa de descryptografia em um arquivo carregado.

Note

Quando você armazena segredos no Secrets Manager, você Conta da AWS incorre em cobranças. Para obter mais informações sobre preços consulte [AWS Secrets Manager Pricing](#).

Para armazenar uma chave privada PGP no Secrets Manager

1. Faça login no Console de gerenciamento da AWS e abra o AWS Secrets Manager console em <https://console.aws.amazon.com/secretsmanager/>.
2. No painel de navegação à esquerda, selecione Segredos.
3. Na página Segredos, escolha Armazenar um novo segredo.
4. Na página Escolher tipo de segredo, em Tipo de segredo, escolha Outro tipo de segredo.
5. Na seção Key/value de pares, escolha a Key/valueguia.
 - Chave — Insira **PGPPrivateKey**.
 - valor – cole o texto da sua chave privada no campo de valor.
6. Escolha Adicionar linha e, na seção Key/value de pares, escolha a Key/valueguia.
 - Chave — Insira **PGPPassphrase**.
 - valor – Insira a senha que você usou ao gerar seu par de chaves PGP em [Etapa 4: Crie um par de chaves PGP](#).
7. Escolha Próximo.
8. Na página Configurar segredo, insira um nome e uma descrição para seu segredo. Você pode criar um segredo para um usuário específico ou um que possa ser usado por todos os usuários. Se o ID do seu servidor for **s-11112222333344445**, você nomeia o segredo da seguinte forma.
 - Para criar um segredo padrão para todos os usuários, nomeie o segredo **aws/transfer/s-11112222333344445/@pgp-default**.

- Para criar um segredo somente para o usuário que você criou anteriormente, nomeie o segredo **aws/transfer/s-1111222233344445/decrypt-user**.
9. Escolha Próximo e aceite os padrões na página Configurar alternância. Em seguida, escolha Próximo.
 10. Na página Revisão, escolha Armazenar para criar e armazenar o segredo.

Para obter mais informações sobre como adicionar sua chave privada PGP ao Secrets Manager, consulte [Usar AWS Secrets Manager para armazenar sua chave PGP](#).

Etapa 6: Criptografe um arquivo

Use o programa gpg para criptografar um arquivo para usar em seu fluxo de trabalho. Execute o seguinte comando para criptografar um arquivo:

```
gpg -e -r marymajor@example.com --openpgp testfile.txt
```

Antes de executar este comando, observe o seguinte:

- Para o argumento `-r`, substitua *marymajor@example.com* pelo endereço de e-mail que você usou ao criar o par de chaves PGP.
- O sinalizador `--openpgp` é opcional. Este sinalizador faz com que o arquivo criptografado esteja em conformidade com o padrão [OpenPGP RFC4880](#).
- Este comando cria um arquivo chamado **testfile.txt.gpg** no mesmo local que **testfile.txt**.

Important

Ao criptografar arquivos para uso com AWS Transfer Family fluxos de trabalho, sempre certifique-se de especificar um destinatário não anônimo usando o parâmetro `-r`. A criptografia anônima (sem especificar um destinatário) pode causar falhas de decodificação no fluxo de trabalho porque o sistema não conseguirá identificar qual chave usar para decodificação. As informações de depuração desse problema estão disponíveis em [Solucionar problemas de criptografia de destinatários anônimos](#)

Etapa 7: Execute o fluxo de trabalho e visualize os resultados

Para executar o fluxo de trabalho, você se conecta ao servidor do Transfer Family com o usuário criado na Etapa 3. Em seguida, é possível pesquisar no bucket do Amazon S3 que você especificou na [Etapa 2.5, configurar os parâmetros de destino](#) para ver o arquivo descriptografado.

Para executar o fluxo de trabalho de descriptografia

1. Abra um terminal de comando.
2. Execute o seguinte comando, substituindo *your-endpoint* pelo seu endpoint real e *transfer-key* pela chave privada SSH do seu usuário:

```
sftp -i transfer-key decrypt-user@your-endpoint
```

Por exemplo, se a chave privada estiver armazenada em `~/.ssh/decrypt-user` e seu endpoint for `s-11112222333344445.server.transfer.us-east-2.amazonaws.com`, o comando será o seguinte:

```
sftp -i ~/.ssh/decrypt-user decrypt-user@s-11112222333344445.server.transfer.us-east-2.amazonaws.com
```

3. Execute o comando `pwd`. Se tiver êxito, o comando retornará o seguinte:

```
Remote working directory: /amzn-s3-demo-bucket/decrypt-user
```

Seu diretório reflete o nome do seu bucket do Amazon S3.

4. Execute o seguinte comando para fazer upload do arquivo e acionar o fluxo de trabalho para ser executado:

```
put testfile.txt.gpg
```

5. Como destino dos arquivos descriptografados, você especificou a pasta `decrypted-files/` ao criar o fluxo de trabalho. Agora, é possível navegar até essa pasta e listar o conteúdo.

```
cd ../decrypted-files/  
ls
```

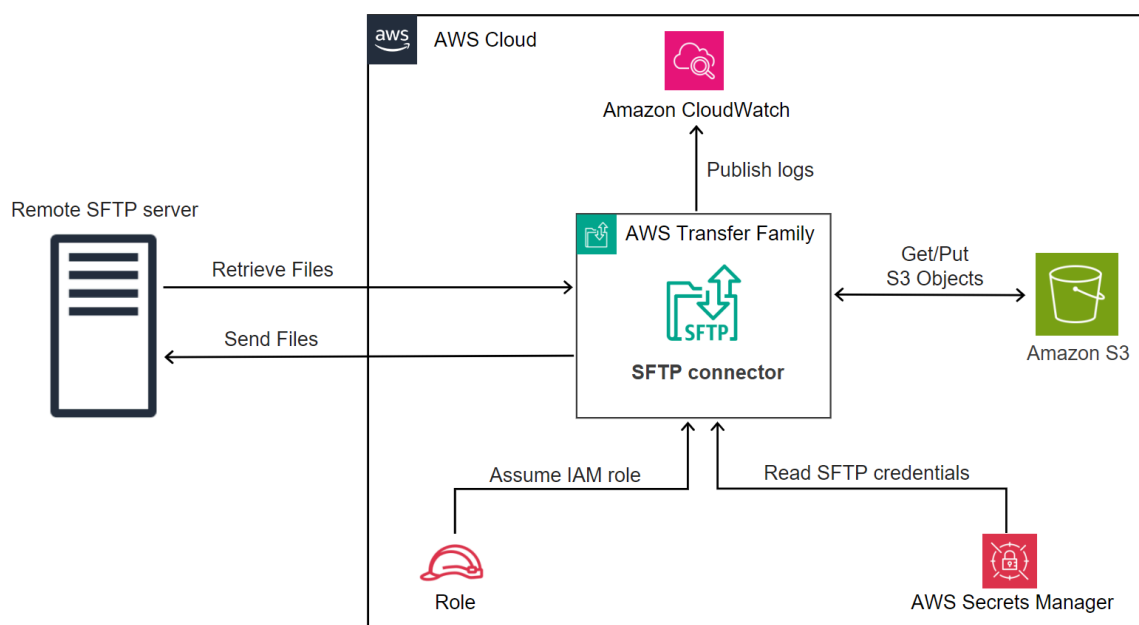
Se for bem-sucedido, o comando `ls` listará o arquivo `testfile.txt`. É possível fazer download desse arquivo e verificar se ele é igual ao arquivo original que você criptografou anteriormente.

Configurando e usando conectores SFTP

O objetivo de um conector é estabelecer uma relação entre seu AWS armazenamento e o servidor SFTP de um parceiro. É possível enviar arquivos do Amazon S3 para um destino externo de propriedade do parceiro. É possível também usar um conector SFTP para recuperar arquivos do servidor SFTP de um parceiro.

Este tutorial ilustra como configurar um conector SFTP com os tipos de saída gerenciado e VPC_LATTICE e, em seguida, transferir arquivos entre o armazenamento do Amazon S3 e um servidor SFTP.

Um conector SFTP recupera as credenciais do SFTP AWS Secrets Manager para se autenticar em um servidor SFTP remoto e estabelecer uma conexão. O conector envia ou recupera arquivos do servidor remoto e armazena os arquivos no Amazon S3. Você pode escolher entre saída gerenciada por serviço (usando infraestrutura AWS gerenciada) ou saída de VPC (roteamento por sua VPC Cross-VPC usando o Resource Access). Uma função do IAM é usada para permitir acesso ao bucket do Amazon S3 e às credenciais armazenadas no Secrets Manager. E você pode fazer login na Amazon CloudWatch.



A postagem de blog a seguir fornece uma arquitetura de referência para criar um fluxo de trabalho de MFT usando conectores SFTP, incluindo criptografia de arquivos usando PGP antes de enviá-los para um servidor SFTP remoto usando conectores SFTP: [Arquitetando transferências de arquivos gerenciadas seguras e compatíveis com conectores SFTP e criptografia PGP](#). AWS Transfer Family

Tipos de saída do conector

Os conectores SFTP oferecem suporte a dois tipos de saída que determinam como seu conector roteia o tráfego para servidores SFTP remotos:

- **SERVICE_MANAGED** (padrão): usa a infraestrutura gerenciada pela AWS Transfer Family com endereços IP estáticos para conexões de saída.
- **VPC**: roteia o tráfego pela sua VPC usando o Cross-VPC Resource Access, permitindo a conectividade privada de endpoints e o uso de seus próprios gateways NAT.

Este tutorial aborda os dois tipos de saída. Escolha o tipo de saída de VPC quando precisar:

- Conecte-se a servidores SFTP privados em sua VPC (endereços IP privados)
- Conecte-se a servidores SFTP locais via Direct Connect ou VPN
- Direcione o tráfego de endpoints públicos por meio de sua VPC para controles de segurança
- Use seus próprios endereços IP elásticos para conexões de saída

Tópicos

- [Etapa 1: criar os recursos de suporte necessários](#)
- [Etapa 2: criar e testar um conector SFTP](#)
- [Etapa 3: Enviar e recuperar arquivos usando o conector SFTP](#)
- [Procedimentos para criar um servidor Transfer Family para usar como seu servidor SFTP remoto](#)

Etapa 1: criar os recursos de suporte necessários

Você pode usar conectores SFTP para copiar arquivos entre o Amazon S3 e qualquer servidor SFTP remoto. Para este tutorial, estamos usando um AWS Transfer Family servidor como nosso servidor SFTP remoto. Precisamos criar e configurar os seguintes recursos:

- Crie buckets Amazon S3 para armazenar arquivos em seu AWS ambiente e para enviar e recuperar arquivos do servidor SFTP remoto: [Crie buckets do Amazon S3](#)

- Crie uma AWS Identity and Access Management função para acessar o armazenamento do Amazon S3 e nosso segredo no Secrets Manager:.. [Crie uma função do IAM com as permissões necessárias](#)
- Crie um servidor Transfer Family que usa o protocolo SFTP, e um usuário gerenciado por serviços que usa o conector SFTP para transferir arquivos de ou para o servidor SFTP:.. [Crie um servidor SFTP Transfer Family e um usuário](#)
- Crie um AWS Secrets Manager segredo que armazene as credenciais usadas pelo conector SFTP para fazer login no servidor SFTP remoto:.. [Crie e armazene um segredo em AWS Secrets Manager](#)

Para conectores do tipo de saída VPC, você também precisa de:

- Uma VPC com sub-redes e grupos de segurança apropriados
- Um gateway de recursos (são necessárias no mínimo 2 zonas de disponibilidade):[Crie um gateway de recursos \(somente tipo de saída de VPC\)](#).
- Uma configuração de recursos apontando para seu servidor SFTP:[Crie uma configuração de recursos \(somente tipo de saída de VPC\)](#). Consulte mais informações em [Resource configurations](#) no Guia do usuário da Amazon VPC Lattice.

Crie buckets do Amazon S3

Como criar um bucket do Amazon S3

1. Faça login no AWS Transfer Family console em <https://console.aws.amazon.com/s3/>.
2. Escolha uma região e insira um nome.

Para este tutorial, nosso bucket está dentro **US East (N. Virginia) us-east-1** e o nome é **sftp-server-storage-east**.

3. Aceite os padrões e escolha Create bucket.

Para obter detalhes completos sobre a criação de buckets do Amazon S3, consulte [Como faço para criar um bucket S3?](#) no Guia do usuário do Amazon Simple Storage Service.

Crie uma função do IAM com as permissões necessárias

Para a função de acesso, crie uma política com as seguintes permissões.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

Substitua os itens da seguinte forma:

- Para `amzn-s3-demo-bucket`, o tutorial usa **`sftp-server-storage-east`**.
- Para **`region`**, o tutorial usa **`us-east-1`**.
- Para **`account-id`**, use seu Conta da AWS ID.
- Pois **`SecretName-6RandomCharacters`**, somos a **`using sftp-connector1`** favor do nome (você terá seus próprios seis caracteres aleatórios para seu segredo).

Você também deve garantir que essa função contenha uma relação de confiança que permita que o conector acesse seus recursos ao atender às solicitações de transferência de seus usuários. Para obter informações sobre como estabelecer um relacionamento de confiança, consulte [Estabelecer um relacionamento de confiança](#).

 Note

Para ver os detalhes da função que estamos usando no tutorial, consulte [Função combinada de usuário e acesso](#).

Crie e armazene um segredo em AWS Secrets Manager

Precisamos armazenar um segredo no Secrets Manager para armazenar as credenciais do usuário para seu conector SFTP. Você pode usar uma senha, chave privada SSH ou ambas. Para o tutorial, estamos usando uma chave privada.

 Note

Quando você armazena segredos no Secrets Manager, você Conta da AWS incorre em cobranças. Para obter mais informações sobre preços consulte [AWS Secrets Manager Pricing](#).

Antes de iniciar o procedimento para armazenar o segredo, recupere e formate sua chave privada. A chave privada deve corresponder à chave pública configurada para o usuário no servidor SFTP remoto. Para nosso tutorial, a chave privada deve corresponder à chave pública armazenada para nosso usuário de teste no servidor SFTP Transfer Family que estamos usando como servidor remoto.

Para fazer isso, execute o seguinte comando:

```
jq -sR . path-to-private-key-file
```

Por exemplo, se seu arquivo de chave privada estiver localizado em `~/ .ssh/sftp-testuser-privatekey`, o comando será o seguinte.

```
jq -sR . ~/ .ssh/sftp-testuser-privatekey
```

Isso gera a chave no formato correto (com caracteres de nova linha incorporados) na saída padrão. Copie esse texto em algum lugar, pois você precisa colá-lo no procedimento a seguir (na etapa 6).

É possível usar o Secrets Manager para armazenar as credenciais do usuário para um conector SFTP.

1. Faça login no Console de gerenciamento da AWS e abra o AWS Secrets Manager console em <https://console.aws.amazon.com/secretsmanager/>.
2. No painel de navegação à esquerda, selecione Segredos.
3. Na página Segredos, escolha Armazenar um novo segredo.
4. Na página Escolher tipo de segredo, em Tipo de segredo, escolha Outro tipo de segredo.
5. Na seção Key/value de pares, escolha a Key/valueguia.
 - Chave — Enter **Username**.
 - valor — Insira o nome do nosso usuário, **sftp-testuser**.
6. Para inserir a chave, recomendamos que você use a guia Texto simples.
 - a. Escolha Adicionar linha e, em seguida, insira **PrivateKey**.
 - b. Escolha a guia Texto simples. O campo agora contém o seguinte texto:

```
{"Username":"sftp-testuser","PrivateKey":""}
```

- c. Cole o texto da sua chave privada (salvo anteriormente) entre aspas duplas vazias ("").

Sua tela deve ter a seguinte aparência (os dados principais estão esmaecidos).



7. Escolha Próximo.
8. Na página Configurar segredo, insira um nome para seu segredo. Neste tutorial, nomeamos o segredo **aws/transfer/sftp-connector1**.
9. Escolha Próximo e aceite os padrões na página Configurar alternância. Em seguida, escolha Próximo.
10. Na página Revisão, escolha Armazenar para criar e armazenar o segredo.

Crie um gateway de recursos (somente tipo de saída de VPC)

Para conectores do tipo de saída VPC, você precisa criar um Resource Gateway em sua VPC. O Resource Gateway serve como ponto de entrada para o acesso aos Cross-VPC recursos.

Para criar um Resource Gateway

1. Execute o comando a seguir para criar um Resource Gateway (substitua o ID da VPC e os IDs da sub-rede pelos seus valores):

```
aws vpc-lattice create-resource-gateway \
  --name my-sftp-resource-gateway \
  --vpc-identifier vpc-12345678 \
  --subnet-ids subnet-12345678 subnet-87654321
```

 Note

Os gateways de recursos exigem sub-redes em pelo menos duas zonas de disponibilidade.

2. Anote o ID do Resource Gateway da resposta para uso na próxima etapa.

Crie uma configuração de recursos (somente tipo de saída de VPC)

Crie uma configuração de recursos que aponte para seu servidor SFTP. Isso pode ser um endereço IP privado para servidores em sua VPC ou um nome DNS público para servidores externos. Para obter mais informações sobre configurações de recursos, consulte Configurações de [recursos no Guia do usuário](#) do Amazon VPC Lattice.

Para criar uma configuração de recursos

1. Para um servidor SFTP privado, execute:

```
aws vpc-lattice create-resource-configuration \  
  --name my-sftp-resource-config \  
  --port-ranges 22 \  
  --type SINGLE \  
  --resource-gateway-identifier rgw-12345678 \  
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"}
```

2. Para um servidor SFTP público (somente nome DNS), execute:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-sftp-resource-config \  
  --port-ranges 22 \  
  --type SINGLE \  
  --resource-gateway-identifier rgw-12345678 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"}
```

 Note

Os endpoints públicos devem usar nomes DNS, não endereços IP.

3. Observe o ARN de configuração de recursos da resposta para uso ao criar o conector.

Etapa 2: criar e testar um conector SFTP

Nesta seção, criamos um conector SFTP que usa todos os recursos que criamos anteriormente. Consulte mais detalhes em [Criação de conectores SFTP](#).

Para criar um conector SFTP

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, escolha Conectores SFTP e, em seguida, escolha Criar conector SFTP.
3. Para Tipo de saída, escolha uma das seguintes opções:
 - Serviço gerenciado (padrão): usa a infraestrutura gerenciada pela AWS Transfer Family com endereços IP estáticos para conexões de saída.
 - VPC Lattice: roteia o tráfego pela sua VPC usando o Resource Access. Cross-VPC Escolha essa opção para conectividade de endpoint privado ou para usar seus próprios gateways NAT.

Important

Você não pode alterar o tipo de saída depois de criar o conector. Escolha com cuidado com base em seus requisitos de conectividade.

4. Na seção Configuração do conector, forneça as seguintes informações:
 - Para o URL, insira o URL do servidor SFTP remoto. Para o tutorial, inserimos a URL do servidor Transfer Family que estamos usando como servidor SFTP remoto.

```
sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
```

1111aaaa2222bbbb3 Substitua pelo ID do servidor Transfer Family.

- Para a função Access, insira a função que criamos anteriormente, **sftp-connector-role**.
- Para ARN de configuração de recursos (somente tipo de saída de rede VPC), insira o ARN da configuração de recursos que você criou anteriormente:

```
arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/rcfg-12345678
```

- Para a função Logging, escolha uma função que inclua uma política de confiança `transfer.amazonaws.com` no elemento Principal.

Dica: Além de adicionar a Transfer Family como uma entidade confiável, você pode adicionar a política `AWSTransferLoggingAccess` AWS gerenciada à função. Essa política é descrita detalhadamente em [AWSTransferLoggingAccess](#).

Connector configuration

Egress type [Info](#)
Choose your SFTP connector's egress type: either directly over public internet, or via your VPC environment

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

URL
Enter the URL of remote server to which you need to connect using the SFTP connector

URL of the remote (target) SFTP server

Access role [Info](#)
IAM Role for Amazon S3 access and AWS Secrets Manager access

Logging role - optional [Info](#)
IAM role for the connector to push events to your CloudWatch logs

5. No painel Configuração do SFTP, forneça as seguintes informações:

- Para credenciais do Connector, escolha o nome do seu recurso do Secrets Manager que contém as credenciais SFTP. Para o tutorial, escolha `aws/transfer/sftp-connector1`.
- Para chaves de host confiáveis, cole na parte pública da chave de host. Você pode recuperar essa chave executando `ssh-keyscan` para o seu servidor SFTP. Para obter detalhes sobre como formatar e armazenar a chave de host confiável, consulte a documentação do tipo de [SftpConnectorConfig](#) dados.
- Em Máximo de conexões simultâneas, selecione um valor inteiro de 1 a 5: o valor padrão é 5.

SFTP configuration [Info](#)

Connector credentials [Info](#)
 Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server

Trusted host keys - optional [Info](#)
 Enter the public portion of the host key(s) that is used to identify the remote server you need to connect to. You can enter the trusted host key(s) now, or add them after creating the connector by using the host key information returned by the TestConnection action.

Connections to the remote server are established only if it's SSH fingerprint matches one of the provided trusted host key(s).

Maximum concurrent connections [Info](#)
 Select the maximum number of concurrent connections that your connector can create to the remote server

- Depois de confirmar todas as configurações, escolha Criar conector para criar o conector SFTP.

Você também pode criar conectores usando o AWS Command Line Interface

- Para criar um conector SFTP com saída gerenciada pelo serviço, execute o seguinte comando:

```
aws transfer create-connector \
  --url "sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-
rsa AAAAB3NzaC..."
```

- Para criar um conector SFTP com VPC-based saída, execute o seguinte comando:

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-rsa
AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn="arn:aws:vpc-lattice:us-
east-1:account-id:resourceconfiguration/rcfg-12345678",PortNumber=22}
```

Depois de criar um conector SFTP, recomendamos que você o teste antes de tentar transferir qualquer arquivo usando o novo conector.

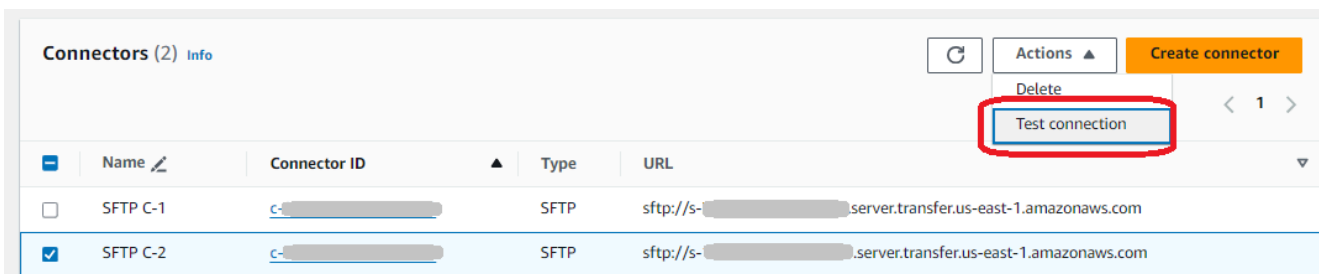
Note

Para conectores do tipo de saída VPC, a resolução do DNS pode levar alguns minutos após a criação. Durante esse período, o status do conector será PENDING e TestConnection retornará “Conector não disponível”. Aguarde até que o status se torne ACTIVE antes de tentar transferir arquivos.

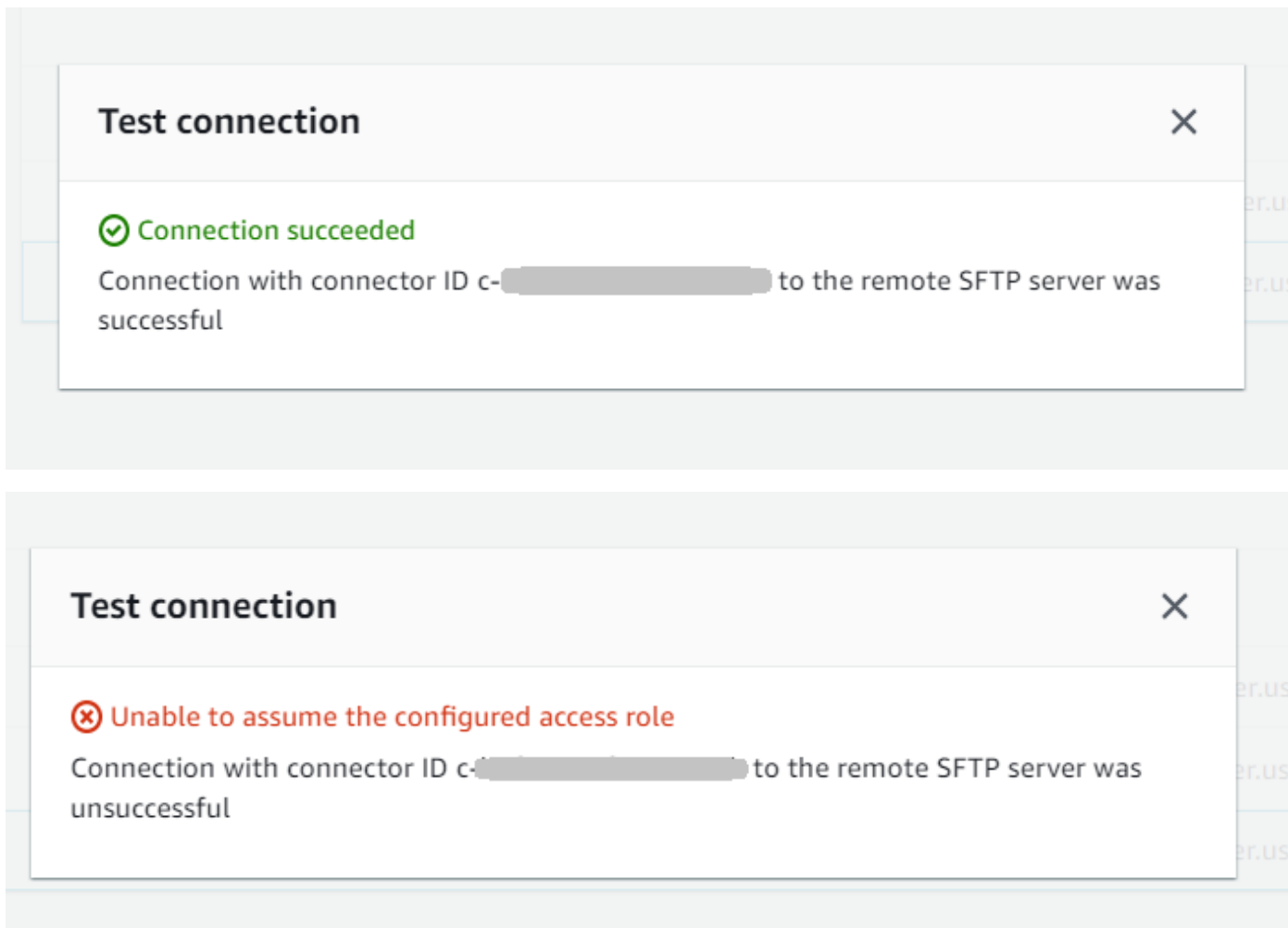
Test a connector using the console

Para testar um conector SFTP

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, escolha Conectores SFTP e selecione um conector.
3. No menu Ações, selecione Testar conexões.



O sistema retorna uma mensagem indicando se o teste foi aprovado ou reprovado. Se o teste falhar, o sistema enviará uma mensagem de erro com base no motivo pelo qual o teste falhou.



Test a connector using the CLI

Para testar um conector usando o AWS Command Line Interface, execute o seguinte comando em um prompt de comando (*connector-id* substitua pelo ID real do conector):

```
aws transfer test-connection --connector-id c-connector-id
```

Se o teste for bem-sucedido, as seguintes linhas serão retornadas:

```
{
  "Status": "OK",
  "StatusMessage": "Connection succeeded"
}
```

Se o teste não for bem-sucedido, você receberá uma mensagem de erro descritiva, por exemplo:

```
{
```



```

    "Status": "ERROR",
    "StatusMessage": "Unable to assume the configured access role"
  }

```

Quando você descreve um conector do tipo de saída VPC, a resposta inclui os novos campos:

```

{
  "Connector": {
    "AccessRole": "arn:aws:iam::219573224423:role/sftp-connector-role",
    "Arn": "arn:aws:transfer:us-east-1:219573224423:connector/c-5dfa309ccabf40759",
    "ConnectorId": "c-5dfa309ccabf40759",
    "Status": "ACTIVE",
    "EgressConfig": {
      "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:025066256552:resourceconfiguration/rcfg-079259b27a357a190"
    },
    "EgressType": "VPC",
    "ServiceManagedEgressIpAddresses": null,
    "SftpConfig": {
      "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
      "UserSecretId": "aws/transfer/sftp-connector1"
    },
    "Url": "sftp://my.sftp.server.com:22"
  }
}

```

Observe que isso `ServiceManagedEgressIpAddresses` é nulo para conectores do tipo de saída de VPC, pois o tráfego é roteado por sua VPC em vez da infraestrutura gerenciada. AWS

Etapa 3: Enviar e recuperar arquivos usando o conector SFTP

Para simplificar, presumimos que você já tenha arquivos em seu bucket do Amazon S3.

Note

O tutorial está usando buckets do Amazon S3 para locais de armazenamento de origem e destino. Se o seu servidor SFTP não usa o armazenamento Amazon S3, onde quer que você `sftp-server-storage-east` veja os comandos a seguir, você pode substituir o caminho por um caminho para locais de arquivos acessíveis a partir do seu servidor SFTP.

- Enviamos um arquivo chamado `SEND-to-SERVER.txt` do armazenamento Amazon S3 para o servidor SFTP.
- Recuperamos um arquivo chamado `RETRIEVE-to-S3.txt` do servidor SFTP para o armazenamento Amazon S3.

Note

Nos comandos a seguir, *connector-id* substitua pelo ID do conector.

Primeiro, enviamos um arquivo do nosso bucket Amazon S3 para o servidor SFTP remoto. Em um prompt de comando, execute o seguinte comando:

```
aws transfer start-file-transfer --connector-id c-connector-id --send-file-paths "/sftp-server-storage-east/SEND-to-SERVER.txt" /--remote-directory-path "/sftp-server-storage-east/incoming"
```

Seu `sftp-server-storage-east` balde agora deve ficar assim.

Amazon S3 > Buckets > sftp-server-storage-east > incoming/

incoming/ Copy S3 URI

Objects | Properties

Objects (1) [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Refresh
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder

Upload

Find objects by prefix

☐	Name	Type	Last modified	Size	Storage class
☐	SEND-to-SERVER.txt	txt	December 18, 2023, 10:36:40 (UTC-05:00)	4.1 KB	Standard

Se você não vê o arquivo conforme o esperado, verifique seus CloudWatch registros.

Para verificar seus CloudWatch registros

1. Abra o CloudWatch console da Amazon em <https://console.aws.amazon.com/cloudwatch/>
2. Selecione Grupos de registros no menu de navegação à esquerda.
3. Insira o ID do conector na barra de pesquisa para encontrar seus registros.
4. Selecione o fluxo de log que é retornado da pesquisa.
5. Expanda a entrada de registro mais recente.

Se for bem-sucedida, a entrada do registro terá a seguinte aparência:

```
{
  "operation": "SEND",
  "timestamp": "2023-12-18T15:26:57.346283Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/sftp-server-storage-east/SEND-to-SERVER.txt",
  "status-code": "COMPLETED",
  "start-time": "2023-12-18T15:26:56.915864Z",
  "end-time": "2023-12-18T15:26:57.298122Z",
  "account-id": "account-id",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
  "remote-directory-path": "/sftp-server-storage-east/incoming"
}
```

Se a transferência do arquivo falhar, a entrada do registro conterá uma mensagem de erro que especifica o problema. As causas comuns de erros são problemas com as permissões do IAM e caminhos de arquivo incorretos.

Em seguida, recuperamos um arquivo do servidor SFTP em um bucket do Amazon S3. Em um prompt de comando, execute o seguinte comando:

```
aws transfer start-file-transfer --connector-id c-connector-id --retrieve-file-paths
"/sftp-server-storage-east/RETRIEVE-to-S3.txt" --local-directory-path "/sftp-server-
storage-east/incoming"
```

Se a transferência for bem-sucedida, seu bucket do Amazon S3 conterá o arquivo transferido, conforme mostrado aqui.

Amazon S3 > Buckets > sftp-server-storage-east > incoming/

incoming/

[Copy S3 URI](#)

Objects | Properties

Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

[Refresh](#)
[Copy S3 URI](#)
[Copy URL](#)
[Download](#)
[Open](#)
[Delete](#)
[Actions](#)
[Create folder](#)

[Upload](#)

Find objects by prefix

☐	Name	Type	Last modified	Size	Storage class
☐	RETRIEVE-to-S3.txt	txt	December 18, 2023, 10:26:58 (UTC-05:00)	4.1 KB	Standard

Se for bem-sucedida, a entrada do registro terá a seguinte aparência:

```
{
  "operation": "RETRIEVE",
  "timestamp": "2023-12-18T15:36:40.017800Z",
  "connector-id": "c-connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://s-server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/sftp-server-storage-east/RETRIEVE-to-S3.txt",
  "status-code": "COMPLETED",
  "start-time": "2023-12-18T15:36:39.727626Z",
  "end-time": "2023-12-18T15:36:39.895726Z",
  "account-id": "account-id",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/c-connector-id",
  "local-directory-path": "/sftp-server-storage-east/incoming"
}
```

Solução de problemas de conectores do tipo de saída VPC

Se você estiver enfrentando problemas com conectores do tipo de saída VPC, verifique o seguinte:

- O status do conector é PENDENTE: a resolução de DNS para conectores VPC pode levar vários minutos. Aguarde até que o status fique ATIVO antes de tentar as conexões.
- Tempos limite de conexão: verifique se os grupos de segurança permitem tráfego na porta 22 entre as sub-redes do Resource Gateway e o servidor SFTP de destino.
- Erros de configuração de recursos: certifique-se de que sua configuração de recursos aponte para o endereço IP ou nome DNS correto e que o Resource Gateway esteja na mesma VPC que seu servidor SFTP (para endpoints privados). Consulte mais informações em [Resource configurations](#) no Guia do usuário da Amazon VPC Lattice.
- Problemas de endpoints públicos: para endpoints públicos, verifique se você está usando um nome DNS, não um endereço IP, em sua configuração de recursos. Verifique se sua VPC tem um gateway NAT para acesso externo à Internet.
- Disponibilidade de AZ: os Resource Gateways exigem sub-redes em pelo menos duas zonas de disponibilidade. Nem todas as AZs oferecem suporte ao VPC Lattice. Verifique as AZs compatíveis em sua região.

Considerações de custo para o tipo de saída de VPC:

- O VPC Lattice cobra \$0. 006/GB para processamento de dados como provedor de recursos (cobrado diretamente pela VPC Lattice)
- AWS Transfer Family absorve os \$0. 01/GB custos do consumidor de recursos (primeiro 1 PB)
- Para endpoints públicos via VPC, taxas adicionais de NAT Gateway e transferência de dados podem ser aplicadas
- Nenhuma cobrança adicional da Transfer Family além do padrão de \$0. 40/GB taxa de processamento de dados

Procedimentos para criar um servidor Transfer Family para usar como seu servidor SFTP remoto

A seguir, descrevemos as etapas para criar um servidor Transfer Family que sirva como seu servidor SFTP remoto para este tutorial. Observe o seguinte:

- Usamos um servidor Transfer Family para representar um servidor SFTP remoto. Os usuários típicos do conector SFTP têm seu próprio servidor SFTP remoto. Consulte [Crie um servidor SFTP Transfer Family e um usuário](#).

- Como estamos usando um servidor Transfer Family, também estamos usando um usuário de SFTP gerenciado pelo serviço. E, para simplificar, combinamos as permissões que esse usuário precisa para acessar o servidor Transfer Family com as permissões necessárias para usar nosso conector. Novamente, a maioria dos casos de uso do conector SFTP tem um usuário SFTP separado que não está associado a um servidor Transfer Family. Consulte [Crie um servidor SFTP Transfer Family e um usuário](#).
- Para o tutorial, como estamos usando o armazenamento Amazon S3 para nosso servidor SFTP remoto, precisamos criar um segundo bucket, **sftp-server-storage-east**, para que possamos transferir arquivos de um bucket para outro.

Crie um servidor SFTP Transfer Family e um usuário

A maioria dos usuários não precisará criar um servidor SFTP Transfer Family e um usuário, pois você já tem um servidor SFTP com usuários e pode usar esse servidor para transferir arquivos de e para. No entanto, para este tutorial, para simplificar, estamos usando um servidor Transfer Family para funcionar como o servidor SFTP remoto.

Siga o procedimento descrito em [Crie um SFTP-enabled servidor](#) para criar um servidor e [Etapa 3: Adicionar um usuário gerenciado de serviço](#) adicionar um usuário. Estes são os detalhes do usuário que estamos usando para o tutorial:

- Crie seu usuário gerenciado por serviços, `sftp-testuser`
 - Defina o diretório inicial como `/sftp-server-storage-east/sftp-testuser`
 - Ao criar o usuário, você armazena uma chave pública. Posteriormente, ao criar o segredo no Secrets Manager, você precisará fornecer a chave privada correspondente.
- Função: `sftp-connector-role`. Para o tutorial, estamos usando a mesma função do IAM para nosso usuário SFTP e para acessar o conector SFTP. Ao criar conectores para sua organização, você pode ter funções de usuário e de acesso separadas.
- Chave do host do servidor: você precisa usar a chave do host do servidor ao criar o conector. Você pode recuperar essa chave executando `ssh-keyscan` para o seu servidor. Por exemplo, se o ID do servidor for `s-1111aaaa2222bbbb3` e o endpoint estiver dentro de `us-east-1`, o comando a seguir recuperará a chave do host do servidor:

```
ssh-keyscan s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
```

Copie esse texto em algum lugar, pois você precisa colá-lo no [Etapa 2: criar e testar um conector SFTP](#) procedimento.

Função combinada de usuário e acesso

Para o tutorial, estamos usando uma única função combinada. Usamos essa função tanto para nosso usuário SFTP quanto para acessar o conector. O exemplo a seguir contém os detalhes dessa função, caso você queira realizar as tarefas do tutorial.

O exemplo a seguir concede as permissões necessárias para acessar nossos dois buckets no Amazon S3 e o segredo `aws/transfer/sftp-connector1` chamado armazenado no Secrets Manager. Para o tutorial, essa função é nomeada `sftp-connector-role`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::sftp-server-storage-east",
        "arn:aws:s3:::sftp-server-storage-east"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ]
    }
  ]
}
```

```

    "Resource": [
      "arn:aws:s3:::sftp-server-storage-east/*",
      "arn:aws:s3:::sftp-server-storage-east/*"
    ],
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-east-1:111122223333:secret:aws/transfer/sftp-connector1-6RandomCharacters"
    }
  ]
}

```

Para obter detalhes completos sobre a criação de funções para Transfer Family, siga o procedimento descrito em [Criação de um perfil de usuário](#) Para criar uma função.

Configurando um método Amazon API Gateway como um provedor de identidade personalizado

Este tutorial ilustra como configurar um método do Amazon API Gateway e usá-lo como um provedor de identidade personalizado para carregar arquivos em um AWS Transfer Family servidor. Este tutorial usa o [Modelo de pilha básica](#) e outras funcionalidades básicas apenas como exemplo.

Tópicos

- [Pré-requisitos](#)
- [Etapa 1: criar uma CloudFormation pilha](#)
- [Etapa 2: Conferir a configuração do método do API Gateway para seu servidor](#)
- [Etapa 3: Visualizar os detalhes do servidor do Transfer Family](#)
- [Etapa 4: Testar se o usuário consegue se conectar ao servidor](#)
- [Etapa 5: Testar a conexão SFTP e a transferência de arquivos](#)
- [Etapa 6: Limitar o acesso ao bucket](#)
- [Atualize o Lambda se estiver usando o Amazon EFS](#)

Pré-requisitos

Antes de criar os recursos do Transfer Family em CloudFormation, crie seu armazenamento e sua função de usuário.

Para especificar o armazenamento e criar uma função de usuário

1. Dependendo do armazenamento que você está usando, consulte a seguinte documentação:
 - Para criar um bucket do Amazon S3, consulte [Como criar um bucket do S3?](#) no Guia do usuário do console do Amazon Simple Storage Service.
 - Para criar um sistema de arquivos Amazon EFS, consulte [Configurar um sistema de arquivos Amazon EFS](#).
2. Para criar uma função de usuário, consulte [Criar uma política e um perfil do IAM](#).

Você insere os detalhes do seu armazenamento e da sua função de usuário ao criar sua pilha CloudFormation na próxima seção.

Etapa 1: criar uma CloudFormation pilha

Para criar uma AWS CloudFormation pilha a partir do modelo fornecido

1. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. Selecione Criar pilha e depois Com novos recursos (padrão).
3. No painel Pré-requisito - Preparar modelo, escolha Escolher um modelo existente.
4. Copie este link, [Modelo básico de pilha](#), e cole-o no campo URL do Amazon S3.
5. Clique em Next.
6. Especifique os parâmetros, incluindo um nome para sua pilha. Não deixe de fazer o seguinte:
 - Substitua os valores padrão por UserNameUserPassworde.
 - Para UserHomeDirectory, insira os detalhes do armazenamento (um bucket do Amazon S3 ou um sistema de arquivos do Amazon EFS) que você criou anteriormente.
 - Substitua o padrão UserRoleArnpela função de usuário que você criou anteriormente. A função AWS Identity and Access Management (IAM) deve ter as permissões apropriadas. Para obter um exemplo de perfil do IAM e política de bucket, consulte [Etapa 6: Limitar o acesso ao bucket](#).

- Se você quiser se autenticar usando uma chave pública em vez de uma senha, insira sua chave pública no UserPublicKey1 campo. A primeira vez que você se conectar ao servidor usando SFTP, fornecerá a chave privada, em vez da senha.
7. Escolha Avançar e então Avançar outra vez na página Configurar opções de pilha.
 8. Revise os detalhes da pilha que você está criando e escolha Criar pilha.

 Note

Na parte inferior da página, em Capacidades, reconheça que CloudFormation pode criar recursos do IAM.

Etapa 2: Conferir a configuração do método do API Gateway para seu servidor

 Note

Para melhorar a segurança, é possível configurar um firewall para aplicações Web. O AWS WAF é um firewall para aplicações Web que permite monitorar as solicitações HTTP e HTTPS que são encaminhadas ao Amazon API Gateway. Para obter detalhes, consulte [Adicione um firewall da aplicação web](#).

 Não habilite o armazenamento em cache do API Gateway

Não habilite o armazenamento em cache para seu método API Gateway ao usá-lo como um provedor de identidade personalizado para Transfer Family. O armazenamento em cache é impróprio e inválido para solicitações de autenticação porque:

- Cada solicitação de autenticação é exclusiva e requer uma resposta ativa, não uma resposta em cache
- O armazenamento em cache não oferece benefícios, pois o Transfer Family nunca envia solicitações duplicadas ou repetidas para o API Gateway.
- A ativação do armazenamento em cache fará com que o API Gateway responda com dados incompatíveis, resultando em respostas inválidas às solicitações de autenticação

Para verificar a configuração do método do API Gateway para seu servidor e implantá-lo.

1. Abra o console do API Gateway em <https://console.aws.amazon.com/apigateway/>.
2. Escolha a API de modelo básico do Transfer Custom Identity Provider que o CloudFormation modelo gerou.
3. No painel Recursos, selecione / e, em seguida, escolha Solicitação de método.
4. Escolha Ações e Implantar API. Para o Estágio de implantação, escolha prod e Implantar.

Depois que o método API Gateway for implantado com sucesso, veja seu desempenho na seção Editor de estágio.

 Note

Copie o endereço do URL de invocação exibido na parte superior da página. Você precisará dele para a próxima etapa.

Etapa 3: Visualizar os detalhes do servidor do Transfer Family

Quando você usa o modelo para criar uma CloudFormation pilha, um servidor Transfer Family é criado automaticamente.

Para visualizar os detalhes do servidor do Transfer Family

1. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. Escolha a pilha que você criou.
3. Escolha a guia Recursos.

Resources (18)			
Search resources			
Logical ID ▲	Physical ID ▼	Type ▼	
ApiCloudWatchLogsRole	-ApiCloudWatchLogsRole-	AWS::IAM::Role	
ApiDeployment202008		AWS::ApiGateway::Deployment	
ApiLoggingAccount		AWS::ApiGateway::Account	
ApiStage	prod	AWS::ApiGateway::Stage	
CloudWatchLoggingRole	-CloudWatchLoggingRole-	AWS::IAM::Role	
CustomIdentityProviderApi		AWS::ApiGateway::RestApi	
GetUserConfigLambda	-GetUserConfigLambda-	AWS::Lambda::Function	
GetUserConfigLambdaPermission	GetUserConfigLambdaPermission-	AWS::Lambda::Permission	
GetUserConfigRequest		AWS::ApiGateway::Method	
GetUserConfigResource		AWS::ApiGateway::Resource	
GetUserConfigResponseModel	UserConfigResponseModel	AWS::ApiGateway::Model	
LambdaExecutionRole	-LambdaExecutionRole-	AWS::IAM::Role	
ServerIdResource		AWS::ApiGateway::Resource	
ServersResource		AWS::ApiGateway::Resource	
TransferIdentityProviderRole	-TransferIdentityProviderRole-	AWS::IAM::Role	
TransferServer	arn:aws:transfer:us-east-2:::server/s-	AWS::Transfer::Server	
UserNameResource		AWS::ApiGateway::Resource	
UsersResource		AWS::ApiGateway::Resource	

O ARN do servidor é mostrado na coluna ID física da TransferServer linha. O ID do servidor está contido no ARN, por exemplo, s-11112222333344445.

- Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>, na página Servidores, escolha o novo servidor.

O ID do servidor corresponde ao ID exibido para o TransferServer recurso em CloudFormation.

Etapa 4: Testar se o usuário consegue se conectar ao servidor

Para testar se o usuário consegue se conectar ao servidor usando o console Transfer Family

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. Na página Servidores, escolha seu novo servidor, escolha Ações e escolha Testar.
3. Insira o texto das suas credenciais de login no campo Nome de usuário e no campo Senha. Esses são os valores que você definiu ao implantar a CloudFormation pilha.
4. Em Protocolo do servidor, selecione SFTP e, em IP de origem, insira **127.0.0.1**.
5. Escolha Testar.

Se a autenticação do usuário for bem-sucedida, o teste retornará uma resposta HTML `Status Code: 200` e um objeto JSON contendo os detalhes das funções e permissões do usuário. Por exemplo:

```
{
  "Response": "{\\"Role\\": \\"arn:aws:iam::123456789012:role/my-user-role\\",
  \\"HomeDirectory\\": \\"/${transfer:HomeBucket}/\\"}",
  "StatusCode": 200,
  "Message": "",
  "Url": "https://1a2b3c4d5e.execute-api.us-east-2.amazonaws.com/prod/servers/s-1234abcd5678efgh0/users/myuser/config"
}
```

Se o teste falhar, adicione uma das políticas AWS gerenciadas do API Gateway à função que você está usando para sua API.

Etapa 5: Testar a conexão SFTP e a transferência de arquivos

Para testar a conexão SFTP

1. Em um dispositivo Linux ou Macintosh, abra um terminal de comando.
2. Digite um dos comandos a seguir, dependendo se você está usando uma senha ou um par de chaves para autenticação.
 - Se você estiver usando uma senha, digite este comando:

```
sftp -o PubkeyAuthentication=no myuser@server-ID.server.transfer.region-code.amazonaws.com
```

Insira sua senha quando for solicitado.

- Se você estiver usando um par chave, digite este comando:

```
sftp -i private-key-file myuser@server-ID.server.transfer.region-code.amazonaws.com
```

Note

Para estes comandos `sftp`, insira o código para a Região da AWS onde seu servidor Transfer Family está localizado. Por exemplo, se seu servidor estiver no Leste dos EUA (Ohio), insira **us-east-2**.

3. No prompt `sftp>`, verifique se é possível fazer upload (put), baixar (get) e visualizar diretórios e arquivos (`pwd` e `ls`).

Etapa 6: Limitar o acesso ao bucket

É possível limitar quem pode acessar um bucket específico do Amazon S3. O exemplo a seguir mostra as configurações a serem usadas em sua CloudFormation pilha e na política que você seleciona para seu usuário.

Neste exemplo, definimos os seguintes parâmetros para a CloudFormation pilha:

- `CreateServer`: `true`
- `UserHomeDirectory`: `/amzn-s3-demo-bucket1`
- `UserName`: `myuser`
- `UserPassword`: `MySuperSecretPassword`

Important

Este é um exemplo de senha. Ao configurar seu método do API Gateway, insira uma senha forte.

- UserPublicKey1: *your-public-key*
- UserRoleArn: arn:aws:iam::*role-id*:role/myuser-api-gateway-role

UserPublicKey1 É uma chave pública que você gerou como parte de um par de public/private chaves.

O *role-id* é único para a função de usuário que você criar. A política do myuser-api-gateway-role a seguir é anexada ao:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectAcl",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    }
  ]
}
```

Para se conectar ao servidor usando SFTP, digite um dos comandos a seguir no prompt.

- Se você estiver usando um par de chaves para autenticação, execute este comando:

```
sftp -o PubkeyAuthentication=no myuser@transfer-server-  
ID.server.transfer.region-id.amazonaws.com
```

Insira sua senha quando for solicitado.

- Se você estiver usando um par chave para autenticação, execute este comando:

```
sftp -i private-key-file myuser@transfer-server-ID.server.transfer.region-id.amazonaws.com
```

Note

Para esses sftp comandos, use o ID de Região da AWS onde seu servidor Transfer Family está localizado. Por exemplo, se seu servidor estiver no Leste dos EUA (Ohio), use us-east-2.

No prompt sftp, você é direcionado ao seu diretório inicial, que pode ser visualizado executando o comando pwd. Por exemplo:

```
sftp> pwd
Remote working directory: /amzn-s3-demo-bucket1
```

O usuário não pode visualizar nenhum diretório acima do diretório inicial. Por exemplo:

```
sftp> pwd
Remote working directory: /amzn-s3-demo-bucket1
sftp> cd ..
sftp> ls
Couldn't read directory: Permission denied
```

Atualize o Lambda se estiver usando o Amazon EFS

Se você selecionou o Amazon EFS como opção de armazenamento para seu servidor do Transfer Family, edite a função do Lambda para sua pilha.

Para adicionar um perfil Posix à sua função Lambda

1. Abra o console Lambda em <https://console.aws.amazon.com/lambda/>
2. Escolha a função do Lambda que você criou anteriormente. A função Lambda tem o formato de ***stack-name***- GetUserConfigLambda - ***lambda-identifier***, onde ***stack-name*** é o nome da CloudFormation pilha e ***lambda-identifier*** é o identificador da função.

3. Na guia Código, selecione `index.js` para exibir o código da função.
4. No response, adicione a seguinte linha entre `Policy` e `HomeDirectory`:

```
PosixProfile: {"Uid": uid-value, "Gid": gid-value},
```

Onde *uid-value* e *gid-value* são números inteiros, 0 ou maiores, que representam a ID do usuário e a ID do grupo, respectivamente.

Por exemplo, depois de adicionar o perfil Posix, o campo de resposta pode ficar assim:

```
response = {  
  Role: 'arn:aws:iam::123456789012:role/api-gateway-transfer-efs-role', // The  
  user will be authenticated if and only if the Role field is not blank  
  Policy: '', // Optional JSON blob to further restrict this user's permissions  
  PosixProfile: {"Gid": 65534, "Uid": 65534},  
  HomeDirectory: '/fs-fab2c234' // Not required, defaults to '/'  
};
```

Configurando uma configuração AS2

Este tutorial explica como definir uma configuração do Applicability Statement 2 (AS2) com AWS Transfer Family. Depois de concluir as etapas descritas aqui, você terá um AS2-enabled servidor pronto para aceitar mensagens AS2 de um parceiro comercial de amostra. Você também terá um conector que pode ser usado para enviar mensagens AS2 para o parceiro comercial de amostra.

Note

Algumas partes do exemplo de configuração usam o AWS Command Line Interface (AWS CLI). Se você ainda não instalou o AWS CLI, consulte [Instalando ou atualizando a versão mais recente do AWS CLI](#) no Guia do AWS Command Line Interface Usuário.

1. Crie certificados para você e seu parceiro comercial. Se você tiver certificados existentes que possa usar, pode ignorar esta seção.

Esse processo é descrito em [Etapa 1: Criar os certificados para AS2](#).

2. Importe os certificados que você criou na etapa 1.

Esse processo é descrito em [Etapa 2: Importar certificados como recursos de certificados do Transfer Family](#).

3. Para configurar seus parceiros comerciais, crie um perfil local e um perfil de parceiro.

Esse processo é descrito em [Etapa 3: Crie perfis para você e seu parceiro comercial](#).

4. Crie um AWS Transfer Family servidor que use o protocolo AS2. Opcionalmente, você pode adicionar um endereço IP elástico ao servidor para torná-lo voltado para a Internet.

Esse processo é descrito em [Etapa 4: Criar um servidor Transfer Family que usa o protocolo AS2](#).

 Note

Você deve criar um servidor Transfer Family somente para transferências de entrada. Se você estiver realizando apenas transferências de saída, não precisará de um servidor Transfer Family.

5. Crie um acordo entre você e seu parceiro comercial.

Esse processo é descrito em [Etapa 5: criar um acordo entre você e seu parceiro](#).

 Note

Você deve criar um contrato somente para transferências de entrada. Se você estiver realizando apenas transferências externas, não precisará de um contrato.

6. Crie um conector entre você e seu parceiro comercial.

Esse processo é descrito em [Etapa 6: criar um conector entre você e seu parceiro](#).

 Note

Você deve criar um conector somente para transferências externas. Se você estiver realizando somente transferências de entrada, você não precisará de um conector.

7. Teste uma troca de arquivos AS2.

Esse processo é descrito em [Etapa 7: Teste a troca de arquivos pelo AS2 usando Transfer Family](#).

Depois de concluir essas etapas, você poderá fazer o seguinte:

- Envie arquivos para um servidor AS2-enabled parceiro remoto com o comando `Transfer Family start-file-transfer` AWS Command Line Interface (AWS CLI).
- Receba arquivos de um servidor AS2-enabled parceiro remoto na porta 5080 por meio de seu endpoint de nuvem privada virtual (VPC).

Etapa 1: Criar os certificados para AS2

Ambas as partes em uma troca AS2 precisam de X.509 certificados. Você pode criar esses certificados da maneira que quiser. Este tópico descreve como usar o [OpenSSL](#) na linha de comando para criar um certificado raiz e, em seguida, assinar certificados subordinados. Ambas as partes devem gerar seus próprios certificados.

Note

O comprimento da chave para certificados AS2 deve ser de pelo menos 2.048 bits e no máximo 4.096.

Para transferir arquivos com um parceiro, observe o seguinte:

- Você pode anexar certificados aos perfis. Os certificados contêm chaves públicas ou privadas.
- Seu parceiro comercial envia suas chaves públicas e você envia as suas.
- Seu parceiro comercial criptografa as mensagens com sua chave pública e as assina com a chave privada. Por outro lado, você criptografa as mensagens com a chave pública do seu parceiro e as assina com sua chave privada.

Note

Se você preferir gerenciar chaves com uma GUI, [Portecle](#) é uma opção que você pode usar.

Para gerar exemplos de certificados

Important

Não envie suas chaves privadas ao seu parceiro. Neste exemplo, você gera um conjunto de chaves públicas e privadas autoassinadas para uma parte. Se você pretende atuar como ambos parceiros comerciais para fins de teste, pode repetir essas instruções para gerar dois conjuntos de chaves: um para cada parceiro comercial. Nesse caso, você não precisa gerar duas autoridades de certificação raiz (CAs).

1. Execute o comando a seguir para gerar uma chave RSA privada com um módulo de 2048 bits.

```
/usr/bin/openssl genrsa -out root-ca-key.pem 2048
```

2. Execute o comando a seguir para criar um certificado autoassinado com seu arquivo `root-ca-key.pem`.

```
/usr/bin/openssl req \  
-x509 -new -nodes -sha256 \  
-days 1825 \  
-subj "/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=R00TCA" \  
-key root-ca-key.pem \  
-out root-ca.pem
```

O argumento `-subj` consiste nos seguintes valores.

	Name (Nome)	Description
C	Código do país	Um código de duas letras para o país em que sua organização está localizada.
ST	Estado, região ou província	O Estado, região ou província em que sua organização está localizada. (Nesse caso, a região não

	Name (Nome)	Description
		se refere à sua Região da AWS.)
L	Nome da localidade	A cidade em que sua organização está localizada.
O	Nome da organização	O nome legal completo da sua organização, incluindo sufixos, como LLC, Corp e assim por diante.
OU	Nome da unidade organizacional	A divisão da sua organização que lida com esse certificado.
CN	Nome comum ou nome de domínio totalmente qualificado (FQDN)	Nesse caso, estamos criando um certificado raiz, então o valor é ROOTCA. Nesses exemplos, estamos usando CN para descrever a finalidade do certificado.

3. Crie uma chave de assinatura e uma chave de criptografia para seu perfil local.

```
/usr/bin/openssl genrsa -out signing-key.pem 2048
/usr/bin/openssl genrsa -out encryption-key.pem 2048
```

Note

Alguns AS2-enabled servidores, como o OpenAS2, exigem que você use o mesmo certificado para assinatura e criptografia. Nesse caso, você pode importar a mesma chave privada e certificado para ambas as finalidades. Para fazer isso, execute este comando em vez dos comandos anteriores:

```
/usr/bin/openssl genrsa -out signing-and-encryption-key.pem 2048
```

4. Execute os comandos a seguir para criar solicitações de assinatura de certificado (CSRs) para a chave raiz assinar.

```
/usr/bin/openssl req -new -key signing-key.pem -subj \  
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Signer" -out signing-  
key-csr.pem
```

```
/usr/bin/openssl req -new -key encryption-key.pem -subj \  
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Encrypter" -out  
encryption-key-csr.pem
```

5. Em seguida, você deve criar um arquivo `signing-cert.conf` e um arquivo `encryption-cert.conf`.

- Use um editor de texto para criar o arquivo `signing-cert.conf` com o seguinte conteúdo:

```
authorityKeyIdentifier=keyid,issuer  
keyUsage = digitalSignature, nonRepudiation
```

- Use um editor de texto para criar o arquivo `encryption-cert.conf` com o seguinte conteúdo:

```
authorityKeyIdentifier=keyid,issuer  
keyUsage = dataEncipherment
```

6. Finalmente, você cria os certificados assinados executando os comandos a seguir.

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in signing-key-  
csr.pem -out signing-cert.pem -CA \  
root-ca.pem -CAkey root-ca-key.pem -extfile signing-cert.conf
```

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in encryption-key-  
csr.pem -out encryption-cert.pem \  
-CA root-ca.pem -CAkey root-ca-key.pem -extfile encryption-cert.conf
```

Etapa 2: Importar certificados como recursos de certificados do Transfer Family

Este procedimento explica como importar certificados usando o AWS CLI. Se você quiser usar o console Transfer Family em vez disso, consulte [the section called “Importar certificados AS2”](#).

Para importar os certificados de assinatura e criptografia que você criou na etapa 1, execute os comandos `import-certificate` a seguir. Se você estiver usando o mesmo certificado para criptografia e assinatura, importe o mesmo certificado duas vezes (uma vez com o uso `SIGNING` e novamente com o uso `ENCRYPTION`).

Note

Se você tiver um arquivo que contenha um certificado e sua cadeia, poderá fornecer esse arquivo ao `import-certificate` comando usando somente o `certificate` parâmetro. Por exemplo:

```
aws transfer import-certificate --usage ENCRYPTION --certificate  
file://combined-cert-and-chain-file.pem
```

Se você usar o `certificate` parâmetro para carregar o certificado e sua cadeia, não use o `certificate-chain` parâmetro.

Se você combinar o certificado e sua cadeia, sua chave será formatada usando os padrões PEM convencionais, que incluem uma nova linha “\n” a cada 64 caracteres. O certificado armazenado é funcionalmente equivalente ao que você carregou, com a única diferença de que a `DescribeCertificate` resposta por meio do AWS CLI conterá esses caracteres de nova linha.

```
aws transfer import-certificate --usage SIGNING --certificate file://signing-cert.pem \  
--private-key file://signing-key.pem --certificate-chain file://root-ca.pem
```

Esse comando retorna sua assinatura `CertificateId`. Na próxima seção, esse ID de certificado é chamado de *my-signing-cert-id*.

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://encryption-  
cert.pem \  

```

```
--private-key file://encryption-key.pem --certificate-chain file://root-ca.pem
```

Esse comando retorna sua criptografia CertificateId. Na próxima seção, esse ID de certificado é chamado de *my-encrypt-cert-id*.

Em seguida, importe os certificados de criptografia e assinatura do seu parceiro executando os comandos a seguir.

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://partner-encryption-cert.pem \  
--certificate-chain file://partner-root-ca.pem
```

Esse comando retorna a criptografia do seu parceiro CertificateId. Na próxima seção, esse ID de certificado é chamado de *partner-encrypt-cert-id*.

```
aws transfer import-certificate --usage SIGNING --certificate file://partner-signing-cert.pem \  
--certificate-chain file://partner-root-ca.pem
```

Esse comando retorna a assinatura do seu parceiro CertificateId. Na próxima seção, esse ID de certificado é chamado de *partner-signing-cert-id*.

Etapa 3: Crie perfis para você e seu parceiro comercial

Este procedimento explica como criar perfis AS2 usando o AWS CLI. Se você quiser usar o console Transfer Family em vez disso, consulte [the section called “Crie perfis AS2”](#).

Crie seu perfil AS2 local executando o comando a seguir. Esse comando faz referência aos certificados que contêm suas chaves públicas e privadas.

```
aws transfer create-profile --as2-id MYCORP --profile-type LOCAL --certificate-ids \  
my-signing-cert-id my-encrypt-cert-id
```

Esse comando retorna o ID do seu perfil. Na próxima seção, esse ID é chamado de *my-profile-id*.

Agora crie o perfil do parceiro executando o comando a seguir. Esse comando usa somente os certificados de chave pública do seu parceiro. Para usar esse comando, substitua o *user input*

placeholders por suas próprias informações; por exemplo, o nome AS2 e os IDs do certificado do seu parceiro.

```
aws transfer create-profile --as2-id PARTNER-COMPANY --profile-type PARTNER --  
certificate-ids \  
partner-signing-cert-id partner-encrypt-cert-id
```

Esse comando retorna o ID do perfil do seu parceiro. Na próxima seção, esse ID é chamado de *partner-profile-id*.

Note

Nos comandos anteriores, *MYCORP* substitua pelo nome da sua organização e *PARTNER-COMPANY* pelo nome da organização do seu parceiro comercial.

Etapa 4: Criar um servidor Transfer Family que usa o protocolo AS2

Este procedimento explica como criar um AS2-enabled servidor usando o Transfer Family AWS CLI.

Note

Muitas das etapas de exemplo usam comandos que carregam parâmetros de um arquivo. Para obter mais detalhes sobre o uso de arquivos para carregar parâmetros, consulte [Como carregar parâmetros de um arquivo](#).

Se você quiser usar o em vez disso, consulte [Crie um servidor AS2 usando o console Transfer Family](#).

Da mesma forma que você cria um AWS Transfer Family servidor SFTP ou FTPS, você cria um AS2-enabled servidor usando o `--protocols AS2` parâmetro do `create-server` AWS CLI comando. Atualmente, o Transfer Family oferece suporte somente aos tipos de endpoint da VPC e ao armazenamento Amazon S3 com o protocolo AS2.

Quando você cria seu AS2-enabled servidor para Transfer Family usando o `create-server` comando, um VPC endpoint é criado automaticamente para você. Esse endpoint expõe a porta TCP 5080 para que possa aceitar mensagens AS2.

Se você quiser expor seu endpoint da VPC publicamente à Internet, você pode associar endereços IP elásticos ao seu endpoint da VPC.

Para usar essas instruções, você precisa do seguinte:

- O ID da sua VPC (por exemplo, vpc-abcdef01).
- Os IDs das suas sub-subredes VPC (por exemplo, subnet-abcdef01, subnet-subnet-abcdef01, subnet-021345ab).
- Um ou mais IDs dos grupos de segurança que permitem tráfego de entrada na porta TCP 5080 de seus parceiros comerciais (por exemplo, sg-1234567890abcdef0 e sg-abcdef01234567890).
- (Opcional) Os endereços IP elásticos que você deseja associar ao seu endpoint da VPC.
- Se seu parceiro comercial não estiver conectado à sua VPC por meio de uma VPN, você precisará de um gateway da internet. Para obter mais informações, consulte [Estabelecer conexão com a Internet usando um gateway da Internet](#) no Guia do usuário da Amazon VPC.

Para criar um AS2-enabled servidor

1. Execute o comando a seguir. Substitua cada *user input placeholder* por suas próprias informações.

```
aws transfer create-server --endpoint-type VPC \
--endpoint-details VpcId=vpc-abcdef01,SubnetIds=subnet-abcdef01,subnet-
abcdef01,subnet-
021345ab,SecurityGroupIds=sg-abcdef01234567890,sg-1234567890abcdef0 --protocols AS2
\
--protocol-details As2Transports=HTTP
```

2. (Opcional) Você pode tornar o endpoint da VPC público. Você pode anexar endereços IP elásticos a um servidor Transfer Family somente por meio de uma operação update-server. Os comandos a seguir param o servidor, o atualizam com endereços IP elásticos e o iniciam novamente.

```
aws transfer stop-server --server-id your-server-id
```

```
aws transfer update-server --server-id your-server-id --endpoint-details \
AddressAllocationIds=eipalloc-abcdef01234567890,eipalloc-
1234567890abcdef0,eipalloc-abcd012345cccccc
```

```
aws transfer start-server --server-id your-server-id
```

Esse comando `start-server` cria automaticamente um registro DNS para você que contém o endereço IP público do seu servidor. Para dar acesso ao servidor ao seu parceiro comercial, você fornece as seguintes informações. Nesse caso, *your-region* refere-se ao seu Região da AWS.

s-your-server-id.server.transfer.*your-region*.amazonaws.com

O URL completo que você fornece ao seu parceiro comercial é o seguinte:

`http://s-your-server-id.server.transfer.your-region.amazonaws.com:5080`

3. Para testar se seu AS2-enabled servidor está acessível, use os comandos a seguir. Certifique-se de que seu servidor possa ser acessado por meio do endereço DNS privado do seu endpoint da VPC ou por meio de seu endpoint público (se você associou um endereço IP elástico ao seu endpoint).

Se o servidor estiver configurado corretamente, a conexão será bem-sucedida. No entanto, você receberá uma resposta do código de status HTTP 400 (Solicitação inválida) porque não está enviando uma mensagem AS2 válida.

- Para um endpoint público (se você associou um endereço IP elástico na etapa anterior), execute o comando a seguir, substituindo o ID do servidor e a região.

```
curl -vv -X POST http://s-your-server-id.transfer.your-region.amazonaws.com:5080
```

- Se você estiver se conectando à sua VPC, consulte o nome DNS privado do seu endpoint da VPC executando os comandos a seguir.

```
aws transfer describe-server --server-id s-your-server-id
```

Esse `describe-server` comando retorna o ID do seu endpoint da VPC no parâmetro `VpcEndpointId`. Use esse valor para executar o comando a seguir.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-your-vpc-endpoint-id
```

Esse comando `describe-vpc-endpoints` retorna uma matriz `DNSEntries`, com vários parâmetros `DnsName`. Use o nome DNS regional (aquele que não inclui a Zona de Disponibilidade) no comando a seguir.

```
curl -vv -X POST http://vpce-your-vpce.vpce-svc-your-vpce-svc.your-region.vpce.amazonaws.com:5080
```

Por exemplo, o comando a seguir mostra valores de amostra para os espaços reservados no comando anterior.

```
curl -vv -X POST http://vpce-0123456789abcdefg-fghij123.vpce-svc-11111aaaa2222bbbb.us-east-1.vpce.amazonaws.com:5080
```

4. (Opcional) Configure uma função `delog`. O Transfer Family registra o status das mensagens enviadas e recebidas em um formato JSON estruturado nos CloudWatch registros da Amazon. Para fornecer à Transfer Family acesso aos CloudWatch registros em sua conta, você deve configurar uma função de registro em seu servidor.

Crie uma função AWS Identity and Access Management (IAM) confiável e `transfer.amazonaws.com` anexe a política `AWSTransferLoggingAccess` gerenciada. Para obter detalhes, consulte [Criar uma política e um perfil do IAM](#). Observe o nome do recurso da Amazon (ARN) do perfil do IAM da Amazon que você acabou de criar junto a este servidor executando o comando `update-server` a seguir:

```
aws transfer update-server --server-id your-server-id --logging-role arn:aws:iam::your-account-id:role/logging-role-name
```

Note

Embora a função de log seja opcional, é altamente recomendável configurá-la para que você possa ver o status de suas mensagens e solucionar problemas de configuração.

Etapa 5: criar um acordo entre você e seu parceiro

Este procedimento explica como criar contratos AS2 usando o AWS CLI. Se você quiser usar o console Transfer Family em vez disso, consulte [the section called “Crie um contrato AS2”](#).

Os acordos reúnem os dois perfis (local e parceiro), seus certificados e uma configuração de servidor que permite transferências AS2 de entrada entre duas partes. Você pode listar seus itens executando os comandos a seguir.

```
aws transfer list-profiles --profile-type LOCAL
aws transfer list-profiles --profile-type PARTNER
aws transfer list-servers
```

Essa etapa requer um bucket do Amazon S3 e uma função do IAM com read/write acesso de e para o bucket. As instruções para criar essa função são as mesmas dos protocolos SFTP, FTP e FTPS da Transfer Family e estão disponíveis em [Criar uma política e um perfil do IAM](#).

Para criar um contrato, você precisa dos seguintes itens:

- O nome do bucket do Amazon S3 (e o prefixo do objeto, se especificado) para armazenar seus arquivos AS2. Recomendamos que você especifique diretórios separados para diferentes tipos de arquivo.
- O ARN do perfil do IAM com acesso ao bucket
- Seu ID do servidor Transfer Family
- Seu ID do perfil e o ID do perfil do seu parceiro

Salve o código a seguir em um arquivo, por exemplo, `agreementDetails.json`. Substitua cada *user input placeholder* por suas próprias informações.

```
{
  "Description": "ExampleAgreementName",
  "ServerId": "your-server-id",
  "LocalProfileId": "your-profile-id",
  "PartnerProfileId": "your-partner-profile-id",
  "AccessRole": "arn:aws:iam::111111111111:role/TransferAS2AccessRole",
  "Status": "ACTIVE",
  "PreserveFilename": "ENABLED",
  "EnforceMessageSigning": "ENABLED",
  "CustomDirectories": {
    "FailedFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-failed",
    "MdnFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-mdn",
    "PayloadFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-payload",
    "StatusFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-status",
    "TemporaryFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-temp"
  }
}
```

```
}
```

Note

Para usar um único diretório base em vez de diretórios separados, remova a `CustomDirectories` linha e suas linhas de diretório individuais do código anterior e, em vez disso, use o seguinte parâmetro:

```
"BaseDirectory": "/amzn-s3-demo-destination-bucket/AS2-inbox"
```

Não use um diretório base e parâmetros de diretório separados, ou o comando falhará.

Em seguida, execute o comando a seguir.

```
aws transfer create-agreement --cli-input-json file://agreementDetails.json
```

Se o comando for bem-sucedido, a ID do contrato será retornada. Você pode então exibir os detalhes do contrato com o comando a seguir.

```
aws transfer describe-agreement --agreement-id agreement-id --server-id your-server-id
```

Etapa 6: criar um conector entre você e seu parceiro

Este procedimento explica como criar conectores AS2 usando o AWS CLI. Se você quiser usar o console Transfer Family em vez disso, consulte [the section called “Configurar conectores AS2”](#).

Você pode usar a operação de API `StartFileTransfer` para enviar arquivos armazenados no Amazon S3 para o endpoint AS2 do seu parceiro comercial usando um conector. Você pode encontrar os perfis que você criou anteriormente executando o comando a seguir.

```
aws transfer list-profiles
```

Ao criar o conector, você deve fornecer a URL do servidor AS2 do seu parceiro. Copie o texto a seguir em um arquivo denominado `testAS2Config.json`.

```
{  
  "Compression": "ZLIB",  
  "EncryptionAlgorithm": "AES256_CBC",  
  "LocalProfileId": "your-profile-id",
```

```
"MdnResponse": "SYNC",
"MdnSigningAlgorithm": "DEFAULT",
"MessageSubject": "Your Message Subject",
"PartnerProfileId": "partner-profile-id",
"PreserveContentType": "FALSE",
"SigningAlgorithm": "SHA256"
}
```

Note

PoisEncryptionAlgorithm, não especifique o DES_EDE3_CBC algoritmo, a menos que você precise oferecer suporte a um cliente antigo que o exija, pois é um algoritmo de criptografia fraco.

Em seguida, execute o seguinte comando para criar o conector.

```
aws transfer create-connector --url "http://partner-as2-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/AWSTransferLoggingAccess
\
--as2-config file:///path/to/testAS2Config.json
```

Etapa 7: Teste a troca de arquivos pelo AS2 usando Transfer Family

Receba um arquivo do seu parceiro comercial

Se você associou um endereço IP elástico público ao seu endpoint da VPC, a Transfer Family criou automaticamente um nome DNS que contém seu endereço IP público. O subdomínio é o ID AWS Transfer Family do seu servidor (do formato-1234567890abcdef0). Forneça a URL do seu servidor ao seu parceiro comercial no formato a seguir.

```
http://s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com:5080
```

Se você não associou um endereço IP elástico público ao seu endpoint da VPC, procure o nome do host do endpoint da VPC que pode aceitar mensagens AS2 via HTTP POST de seus parceiros comerciais na porta 5080. Para recuperar os detalhes do endpoint da VPC, use o comando a seguir.

```
aws transfer describe-server --server-id s-1234567890abcdef0
```

Por exemplo, suponha que o comando anterior retorne um ID de endpoint da VPC de. `vpce-1234abcd5678efghi`. Então, você usaria o comando a seguir para recuperar os nomes do DNS.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1234abcd5678efghi
```

Esse comando retorna todos os detalhes do endpoint da VPC necessários para executar o comando a seguir.

O nome DNS está listado na matriz `DnsEntries`. Seu parceiro comercial deve estar em sua VPC para acessar seu endpoint da VPC (por exemplo, por meio de AWS PrivateLink ou de uma VPN). Forneça o URL do seu endpoint da VPC ao seu parceiro no formato a seguir.

```
http://vpce-your-vpce-id.vpce-svc-your-vpce-svc-id.your-region.vpce.amazonaws.com:5080
```

Por exemplo, o URL a seguir mostra exemplos de valores para os espaços reservados nos comandos anteriores.

```
http://vpce-0123456789abcdefg-fghij123.vpce-svc-11111aaaa2222bbbb.us-east-1.vpce.amazonaws.com:5080
```

Neste exemplo, as transferências bem-sucedidas são armazenadas no local especificado no parâmetro `base-directory` que você especificou em [Etapa 5: criar um acordo entre você e seu parceiro](#). Se recebermos com sucesso os arquivos chamados `myfile1.txt` e `myfile2.txt`, os arquivos serão armazenados como `/path-defined-in-the-agreement/processed/original_filename.messageId.original_extension`. Aqui, os arquivos são armazenados como `/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile1.messageId.txt` e `/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile2.messageId.txt`.

Se você configurou uma função de registro ao criar seu servidor Transfer Family, também poderá verificar seus CloudWatch registros quanto ao status das mensagens AS2.

Envie um arquivo para seu parceiro comercial

Você pode usar o Transfer Family para enviar mensagens AS2 referenciando o ID do conector e os caminhos para os arquivos, conforme ilustrado no seguinte comando `start-file-transfer` AWS Command Line Interface (AWS CLI):


```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \  
--send-file-paths "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-source-  
bucket/myfile2.txt"
```

Para obter detalhes dos conectores, execute o seguinte comando:

```
aws transfer list-connectors
```

O comando `list-connectors` retorna os IDs do conector, os URLs e nomes do recurso da Amazon (ARNs) dos seus conectores.

Para retornar as propriedades de um conector específico, execute o comando a seguir com o ID que você deseja usar:

```
aws transfer describe-connector --connector-id your-connector-id
```

O comando `describe-connector` retorna todas as propriedades do conector, incluindo URL, funções, perfis, avisos de disposição de mensagens (MDNs), tags e métricas de monitoramento.

Você pode confirmar que o parceiro recebeu os arquivos com êxito visualizando os arquivos JSON e MDN. Esses arquivos são nomeados de acordo com as convenções descritas em [Nomes e localizações dos arquivos](#). Se você configurou uma função de registro ao criar o conector, também poderá verificar seus CloudWatch registros quanto ao status das mensagens AS2.

Tutorial: Configurando um aplicativo web básico do Transfer Family

Este tutorial explica como configurar um aplicativo web Transfer Family. Os aplicativos web Transfer Family permitem uma interface simples para transferir dados de e para o Amazon S3 por meio de um navegador da web. Para obter a documentação detalhada desse recurso, consulte [Aplicativos web Transfer Family](#).

Tutorial de aplicativos web: pré-requisitos

- Crie uma instância de conta ou uma instância de organização do Centro de Identidade do AWS IAM. Para obter detalhes, consulte [Configure seu provedor de identidade para os aplicativos web Transfer Family](#).

Se você não estiver usando o IAM Identity Center como seu provedor de identidade, [Integre o Okta como seu provedor de identidade para aplicativos da web](#) ilustra como usar um provedor de identidade alternativo (neste caso, Okta).

- Você precisa de um bucket Amazon S3 para interagir com seu aplicativo web Transfer Family. Para obter detalhes, consulte [Configurar um bucket do Amazon S3](#)

Note

Este tutorial pressupõe que você esteja usando o diretório do IAM Identity Center para seu provedor de identidade. Se esse não for o caso, consulte [Configure seu provedor de identidade para os aplicativos web Transfer Family](#) antes de continuar com este tutorial.

Depois de concluir o tutorial, seu usuário pode fazer login e interagir com o aplicativo web que você criou.

Etapa 1: criar os recursos de suporte necessários

Você precisa adicionar um usuário ao seu diretório do IAM Identity Center. Você também precisa de duas funções: uma para usar como portador de identidade para seu aplicativo web e uma segunda para configurar uma concessão de acesso ao Amazon S3. Para o tutorial, permitimos que AWS os serviços criem essas funções para nós.

Para adicionar um usuário

1. Faça login no Console de gerenciamento da AWS e abra o Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. No painel de navegação esquerdo, escolha Usuários.
3. Escolha Adicionar usuário e especifique os detalhes do usuário.

Especifique um nome de usuário, endereço de e-mail e outras informações necessárias. Você pode optar por enviar um e-mail ao usuário com instruções para configurar sua senha ou gerar uma senha de uso único para compartilhar com ele.

4. Escolha Avançar e, opcionalmente, atribua o novo usuário a um ou mais grupos.
5. Escolha Avançar e revise suas escolhas.

Se tudo estiver correto, escolha Adicionar usuário para criar o novo usuário com os detalhes que você especificou.

Para o tutorial, o usuário de exemplo é Bob Stiles, nome de usuário bobstiles e endereço de e-mail bobstiles@example.com.

Etapa 2: criar um aplicativo web Transfer Family

Para criar um aplicativo web Transfer Family

1. Faça login no Console de gerenciamento da AWS e abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, escolha Aplicativos Web.
3. Escolha Criar aplicativo web.

Para acesso à autenticação, observe que o serviço encontra automaticamente a Centro de Identidade do AWS IAM instância que você configurou como pré-requisito.

4. No painel Tipo de permissão, selecione Criar e usar uma nova função de serviço. O serviço cria a função de portador de identidade para você. Uma função de portador de identidade inclui a identidade de um usuário autenticado em suas sessões.
5. No painel Unidades do aplicativo Web, aceite o valor padrão de 1 ou ajuste para um valor maior, se necessário.
6. Adicione uma tag para ajudar você a organizar seus aplicativos da web. Para o tutorial, insira Nome para a chave e Aplicativo Web Tutorial para o valor.

Tip

Você pode editar o nome do aplicativo Web diretamente da página da lista de aplicativos Web depois de criá-lo.

7. Escolha Avançar para abrir a página Design do aplicativo web. Nessa tela, forneça as seguintes informações.

Opcionalmente, você pode fornecer um título para seu aplicativo web. Você também pode fazer upload de arquivos de imagem para seu logotipo e favicon.

- Para o título da página, personalize o título da guia do navegador que seus usuários veem quando se conectam ao aplicativo web. Se você não inserir nada para o título da página, o padrão será Transfer Web App.
- Para o logotipo, faça o upload de um arquivo de imagem. O tamanho máximo do arquivo para a imagem do seu logotipo é de 50 KB.
- Para o favicon, faça upload de um arquivo de imagem. O tamanho máximo do arquivo para seu favicon é 20 KB.

8. Escolha Avançar e, em seguida, escolha Criar aplicativo web.

Para fornecer uma experiência de marca, você pode fornecer um URL personalizado para que seus usuários acessem seu aplicativo web Transfer Family. Para obter detalhes, consulte [Atualize seu endpoint de acesso com um URL personalizado](#).

Etapa 3: configurar o compartilhamento Cross-origin de recursos (CORS) para seu bucket

Você deve configurar o compartilhamento de recursos de origem cruzada (CORS) para todos os buckets usados pelo seu aplicativo web. Uma configuração CORS é um documento que define regras que identificam as origens que você permitirá acessar seu bucket. Para obter mais informações sobre o CORS, consulte [Configurando o compartilhamento de recursos de origem cruzada \(CORS\)](#).

Para configurar o compartilhamento Cross-origin de recursos (CORS) para seu bucket Amazon S3

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em. <https://console.aws.amazon.com/s3/>
2. Escolha Buckets no painel de navegação esquerdo, pesquise seu bucket na caixa de diálogo de pesquisa e, em seguida, escolha a guia Permissões.
3. Em compartilhamento Cross-origin de recursos (CORS), escolha Editar e cole o código a seguir. **AccessEndpoint** Substitua pelo endpoint de acesso real do seu aplicativo web. Certifique-se de não inserir barras finais, pois isso causa erros quando os usuários tentam fazer login no seu aplicativo web.
 - Exemplo incorreto: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Exemplo correto: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`

Se você estiver reutilizando um bucket para vários aplicativos web, anexe seus endpoints de acesso ao aplicativo web à lista. AllowedOrigins

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://AccessEndpoint"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
      "x-amz-cf-id",
      "x-amz-storage-class",
      "access-control-expose-headers"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

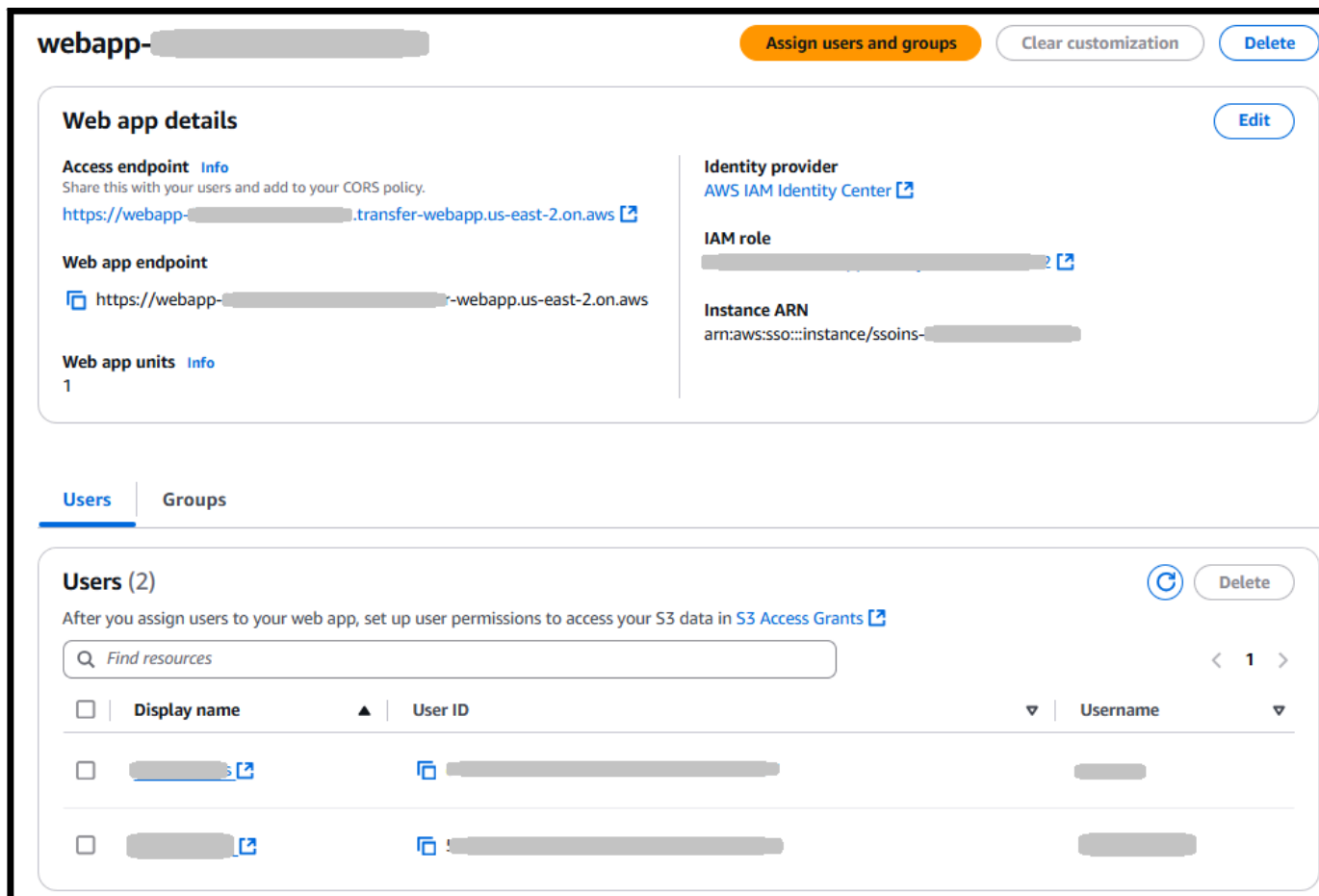
4. Escolha Salvar alterações para atualizar o CORS.

Etapa 4: adicionar um usuário ao seu aplicativo web Transfer Family

Adicione o usuário que você criou anteriormente no IAM Identity Center.

Para atribuir usuários a um aplicativo web Transfer Family

1. Navegue até o aplicativo web que você criou anteriormente.
2. Escolha Atribuir usuários e grupos.



3. Para atribuir o usuário que você criou anteriormente no IAM Identity Center, selecione Atribuir usuários e grupos existentes e selecione Avançar.
 - a. Pesquise o usuário pelo nome de exibição. Observe que nenhum usuário aparece até você começar a inserir seus critérios de pesquisa. Para adicionar **Bob Stiles**, digite bob na caixa de pesquisa. Se você não conseguir encontrar seu usuário, navegue até o console de gerenciamento do IAM Identity Center, encontre o usuário e, em seguida, copie e cole o nome de exibição dele aqui.
 - b. Escolha o **Bob Stiles** usuário e, em seguida, escolha Atribuir.

Etapa 5: registrar um local no Amazon S3 e criar uma concessão de acesso

Depois de atribuir um usuário ao seu aplicativo web, você precisa registrar um bucket e criar uma concessão de acesso para esse usuário.

Note

Você deve ter uma instância do S3 Access Grants antes de continuar. Para obter detalhes, consulte [Criar uma instância do S3 Access Grants](#) no Guia do usuário do Amazon Simple Storage Service.

Para registrar um local e criar uma concessão de acesso

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em. <https://console.aws.amazon.com/s3/>
2. Escolha Access Grants no painel de navegação esquerdo.
3. Escolha Exibir detalhes para ver os detalhes da sua instância do S3 Access Grants.
4. Selecione a guia Localizações e escolha Registrar localização.
5. Forneça as informações a seguir.
 - Para o Escopo, procure um bucket ou insira o nome do seu bucket e, opcionalmente, um prefixo. Observe que o escopo começa com a string **s3://**.
 - Para a função do IAM, escolha Create new role para que o Amazon S3 crie uma função. Essa função permite que o S3 Access Grants acesse seu escopo de localização especificado.

Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Register location

Register location [Info](#)

Registering a location for S3 your S3 Access Grants instance assigns an IAM role the permission to get temporary credentials to access resources within the specified scope.

Location [Info](#)

Location scope [Info](#)

You can't edit the location scope after registering the location.

Scope

[View](#) [Browse S3](#)

Format for all buckets: s3://
 Format for bucket: s3://<bucket>
 Format for prefix: s3://<bucket>/<prefix-with-path>

Permissions

This IAM role allows S3 Access Grants to access your specified location scope.

Permissions

To ensure the role has proper permissions to access the location scope, consult the [list of permissions](#).

IAM role [Info](#)

This IAM role allows S3 Access Grants to access your specified location scope.

☒ Create new role
☐ Choose from existing IAM roles
☐ Enter IAM role ARN

[Cancel](#) [Register location](#)

Escolha Registrar local para continuar.

6. Selecione a guia Concessões e, em seguida, escolha Criar concessão e forneça os detalhes a seguir.

- Em Local, selecione Procurar locais e escolha o local que você registrou na etapa anterior.
- Em Subprefixo, insira * para indicar que a concessão de acesso se aplica a todo o bucket.
- Em Permissões, selecione Ler e gravar.
- Para o tipo de beneficiário, escolha Identidade do diretório no IAM Identity Center.
- Em Tipo de identidade de diretório, selecione Usuário.
- No ID de usuário/ID do IAM Identity Center, copie e cole o ID do usuário para **Bob Stiles**. Essa ID está disponível no painel Usuários do seu aplicativo web Transfer Family.

7. Escolha Criar concessão.

A concessão de acesso é criada.

Etapa 6: Acesse seu aplicativo web Transfer Family como usuário

Agora, navegamos até o URL do aplicativo web e fazemos login como o usuário que atribuímos anteriormente.

Para fazer login no aplicativo web Transfer Family

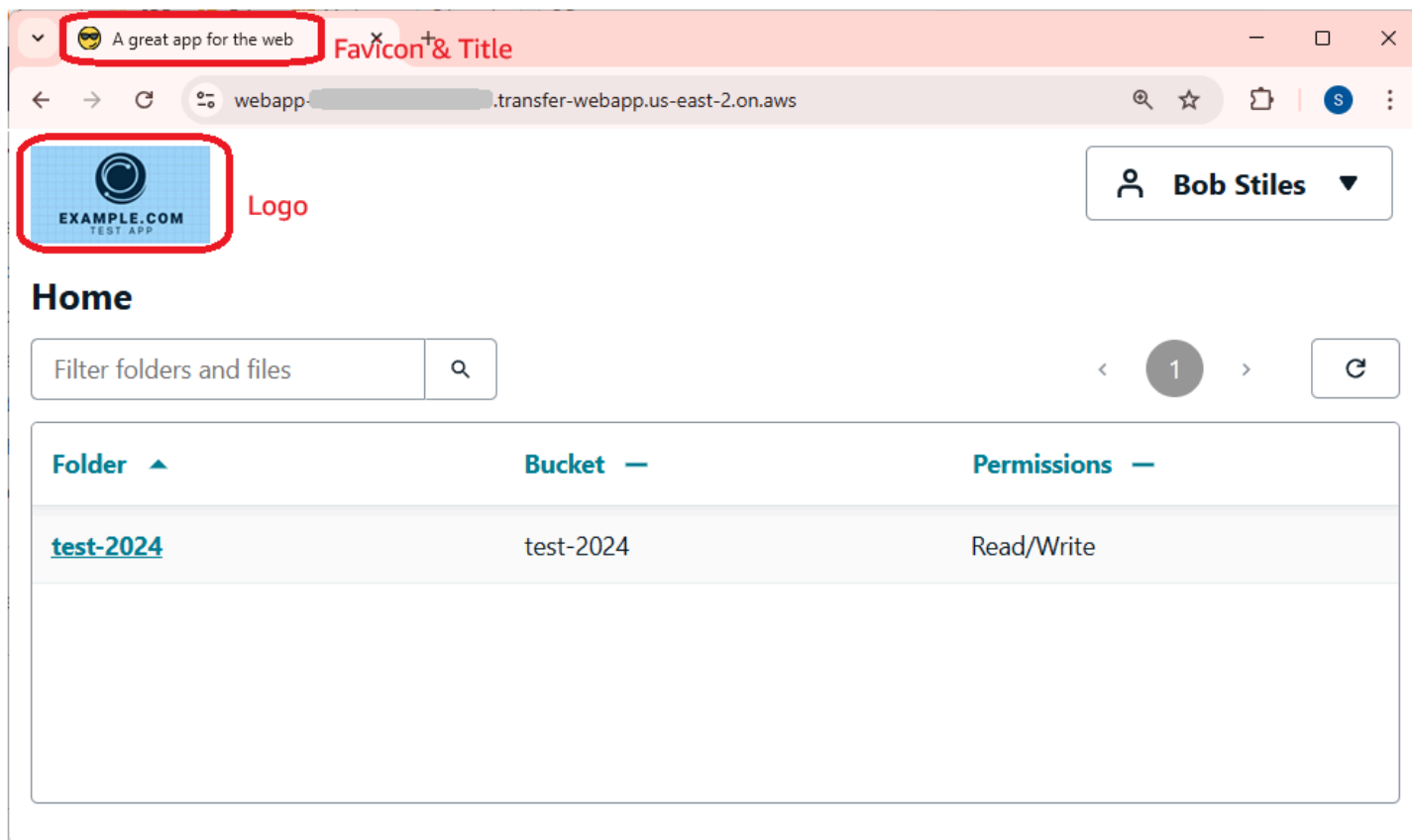
1. Navegue até seu aplicativo web
2. Escolha o endpoint do Access no painel de detalhes do aplicativo Web.

The screenshot shows the AWS Transfer Family console interface. At the top, there's a header for a specific web app, 'webapp-...', with buttons for 'Assign users and groups', 'Clear customization', and 'Delete'. Below this is a 'Web app details' section. The 'Access endpoint' is highlighted with a red box and contains the URL 'https://webapp-...transfer-webapp.us-east-2.on.aws'. Other details include 'Web app endpoint', 'Web app units' (1), 'Identity provider' (AWS IAM Identity Center), 'IAM role' (AWSTransferWebAppIdentityBearer-us-east-2), and 'Instance ARN'. Below the details section, there are tabs for 'Users' and 'Groups'. The 'Users' tab is active, showing a list of users. One user, 'Bob Stiles', is highlighted with a red box, with a 'Username' of 'bobstiles'.

3. Na tela de login, insira o usuário que você criou **bobstiles** e selecione Avançar.
4. Digite a senha que o sistema atribuiu a esse usuário quando foi criada e selecione Avançar.
5. Se sua organização exige autenticação multifator (MFA), você precisa configurá-la agora. Caso contrário, vá para a etapa 6.
 - a. Você verá uma tela para registrar seu dispositivo de MFA. Escolha uma das opções disponíveis e selecione Avançar.
 - b. Execute as etapas necessárias para configurar a MFA para esse usuário: as etapas dependem da opção de MFA escolhida.

- c. Talvez seja necessário definir uma nova senha para seu usuário: se necessário, faça isso agora. O sistema também pode exigir que você faça login novamente, usando as novas credenciais de MFA que você configurou.

Seu usuário deve ver uma tela semelhante à seguinte. Observe que essa captura de tela inclui a personalização do favicon e do logotipo.



Próximas etapas

Você configurou com êxito um aplicativo web básico do Transfer Family com acesso padrão ao bucket do S3. Se você precisar de um controle mais granular sobre as permissões do bucket, como permitir que os usuários baixem de um bucket e façam o upload para outro, consulte [Tutorial: Configurando um aplicativo AWS Transfer Family web com acesso seletivo a vários buckets](#).

Integre o Okta como seu provedor de identidade para aplicativos da web

Você pode integrar um provedor de identidade externo aos aplicativos web Transfer Family. Esta seção descreve como configurar o Okta como seu provedor de identidade.

1. No Okta, crie um usuário, um grupo e um aplicativo. Para obter detalhes sobre como fazer isso, consulte [Configurar SAML e SCIM com o Okta e o IAM Identity Center](#).

The screenshot displays the AWS IAM Identity Center console. The left sidebar contains navigation links: Applications, Self Service, API Service Integrations, Your OIN Integrations, Security, Workflow, Reports, and Settings. The main panel is titled 'AWS IAM Identity Center' and has tabs for General, Sign On, Provisioning, Import, Assignments, and Push Groups. The 'Push Groups' tab is active, showing a table of pushed groups. The table has columns: Pushed Groups, Group in Okta, Group in AWS IAM Identity Center, Last Push, and Push Status. One group, 'Examplegroup', is shown with a status of 'Active'.

2. Conecte o Okta e importe usuários e grupos do Okta para o Centro de Identidade do AWS IAM. Siga as etapas de 1 a 4 em [Configurar SAML e SCIM com Okta e IAM Identity Center](#).

The screenshot shows the AWS IAM Identity Center console with the 'Users' tab selected. The left sidebar includes links for Dashboard, Users, Groups, Settings, and Multi-account permissions. The main panel displays a message about the external identity provider configuration. Below, a table lists users. The 'Exampleuser' entry is highlighted with a red box, showing its status as 'Enabled' and created by 'SCIM'.

Username	Display name	Status	Created by
Exampleuser	Example User	Enabled	SCIM
johnstiles	John Stiles	Enabled	Manual

IAM Identity Center

Managing instance
ssoins-6684735b83d16df8

Dashboard

Users

Groups

Settings

Multi-account permissions

AWS accounts

Permission sets

Your identity source is currently configured as 'External identity provider'. To add new groups or edit their memberships, you must do this using your external identity provider.

Groups (2)

With groups, you can grant or deny permissions to groups of workforce users, rather than having to apply those permissions to each user. [Learn more](#)

Find groups by group name

< 1 >

	Group name	Users	Description	Created by
☐	Examplegroup	1 user	-	SCIM
☐	dev	1 user	-	Manual

3. Confirme se a fonte de identidade no IAM Identity Center é SAML 2.0.

Settings

Details

Configure your identity source and multi-factor authentication settings for use when managing access to your AWS accounts, resources, and cloud applications.

Instance name - [Edit](#)

Region
US East (Ohio) | us-east-2

Instance ID
ssoins-

Date created
Thursday, November 14, 2024 at 4:11:19 PM EST

Organization ID
AWS Organizations not enabled

Instance ARN
[arn:aws:sso:::instance/ssoins-](#)

Identity source

Authentication

Management

Tags

Identity source

Choose the directory where you want to manage your users and groups. [Learn More](#)

Identity source
External identity provider

Authentication method
SAML 2.0

Provisioning method
SCIM

AWS access portal URL
[https://.awsapps.com/start](#)

Identity store ID
d-

Issuer URL
[https://identitycenter.amazonaws.com/ssoins-](#)

Actions

Integre o Okta como seu provedor de identidade para aplicativos da web

104

4. Atribua seu usuário e grupo, conforme descrito em [Etapa 4: adicionar um usuário ao seu aplicativo web Transfer Family](#).
5. Para evitar que seus usuários precisem usar o MFA ao fazer login em seu aplicativo web, execute as etapas a seguir no Okta.
 - a. No console de administração do Okta, acesse [Aplicativos] - [Aplicativos] e selecione o Centro de Identidade do AWS IAM aplicativo.
 - b. Na guia Entrar, selecione [Autenticação do usuário] - Editar.
 - c. Selecione Somente senha.

Depois de realizar todas as outras etapas do tutorial, seu usuário deverá conseguir acessar seu aplicativo web Transfer Family navegando até o ponto final de acesso do aplicativo web em um navegador da web.

Tutorial: Configurando um aplicativo AWS Transfer Family web com acesso seletivo a vários buckets

Este tutorial orienta você na configuração de um aplicativo web Transfer Family com permissões específicas de bucket do Amazon S3 para um único usuário. Você aprenderá a configurar uma solução que permita aos usuários fazer o download de um bucket e fazer o upload para outro, mantendo a segurança. Este é um tutorial avançado que se baseia nos conceitos abordados no tutorial básico. Se você é novato em aplicativos AWS Transfer Family da web, considere começar com [Tutorial: Configurando um aplicativo web básico do Transfer Family](#).

Pré-requisitos

Antes de iniciar este tutorial, será necessário:

- O IAM Identity Center está configurado na mesma região do seu aplicativo AWS Transfer Family web. Observe que AWS permite apenas uma instância do IAM Identity Center por AWS conta para todas as regiões.
- Pelo menos um usuário configurado no IAM Identity Center.
- Dois buckets S3: um para downloads e outro para uploads.

 Note

Este tutorial compartilha muitos pré-requisitos com o tutorial básico do aplicativo web. Para obter mais informações sobre como configurar o IAM Identity Center e criar usuários, consulte [Tutorial: Configurando um aplicativo web básico do Transfer Family](#).

Etapa 1: criar um aplicativo web Transfer Family

Para criar um aplicativo web Transfer Family

1. Faça login no Console de gerenciamento da AWS e abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, escolha Aplicativos Web.
3. Escolha Criar aplicativo web.

Para acesso à autenticação, observe que o serviço encontra automaticamente a Centro de Identidade do AWS IAM instância que você configurou como pré-requisito.

4. No painel Tipo de permissão, selecione Criar e usar uma nova função de serviço. O serviço cria a função de portador de identidade para você. Uma função de portador de identidade inclui a identidade de um usuário autenticado em suas sessões.
5. No painel Unidades do aplicativo Web, aceite o valor padrão de 1 ou ajuste para um valor maior, se necessário.
6. Adicione uma tag para ajudar você a organizar seus aplicativos da web. Para o tutorial, insira Nome para a chave e Aplicativo Web Tutorial para o valor.

 Tip

Você pode editar o nome do aplicativo Web diretamente da página da lista de aplicativos Web depois de criá-lo.

7. Escolha Avançar para abrir a página Design do aplicativo web. Nessa tela, forneça as seguintes informações.

Opcionalmente, você pode fornecer um título para seu aplicativo web. Você também pode fazer upload de arquivos de imagem para seu logotipo e favicon.

- Para o título da página, personalize o título da guia do navegador que seus usuários veem quando se conectam ao aplicativo web. Se você não inserir nada para o título da página, o padrão será Transfer Web App.
- Para o logotipo, faça upload de um arquivo de imagem. O tamanho máximo do arquivo para a imagem do seu logotipo é de 50 KB.
- Para o favicon, faça upload de um arquivo de imagem. O tamanho máximo do arquivo para seu favicon é 20 KB.

8. Escolha Avançar e, em seguida, escolha Criar aplicativo web.

Etapa 2: configurar funções do IAM para acesso ao S3

Você precisa criar duas funções do IAM: uma com acesso somente para download ao primeiro bucket e outra com acesso somente para upload ao segundo bucket.

Política de confiança para ambas as funções

Use a seguinte política de confiança para as duas funções do IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AccessGrantsTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity",
        "sts:SetContext"
      ]
    }
  ]
}
```

Política do IAM para bucket de download

Crie uma função do IAM com a seguinte política para acesso somente de leitura ao seu bucket de download:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        "arn:aws:s3:::amzn-s3-demo-bucket1"
      ]
    }
  ]
}
```

Important

Substitua amzn-s3-demo-bucket1 pelo nome real do seu bucket de download.

Política do IAM para bucket de upload

Crie outra função do IAM com a seguinte política para acesso de gravação ao seu bucket de upload:

```
{
  "Version": "2012-10-17",
  "Statement": [
```



```
{
  "Sid": "ObjectLevelWritePermissions",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:PutObjectVersionAcl",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:AbortMultipartUpload",
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket2/*",
    "arn:aws:s3:::amzn-s3-demo-bucket2"
  ]
}
```

 Important

Substitua amzn-s3-demo-bucket2 pelo nome real do seu bucket de upload.

Etapa 3: configurar o S3 Access Grants

1. Abra o console S3 em. <https://console.aws.amazon.com/s3/>
2. No painel de navegação, escolha Access Grants.
3. Clique em Criar instância do S3 Access Grants.
4. Selecione a opção Adicionar instância do IAM Identity Center e insira o ARN da instância do centro de identidade.
5. Clique em Avançar e depois em Cancelar para concluir a criação da instância do S3 Access Grants sem prosseguir com etapas adicionais.

Essa etapa cria a instância S3 Access Grants. Agora você registrará locais e criará concessões de acesso.

Etapa 4: registrar os locais dos buckets do S3

Registre os dois buckets do S3 como locais com o S3 Access Grants:

1. No console do S3 Access Grants, navegue até Localizações e clique em Registrar localização.
2. Em Escopo de localização, escolha o bucket S3 específico para downloads (amzn-s3-demo-bucket1).
3. Quando solicitado a escolher uma função do IAM, selecione a função do IAM de download que você criou anteriormente.
4. Conclua o processo de registro.
5. Repita o processo para registrar o bucket de upload (amzn-s3-demo-bucket2), selecionando a função de upload do IAM quando solicitado.

Etapa 5: criar concessões de acesso

Crie duas bolsas, uma para cada local registrado:

1. No console do S3 Access Grants, navegue até Grants e clique em Create grant.
2. Em Localização, clique em Procurar localização e selecione a localização do bucket de download (amzn-s3-demo-bucket1).
3. Em Subprefixo (opcional), insira * para permitir o acesso ao bucket inteiro ou especifique um caminho, como restringir folder1/folder2/* o acesso a um prefixo específico.

O uso * definirá o escopo da concessão `s3://bucket-name/*` como, permitindo acesso a todo o bucket. Para permitir o acesso somente a um prefixo específico, insira um caminho como `folder1/folder2/*`, que definirá o escopo da concessão como `s3://bucket-name/folder1/folder2/*`

4. Em Permissões e acesso, selecione Ler para o bucket de download.
5. Em Tipo de beneficiário, escolha Identidade do diretório no IAM Identity Center.
6. Para o tipo principal do IAM, selecione Usuário e insira o ID de usuário do seu usuário do IAM Identity Center.
7. Conclua o processo de criação do subsídio.
8. Repita o processo para criar uma concessão para o bucket de upload (amzn-s3-demo-bucket2), mas selecione as permissões. Read-write

Etapa 6: Configurar a política CORS para buckets S3

Configure uma política de CORS para os dois buckets do S3 para permitir o acesso por meio de: AWS Transfer Family WebApp

1. Abra o console do S3 e navegue até seu bucket de download (amzn-s3-demo-bucket1).
2. Selecione a guia Permissões.
3. Role para baixo até a seção Cross-origin de compartilhamento de recursos (CORS) e clique em Editar.
4. Adicione a seguinte configuração de CORS, *WebAppEndpoint* substituindo-a pela URL real do WebApp endpoint:

Você pode encontrar a URL do endpoint do seu aplicativo web no AWS Transfer Family console abaixo WebApps. Será semelhante a `https://webapp-*****.transfer-webapp.us-west-2.on.aws`.

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://WebAppEndpoint"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
      "x-amz-cf-id",
```

```
        "x-amz-storage-class",  
        "access-control-expose-headers"  
    ],  
    "MaxAgeSeconds": 3000  
}  
]
```

5. Clique em Salvar alterações.
6. Repita o processo para seu bucket de upload (amzn-s3-demo-bucket2).

Etapa 7: testar a configuração

1. Abra o URL do seu aplicativo AWS Transfer Family web. Você pode encontrar esse URL no AWS Transfer Family console, abaixo WebApps do campo Endpoint do Access.
2. Faça login usando as credenciais de usuário do IAM Identity Center que você configurou com concessões de acesso.
3. Depois de fazer login, você deve ver os dois locais do S3 na página inicial.
4. Navegue até o bucket de download (amzn-s3-demo-bucket1) e verifique se você pode baixar arquivos, mas não fazer upload.
5. Navegue até o bucket de upload (amzn-s3-demo-bucket2) e verifique se você pode fazer upload de arquivos.

Conclusão

Você configurou AWS Transfer Family WebApp com sucesso o acesso seletivo ao bucket do S3 para um único usuário. Essa configuração permite que o usuário faça o download de um bucket e faça o upload para outro, mantendo a segurança por meio de funções do IAM e concessões de acesso do S3.

Essa abordagem pode ser estendida a vários usuários criando concessões adicionais no S3 Access Grants para cada usuário, permitindo um controle granular sobre as permissões de acesso ao bucket. Para obter informações sobre a configuração básica do aplicativo web, consulte [Tutorial: Configurando um aplicativo web básico do Transfer Family](#).

Configurando um endpoint de servidor SFTP, FTPS ou FTP

Este tópico fornece detalhes sobre como criar e usar endpoints de AWS Transfer Family servidor que usam um ou mais dos protocolos SFTP, FTPS e FTP.

Tópicos

- [Opções do provedor de identidade](#)
- [AWS Transfer Family matriz de tipo de endpoint](#)
- [Configurando um endpoint de servidor SFTP, FTPS ou FTP](#)
- [Considerações sobre o Network Load Balancer de FTP e FTPS](#)
- [Transferindo arquivos em um endpoint de servidor usando um cliente](#)
- [Gerenciando usuários para endpoints de servidor](#)
- [Como usar diretórios lógicos para simplificar suas estruturas de diretórios do Transfer Family](#)
- [Acesse seus sistemas de arquivos FSx for NetApp ONTAP com Transfer Family](#)

Opções do provedor de identidade

AWS Transfer Family fornece vários métodos para autenticar e gerenciar usuários. A tabela a seguir compara os provedores de identidade disponíveis que é possível usar com o Transfer Family.

Ação	AWS Transfer Family serviço gerenciado	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
Protocolos compatíveis	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
Key-based authentication	Sim	Não	Sim	Sim
Autenticação com senha	Não	Sim	Sim	Sim
AWS Identity and Access	Sim	Sim	Sim	Sim

Ação	AWS Transfer Family serviço gerenciado	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
Management (IAM) e POSIX				
Diretório inicial lógico	Sim	Sim	Sim	Sim
Acesso parametrizado (baseado em nome de usuário)	Sim	Sim	Sim	Sim
Estrutura de acesso ad hoc	Sim	Não	Sim	Sim
AWS WAF	Não	Não	Sim	Não

Observações:

- O IAM é usado para controlar o acesso ao armazenamento de apoio do Amazon S3, e o POSIX é usado para o Amazon EFS.
- Ad hoc se refere à capacidade de enviar o perfil do usuário em runtime. Por exemplo, é possível direcionar os usuários para seus diretórios pessoais ao passar o nome de usuário como uma variável.
- Para obter detalhes sobre AWS WAF, consulte [Adicione um firewall da aplicação web](#).
- Há uma postagem no blog que descreve o uso de uma função Lambda integrada ao Microsoft Entra ID (antigo Azure AD) como seu provedor de identidade do Transfer Family. Para obter detalhes, consulte [Autenticando AWS Transfer Family com o Azure Active Directory e AWS Lambda](#).
- Fornecemos vários CloudFormation modelos para ajudar você a implantar rapidamente um servidor Transfer Family que usa um provedor de identidade personalizado. Para obter detalhes, consulte [Modelos de função do Lambda](#).

Nos procedimentos a seguir, você pode criar um SFTP-enabled servidor, FTPS-enabled servidor, FTP-enabled servidor ou AS2-enabled servidor.

Próxima etapa

- [Crie um SFTP-enabled servidor](#)
- [Crie um FTPS-enabled servidor](#)
- [Crie um FTP-enabled servidor](#)
- [Configurar AS2](#)

AWS Transfer Family matriz de tipo de endpoint

Ao criar um servidor Transfer Family, você escolhe o tipo de endpoint a ser usado. A tabela a seguir descreve as características de cada tipo de endpoint.

Matriz de tipo de endpoint

Característica	Public	VPC - Internet	VPC - Interna	VPC_Endpoint (obsoleto)
Protocolos compatíveis	SFTP	SFTP, FTPS, AS2	SFTP, FTPS, FTP, AS2	SFTP
Acesso	Da Internet. Esse tipo de endpoint não exige nenhuma configuração especial em seu VPC.	Pela Internet e de dentro da VPC e de VPC-connected ambientes, como um data center local ou VPN. Direct Connect	De dentro da VPC e de VPC-connected ambientes, como um data center local ou VPN. Direct Connect	De dentro da VPC e de VPC-connected ambientes, como um data center local ou VPN. Direct Connect
Endereços IP estáticos	Você não pode anexar um endereço IP estático. AWS fornece endereços	É possível anexar endereços IP elásticos ao endpoint. Eles podem ser	Os endereços IP privados anexados ao endpoint não mudam.	Os endereços IP privados anexados ao endpoint não mudam.

Característica	Public	VPC - Internet	VPC - Interna	VPC_Endpoint (obsoleto)
	IP que estão sujeitos a alterações.	endereços IP da AWS ou seus próprios endereços IP (Trazer seus próprios endereços IP). Endereços IP elásticos anexados ao endpoint não mudam. Os endereços IP privados anexados ao servidor também não mudam.		

Característica	Public	VPC - Internet	VPC - Interna	VPC_Endpoint (obsoleto)
Lista de permissões de IP de origem	Esse tipo de endpoint não oferece suporte a listas de permissões por endereços IP de origem. O endpoint é acessível ao público e recebe o tráfego pela porta 22.  Note Para VPC-hosted endpoints, os servidores SFTP Transfer Family podem operar na porta 22 (o padrão), 2222, 2223 ou 22000.	Para permitir o acesso por endereço IP de origem, é possível usar grupos de segurança conectados aos endpoints do servidor e ACLs de rede conectadas à sub-rede em que o endpoint está.	Para permitir o acesso por endereço IP de origem, é possível usar grupos de segurança conectados aos endpoints do servidor e lista de controle de acesso à rede (ACL da rede) conectadas à sub-rede em que o endpoint está.	Para permitir o acesso por endereço IP de origem, é possível usar grupos de segurança conectados aos endpoints do servidor e ACLs de rede conectadas à sub-rede em que o endpoint está.

Característica	Public	VPC - Internet	VPC - Interna	VPC_Endpoint (obsoleto)
Lista de permissões do firewall do cliente	Você deve permitir o nome DNS do servidor. Como os endereços IP estão sujeitos a alterações, evite usar endereços IP na lista de permissões do firewall do cliente.	É possível permitir o nome DNS do servidor ou os endereços IP elásticos anexados ao servidor.	É possível permitir os endereços IP privados ou o nome DNS dos endpoints.	É possível permitir os endereços IP privados ou o nome DNS dos endpoints.
Tipo de endereço IP	IPv4 (padrão) ou pilha dupla (IPv4 e IPv6)	Somente IPv4 (pilha dupla não suportada)	IPv4 (padrão) ou pilha dupla (IPv4 e IPv6)	Somente IPv4 (pilha dupla não suportada)

Note

O tipo de endpoint VPC_ENDPOINT agora está obsoleto e não pode ser usado para criar novos servidores. Em vez de usar `EndpointType=VPC_ENDPOINT`, use o VPC endpoint type (`EndpointType=VPC`), que você pode usar como interno ou voltado para a Internet, conforme descrito na tabela anterior.

- Para obter detalhes sobre a suspensão de uso, consulte. [Interromper o uso do VPC_ENDPOINT](#)
- Para obter informações sobre o gerenciamento de permissões de VPC endpoint, consulte. [Limitando o acesso ao VPC endpoint para servidores Transfer Family](#)

Considere as seguintes opções para aumentar a postura de segurança do seu servidor AWS Transfer Family :

- Use um VPC endpoint com acesso interno, para que o servidor possa ser acessado somente por clientes dentro de sua VPC ou VPC-connected ambientes como um data center local ou VPN.
Direct Connect
- Para permitir que os clientes acessem o endpoint pela Internet e protejam seu servidor, use um endpoint da VPC com acesso voltado para a Internet. Em seguida, modifique os grupos de segurança da VPC para permitir o tráfego somente de determinados endereços IP que hospedam os clientes dos seus usuários.
- Se você precisar de autenticação baseada em senha e usar um provedor de identidade personalizado com seu servidor, recomenda-se que sua política de senhas evite que os usuários criem senhas fracas e limite o número de tentativas de login malsucedidas.
- AWS Transfer Family é um serviço gerenciado e, portanto, não fornece acesso ao shell. Você não pode acessar diretamente o servidor SFTP subjacente para executar comandos nativos do sistema operacional nos servidores do Transfer Family.
- Use um Network Load Balancer na frente de um endpoint da VPC com acesso interno. Altere a porta do receptor no balanceador de carga da porta 22 para uma porta diferente. Isso pode reduzir, mas não eliminar, o risco de scanners de portas e bots sondarem seu servidor, porque a porta 22 é mais comumente usada para escaneamento. Para obter detalhes, consulte a postagem do blog [Os balanceadores de carga de rede agora oferecem suporte a grupos de segurança](#).

 Note

Se você usa um Network Load Balancer, AWS Transfer Family CloudWatch os registros mostram o endereço IP do NLB, em vez do endereço IP real do cliente.

Configurando um endpoint de servidor SFTP, FTPS ou FTP

Você pode criar um servidor de transferência de arquivos usando o AWS Transfer Family serviço. Os seguintes protocolos de transferência de arquivos estão disponíveis:

- (Secure Shell (SSH) (Protocolo de transferência de arquivos): transferência de arquivos por SSH. Para obter detalhes, consulte [the section called “Crie um SFTP-enabled servidor”](#).

 Note

Fornecemos um AWS CDK exemplo para criar um servidor SFTP Transfer Family. O exemplo usa TypeScript e está disponível GitHub [aqui](#).

- Protocolo de Transferência de Arquivos Segura (FTPS): transferência de arquivos com criptografia TLS. Para obter detalhes, consulte [the section called “Crie um FTPS-enabled servidor”](#).
- Protocolo de Transferência de Arquivos (FTP): transferência de arquivos não criptografados. Para obter detalhes, consulte [the section called “Crie um FTP-enabled servidor”](#).
- Declaração de Aplicabilidade 2 (AS2) - Transferência de Arquivos usada para transportar dados estruturados entre empresas. Para obter detalhes, consulte [the section called “Configurar AS2”](#). Para o AS2, você pode criar rapidamente uma CloudFormation pilha para fins de demonstração. Este procedimento está descrito em [Use um modelo para criar uma pilha de demonstração do Transfer Family AS2](#).

É possível criar um servidor com vários protocolos.

 Note

Se você tiver vários protocolos habilitados para o mesmo endpoint do servidor, e quiser fornecer acesso usando o mesmo nome de usuário em vários protocolos, poderá fazer isso desde que as credenciais específicas do protocolo tenham sido configuradas no seu provedor de identidade. Para FTP, recomendamos manter credenciais separadas do SFTP e do FTPS. Isso ocorre porque, diferentemente do SFTP e do FTPS, o FTP transmite credenciais em texto não criptografado. Ao isolar as credenciais de FTP do SFTP ou FTPS, se as credenciais de FTP forem compartilhadas ou expostas, suas cargas de trabalho usando SFTP ou FTPS permanecerão seguras.

Ao criar um servidor, você escolhe um específico Região da AWS para executar as solicitações de operação de arquivo dos usuários atribuídos a esse servidor. Além de atribuir ao servidor um ou mais protocolos, você também atribui um dos seguintes tipos de provedor de identidade:

- Serviço gerenciado usando chaves SSH. Para obter detalhes, consulte [Trabalhar com usuários gerenciados por serviços](#).

- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Esse método permite que você integre seus grupos do Microsoft Active Directory para fornecer acesso aos seus servidores Transfer Family. Para obter detalhes, consulte [Usando o AWS Directory Service para o Microsoft Active Directory](#).
- Um provedor de identidade personalizado. O Transfer Family oferece várias opções para usar um provedor de identidade personalizado, conforme descrito no [Trabalhar com provedores de identidade personalizados](#) tópico.

Você também atribui ao servidor um tipo de endpoint (acessível publicamente ou hospedado em VPC) e um nome de host usando o endpoint padrão do servidor, ou um nome de host personalizado usando o serviço Amazon Route 53 ou usando um serviço de Sistema de Nomes de Domínio (DNS) de sua escolha. O nome de host do servidor deve ser exclusivo na Região da AWS local em que foi criado.

Além disso, você pode atribuir uma função de CloudWatch registro da Amazon para enviar eventos aos seus CloudWatch registros, escolher uma política de segurança que contenha os algoritmos criptográficos habilitados para uso pelo seu servidor e adicionar metadados ao servidor na forma de tags que são pares de valores-chave.

Important

Você será cobrado pelos custos de servidores instanciados e por transferência de dados. Para obter informações sobre preços e como usar AWS Calculadora de Preços para obter uma estimativa do custo de uso do Transfer Family, consulte [AWS Transfer Family preços](#).

Crie um SFTP-enabled servidor

O File Transfer Protocol (SFTP) do Secure Shell (SSH) é um protocolo de rede usado para transferência segura de dados pela internet. O protocolo suporta toda a funcionalidade de segurança e autenticação do SSH. É amplamente usado para trocar dados, incluindo informações confidenciais entre parceiros de negócios em diversos setores, como serviços financeiros, saúde, varejo e publicidade.

Observe o seguinte

- Os servidores SFTP do Transfer Family operam na porta 22. Para VPC-hosted endpoints, os servidores SFTP Transfer Family também podem operar nas portas 2222, 2223 ou 22000. Para obter detalhes, consulte [Crie um servidor em uma VPC \(virtual private cloud\)](#).
- Os endpoints públicos não podem restringir o tráfego por meio de grupos de segurança. Para usar grupos de segurança com seu servidor Transfer Family, você deve hospedar o endpoint do seu servidor em uma nuvem privada virtual (VPC), conforme descrito em [Crie um servidor em uma VPC \(virtual private cloud\)](#).

Consulte também

- Fornecemos um AWS CDK exemplo para criar um servidor SFTP Transfer Family. O exemplo usa TypeScript e está disponível GitHub [aqui](#).
- Para ver um passo a passo de como implantar um servidor Transfer Family dentro de uma VPC, consulte [Use a lista de permissões de IP para proteger](#) seus servidores. AWS Transfer Family

Para criar um SFTP-enabled servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/> e selecione Servidores no painel de navegação e escolha Criar servidor.
2. Em Escolher protocolos, selecione SFTP e escolha Avançar.
3. Em Escolher um provedor de identidade, escolha o provedor de identidade que você deseja usar para gerenciar o acesso do usuário. Você tem as seguintes opções:
 - Serviço gerenciado — Você armazena identidades e chaves de usuário em AWS Transfer Family.
 - AWS Directory Service for Microsoft Active Directory — Você fornece um diretório Directory Service para acessar o endpoint. Ao fazer isso, será possível usar credenciais armazenadas no Active Directory para autenticar seus usuários. Para saber mais sobre como trabalhar com provedores de AWS Managed Microsoft AD identidade, consulte [Usando o AWS Directory Service para o Microsoft Active Directory](#).

Note

- Cross-Account e não há suporte para AWS Managed Microsoft AD diretórios compartilhados.

- Para configurar um servidor com o Directory Service como seu provedor de identidade, você precisa adicionar algumas Directory Service permissões. Para obter detalhes, consulte [Antes de começar a usar AWS Directory Service for Microsoft Active Directory](#).
- Provedor de identidade personalizado — Escolha uma das seguintes opções:
 - Use AWS Lambda para conectar seu provedor de identidade — Você pode usar um provedor de identidade existente, apoiado por uma função Lambda. Você fornece o nome da função do Lambda. Para obter mais informações, consulte [Usando AWS Lambda para integrar seu provedor de identidade](#).
 - Usar o Amazon API Gateway para conectar seu provedor de identidade — É possível criar um método de API Gateway apoiado por uma função do Lambda para uso como provedor de identidade. Você fornece um URL do Amazon API Gateway e um perfil de invocação. Para obter mais informações, consulte [Usando para integrar seu provedor de identidade](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

☒ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function





Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ **Password OR public key**

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

 Either a valid password or valid private key will be required during user authentication

[Cancel](#) [Previous](#) [Next](#)

4. Escolha Próximo.
5. Em Escolha um endpoint, faça o seguinte:
 - a. Em Tipo de endpoint, escolha o tipo de endpoint Acessível publicamente. Para um endpoint hospedado no VPC, consulte [Crie um servidor em uma VPC \(virtual private cloud\)](#).
 - b. Para o tipo de endereço IP, escolha IPv4 (padrão) para compatibilidade com versões anteriores ou para Dual-stack habilitar conexões IPv4 e IPv6 com seu endpoint.

 Note

Dual-stack O modo permite que seu endpoint Transfer Family se comunique com clientes habilitados para IPv4 e IPv6. Isso permite que você faça a transição gradual de sistemas baseados em IPv4 para IPv6 sem precisar alternar tudo de uma vez.

- c. (Opcional) Em Nome de host personalizado, escolha Nenhum.

Você recebe um nome de host do servidor fornecido por AWS Transfer Family. O nome do host do servidor tem a forma de `serverId.server.transfer.regionId.amazonaws.com`.

Para um nome de host personalizado, você especifica um alias personalizado para o endpoint do seu servidor. Para saber mais sobre como trabalhar com nomes de host personalizados, consulte [Trabalhar com nomes de host personalizados](#).

- d. (Opcional) Para FIPS ativado, marque a caixa de seleção Endpoint habilitado para FIPS para garantir que o endpoint esteja em conformidade com os Padrões Federais de Processamento de Informações (FIPS).

 Note

FIPS-enabled os endpoints estão disponíveis somente nas AWS regiões da América do Norte. Para saber as regiões disponíveis, consulte [Endpoints e cotas do AWS Transfer Family](#) em Referência geral da AWS. Para obter mais informações, consulte [FIPS – Padrão federal de processamento de informações 140-2](#).

- e. Escolha Próximo.

6. Na página Escolher domínio, escolha o serviço AWS de armazenamento que você deseja usar para armazenar e acessar seus dados pelo protocolo selecionado:

- Escolha o Amazon S3 para armazenar e acessar seus arquivos como objetos no protocolo selecionado.
- Escolha o Amazon EFS para armazenar e acessar seus arquivos em seu sistema de arquivos Amazon EFS usando o protocolo selecionado.

Escolha Próximo.

7. Em Configuração de detalhes adicionais, faça o seguinte:
- Para registro em log, especifique um grupo de logs existente ou crie um novo (a opção padrão). Se você escolher um grupo de registros existente, deverá selecionar um que esteja associado ao seu Conta da AWS.

The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains two sections: 'Logging' and 'Logging role'. The 'Logging' section has a heading 'Log group' and a description: 'Choose the CloudWatch log group where your events will be delivered in a structured JSON format'. It offers two options: 'Create a new log group' (unselected) and 'Choose an existing log group' (selected). Below these is a text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. The 'Logging role' section has a heading 'Logging role' and a description: 'Choose the IAM role that will be used to deliver events to your CloudWatch logs'. It offers two options: 'Create a new role' (unselected) and 'Choose an existing role' (unselected). At the bottom, a blue information box states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Se você escolher Criar grupo de registros, o CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) abrirá a página Criar grupo de registros. Para obter detalhes, consulte [Criar um grupo de CloudWatch registros em Registros](#).

- (Opcional) Para Fluxos de trabalho gerenciados, escolha IDs de fluxo de trabalho (e uma função correspondente) que o Transfer Family deve assumir ao executar o fluxo de trabalho. É possível escolher um fluxo de trabalho para executar em um upload completo e outro para executar em um upload parcial. Para saber mais sobre como processar seus arquivos usando fluxos de trabalho gerenciados, consulte [AWS Transfer Family fluxos de trabalho gerenciados](#).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

- c. Para Opções de algoritmo criptográfico, escolha uma política de segurança que contenha os algoritmos criptográficos habilitados para uso pelo seu servidor. Nossa política de segurança mais recente é a padrão: para obter detalhes, consulte [Políticas de segurança para AWS Transfer Family servidores](#).
- d. (Opcional) Para Chave de host do servidor, insira uma chave privada RSA, ED25519 ou ECDSA que será usada para identificar seu servidor quando os clientes se conectarem a ele por SFTP. Você também pode adicionar uma descrição para diferenciar entre várias chaves de host.

Depois de criar seu servidor, é possível adicionar mais chaves de host. Ter várias chaves de host é útil se você quiser rotar chaves ou se quiser ter diferentes tipos de chaves, como uma chave RSA e também uma chave ECDSA.

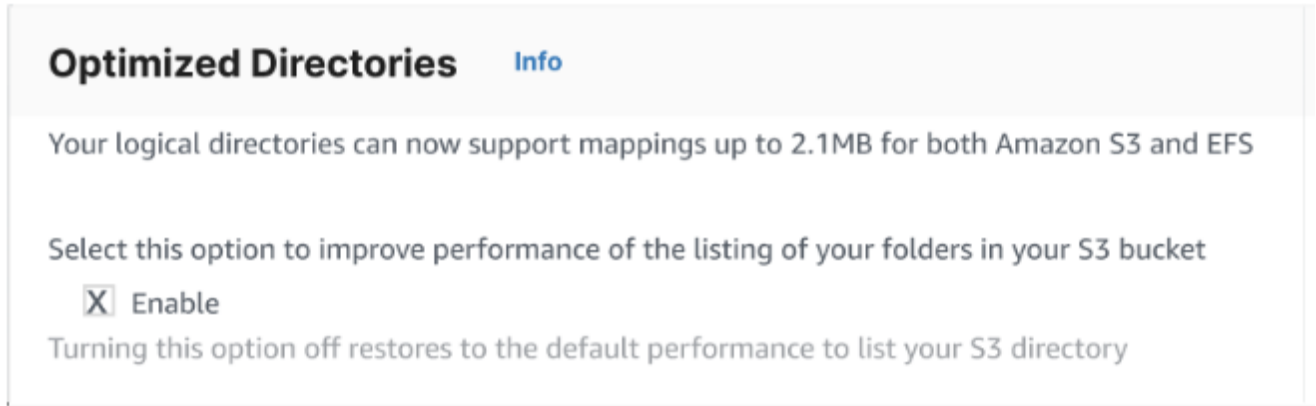
Note

A seção Chave do Host do Servidor é usada somente para migrar usuários de um SFTP-enabled servidor existente.

- e. (Opcional) Em Tags, para Chave e Valor, insira uma ou mais tags como pares de valor-chave e escolha Adicionar tag.
- f. Escolha Próximo.
- g. Você pode otimizar o desempenho dos seus diretórios do Amazon S3. Por exemplo, suponha que você acesse seu diretório inicial e tenha 10.000 subdiretórios. Em outras palavras, seu bucket do Amazon S3 tem 10.000 pastas. Nesse cenário, se você executar o

comando `ls` (list), a operação de lista levará entre seis e oito minutos. No entanto, se você otimizar seus diretórios, essa operação levará apenas alguns segundos.

Quando você cria seu servidor usando o console, os diretórios otimizados são habilitados por padrão. Se você criar seu servidor usando a API, esse comportamento não será ativado por padrão.



- h. (Opcional) Configure AWS Transfer Family servidores para exibir mensagens personalizadas, como políticas organizacionais ou termos e condições, para seus usuários finais. Em Exibir banner, na caixa de texto Pre-authentication Exibir banner, insira a mensagem de texto que você deseja exibir para seus usuários antes que eles se autenticarem.
- i. (Opcional) É possível configurar as seguintes opções adicionais.
 - SetStat opção: habilite essa opção para ignorar o erro gerado quando um cliente tenta usar SETSTAT em um arquivo que você está carregando em um bucket do Amazon S3. Para obter detalhes adicionais, consulte a [SetStatOption](#) documentação no [ProtocolDetails](#).
 - Retomada da sessão TLS: essa opção só estará disponível se você tiver habilitado o FTPS como um dos protocolos desse servidor.
 - IP passivo: essa opção só estará disponível se você tiver habilitado o FTPS ou o FTP como um dos protocolos desse servidor.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

To enable TLS session resumption, enable FTPS as one of the protocols selected in Step 1

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

To enable Passive IP, enable FTP or FTPS as one of the protocols selected in Step 1

8. Em Revisar e criar, revise as suas escolhas.

- Se você quiser editar algum deles, escolha Editar ao lado da etapa.

Note

Você deve revisar cada etapa após a etapa que você escolheu editar.

- Se você não tiver alterações, escolha Criar servidor para criar seu servidor. Você será direcionado à página Servidores, exibida a seguir, onde seu novo servidor estará listado.

Pode levar alguns minutos até que o status de seu novo servidor mude para Online. Nesse ponto, seu servidor pode realizar operações com arquivos, mas primeiro você precisa criar um usuário.

Para obter detalhes sobre a criação de usuários, consulte [Gerenciando usuários para endpoints de servidor](#).

Crie um FTPS-enabled servidor

O protocolo de Transferência de Arquivos em SSL (FTPS) é uma extensão do FTP. Ele usa os protocolos criptográficos Transport Layer Security (TLS) e Secure Sockets Layer (SSL) para criptografar o tráfego. O FTPS permite a criptografia das conexões do canal de controle e de dados simultaneamente ou de forma independente.

Note

Para considerações importantes sobre balanceadores de carga de rede, consulte [Evite colocar NLBs e NATs na frente de AWS Transfer Family servidores](#)

Para criar um FTPS-enabled servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/> e selecione Servidores no painel de navegação e escolha Criar servidor.
2. Em Escolher protocolos, selecione FTPS.

Em Certificado de servidor, escolha um certificado armazenado em AWS Certificate Manager (ACM) que será usado para identificar seu servidor quando os clientes se conectarem a ele via FTPS e, em seguida, escolha Avançar.

Para solicitar um novo certificado público, consulte [Solicitar um certificado público](#) no Guia do usuário do AWS Certificate Manager .

Para importar um certificado existente para o ACM, consulte [Importar certificados para o ACM](#) no Guia do usuário do AWS Certificate Manager .

Para solicitar um certificado privado para usar FTPS por meio de endereços IP privados, consulte [Solicitar um certificado privado](#) no Guia do usuário do AWS Certificate Manager .

Os certificados com os seguintes algoritmos criptográficos e tamanhos de chave são compatíveis:

- RSA de 2048 bits (RSA_2048)
- RSA de 4096 bits (RSA_4096)

- Elliptic Prime Curve de 256 bits (EC_prime256v1)
- Elliptic Prime Curve de 384 bits (EC_secp384r1)
- Elliptic Prime Curve de 521 bits (EC_secp521r1)

 Note

O certificado deve ser um certificado válido da SSL/TLS X.509 versão 3 com FQDN ou endereço IP especificado e conter informações sobre o emissor.

3. Em Escolher um provedor de identidade, escolha o provedor de identidade que você deseja usar para gerenciar o acesso do usuário. Você tem as seguintes opções:

- AWS Directory Service for Microsoft Active Directory— Você fornece um Directory Service diretório para acessar o endpoint. Ao fazer isso, será possível usar credenciais armazenadas no Active Directory para autenticar seus usuários. Para saber mais sobre como trabalhar com provedores de AWS Managed Microsoft AD identidade, consulte [Usando o AWS Directory Service para o Microsoft Active Directory](#).

 Note

- Cross-Account e não há suporte para AWS Managed Microsoft AD diretórios compartilhados.
- Para configurar um servidor com o Directory Service como seu provedor de identidade, você precisa adicionar algumas Directory Service permissões. Para obter detalhes, consulte [Antes de começar a usar AWS Directory Service for Microsoft Active Directory](#).

- Provedor de identidade personalizado — Escolha uma das seguintes opções:
 - Use AWS Lambda para conectar seu provedor de identidade — Você pode usar um provedor de identidade existente, apoiado por uma função Lambda. Você fornece o nome da função do Lambda. Para obter mais informações, consulte [Usando AWS Lambda para integrar seu provedor de identidade](#).
 - Usar o Amazon API Gateway para conectar seu provedor de identidade — É possível criar um método de API Gateway apoiado por uma função do Lambda para uso como provedor de identidade. Você fornece um URL do Amazon API Gateway e um perfil de invocação. Para obter mais informações, consulte [Usando para integrar seu provedor de identidade](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory

Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity

Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

- Escolha Próximo.
- Em Escolha um endpoint, faça o seguinte:

[i](#) Note

Os servidores FTPS do Transfer Family operam na porta 21 (canal de controle) e no intervalo de portas 8192—8200 (canal de dados).

- a. Em Tipo de endpoint, escolha o tipo de endpoint Hospedado em VPC para hospedar o endpoint do seu servidor. Para obter mais informações sobre como configurar endpoint hospedado no VPC, consulte [Crie um servidor em uma VPC \(virtual private cloud\)](#).

 Note

Não há suporte para endpoints acessíveis publicamente.

- b. (Opcional) Para FIPS ativado, marque a caixa de seleção Endpoint habilitado para FIPS para garantir que o endpoint esteja em conformidade com os Padrões Federais de Processamento de Informações (FIPS).

 Note

FIPS-enabled os endpoints estão disponíveis somente nas AWS regiões da América do Norte. Para saber as regiões disponíveis, consulte [Endpoints e cotas do AWS Transfer Family](#) em Referência geral da AWS. Para obter mais informações, consulte [FIPS – Padrão federal de processamento de informações 140-2](#).

- c. Escolha Próximo.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

6. Na página Escolher domínio, escolha o serviço AWS de armazenamento que você deseja usar para armazenar e acessar seus dados pelo protocolo selecionado:
- Escolha o Amazon S3 para armazenar e acessar seus arquivos como objetos no protocolo selecionado.
 - Escolha o Amazon EFS para armazenar e acessar seus arquivos em seu sistema de arquivos Amazon EFS usando o protocolo selecionado.

Escolha Próximo.

7. Em Configuração de detalhes adicionais, faça o seguinte:

- a. Para registro em log, especifique um grupo de logs existente ou crie um novo (a opção padrão).

The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains a 'Logging' section. Under 'Log group', it instructs to 'Choose the CloudWatch log group where your events will be delivered in a structured JSON format'. There are two radio buttons: 'Create a new log group' (unselected) and 'Choose an existing log group' (selected). Below the radio buttons is a text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. Under 'Logging role', it instructs to 'Choose the IAM role that will be used to deliver events to your CloudWatch logs'. There are two radio buttons: 'Create a new role' (unselected) and 'Choose an existing role' (unselected). At the bottom, a blue information box states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Se você escolher Criar grupo de registros, o CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) abrirá a página Criar grupo de registros. Para obter detalhes, consulte [Criar um grupo de CloudWatch registros em Registros](#).

- b. (Opcional) Para Fluxos de trabalho gerenciados, escolha IDs de fluxo de trabalho (e uma função correspondente) que o Transfer Family deve assumir ao executar o fluxo de trabalho. É possível escolher um fluxo de trabalho para executar em um upload completo e outro para executar em um upload parcial. Para saber mais sobre como processar seus arquivos usando fluxos de trabalho gerenciados, consulte [AWS Transfer Family fluxos de trabalho gerenciados](#).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

- c. Para Opções de algoritmo criptográfico, escolha uma política de segurança que contenha os algoritmos criptográficos habilitados para uso pelo seu servidor. Nossa política de segurança mais recente é a padrão: para obter detalhes, consulte [Políticas de segurança para AWS Transfer Family servidores](#).
- d. Em Chave do host do servidor, mantenha-a em branco.
- e. (Opcional) Em Tags, para Chave e Valor, insira uma ou mais tags como pares de valor-chave e escolha Adicionar tag.
- f. Você pode otimizar o desempenho dos seus diretórios do Amazon S3. Por exemplo, suponha que você acesse seu diretório inicial e tenha 10.000 subdiretórios. Em outras palavras, seu bucket do Amazon S3 tem 10.000 pastas. Nesse cenário, se você executar o comando `ls` (list), a operação de lista levará entre seis e oito minutos. No entanto, se você otimizar seus diretórios, essa operação levará apenas alguns segundos.

Quando você cria seu servidor usando o console, os diretórios otimizados são habilitados por padrão. Se você criar seu servidor usando a API, esse comportamento não será ativado por padrão.

Optimized Directories [Info](#)

Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

- g. Escolha Próximo.
- h. (Opcional) Você pode configurar AWS Transfer Family servidores para exibir mensagens personalizadas, como políticas organizacionais ou termos e condições, para seus usuários finais. Você também pode exibir a Mensagem do Dia (MOTD) personalizada para usuários que se autenticaram com sucesso.

Em Exibir banner, na caixa de texto Pre-authentication Exibir banner, insira a mensagem de texto que você deseja exibir para seus usuários antes da autenticação e, na caixa de texto Post-authentication Exibir banner, insira o texto que você deseja exibir para seus usuários após a autenticação bem-sucedida.

- i. (Opcional) É possível configurar as seguintes opções adicionais.
 - SetStat opção: habilite essa opção para ignorar o erro gerado quando um cliente tenta usar SETSTAT em um arquivo que você está carregando em um bucket do Amazon S3. Para obter detalhes adicionais, consulte a SetStatOption documentação no [ProtocolDetails](#) tópico.
 - Retomada da sessão TLS: fornece um mecanismo para retomar ou compartilhar uma chave secreta negociada entre o controle e a conexão de dados para uma sessão FTPS. Para obter detalhes adicionais, consulte a TlsSessionResumptionMode documentação no [ProtocolDetails](#) tópico.
 - IP Passivo: indica o modo passivo, para protocolos FTP e FTPS. Insira um único endereço IPv4, como o endereço IP público de um firewall, roteador ou balanceador de carga. Para obter detalhes adicionais, consulte a PassiveIp documentação no [ProtocolDetails](#) tópico.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. Em Revisar e criar, revise as suas escolhas.

- Se você quiser editar algum deles, escolha Editar ao lado da etapa.

 Note

Você deve revisar cada etapa após a etapa que você escolheu editar.

- Se você não tiver alterações, escolha Criar servidor para criar seu servidor. Você será direcionado à página Servidores, exibida a seguir, onde seu novo servidor estará listado.

Pode levar alguns minutos até que o status de seu novo servidor mude para Online. Nesse momento, seu servidor poderá realizar operações de arquivo para seus usuários.

Próximas etapas: Para a próxima etapa, continue em [Trabalhar com provedores de identidade personalizados](#) para configurar usuários.

Crie um FTP-enabled servidor

O Protocolo de Transferência de Arquivos (SFTP) é um protocolo de rede usado para transferência segura de dados. O FTP usa um canal separado para controle e transferência de dados. O canal de controle está aberto até ser encerrado ou até o tempo limite de inatividade. O canal de dados fica ativo durante a transferência. O FTP usa texto não criptografado e não suporta criptografia de tráfego.

Note

Ao habilitar o FTP, você deve escolher a opção de acesso interno para o VPC-hosted endpoint. Se você precisar que seu servidor tenha dados atravessando a rede pública, você deve usar protocolos seguros, como SFTP ou FTPS.

Note

Para considerações importantes sobre balanceadores de carga de rede, consulte [Evite colocar NLBs e NATs na frente de AWS Transfer Family servidores](#)

Para criar um FTP-enabled servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/> e selecione Servidores no painel de navegação e escolha Criar servidor.
2. Em Escolher protocolos, selecione FTP e escolha Avançar.
3. Em Escolher um provedor de identidade, escolha o provedor de identidade que você deseja usar para gerenciar o acesso do usuário. Você tem as seguintes opções:
 - AWS Directory Service for Microsoft Active Directory— Você fornece um Directory Service diretório para acessar o endpoint. Ao fazer isso, será possível usar credenciais armazenadas no Active Directory para autenticar seus usuários. Para saber mais sobre como trabalhar com provedores de AWS Managed Microsoft AD identidade, consulte [Usando o AWS Directory Service para o Microsoft Active Directory](#).

 Note

- Cross-Account e não há suporte para AWS Managed Microsoft AD diretórios compartilhados.
- Para configurar um servidor com o Directory Service como seu provedor de identidade, você precisa adicionar algumas Directory Service permissões. Para obter detalhes, consulte [Antes de começar a usar AWS Directory Service for Microsoft Active Directory](#).

- Provedor de identidade personalizado — Escolha uma das seguintes opções:
 - Use AWS Lambda para conectar seu provedor de identidade — Você pode usar um provedor de identidade existente, apoiado por uma função Lambda. Você fornece o nome da função do Lambda. Para obter mais informações, consulte [Usando AWS Lambda para integrar seu provedor de identidade](#).
 - Usar o Amazon API Gateway para conectar seu provedor de identidade — É possível criar um método de API Gateway apoiado por uma função do Lambda para uso como provedor de identidade. Você fornece um URL do Amazon API Gateway e um perfil de invocação. Para obter mais informações, consulte [Usando para integrar seu provedor de identidade](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

- ☐ **Service managed**
Create and manage users within the service
- ☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS
- ☒ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

- ☒ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization
- ☐ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

- ☒ Password OR public key
- ☐ Password ONLY
- ☐ Public Key ONLY
- ☐ Password AND public key

To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

- Escolha Próximo.
- Em Escolha um endpoint, faça o seguinte:

Note

Os servidores FTP do Transfer Family operam na porta 21 (canal de controle) e no intervalo de portas 8192—8200 (canal de dados).

- a. Em Tipo de endpoint, escolha Hospedado no VPC para hospedar o endpoint do seu servidor. Para obter mais informações sobre como configurar endpoint hospedado no VPC, consulte [Crie um servidor em uma VPC \(virtual private cloud\)](#).

 Note

Não há suporte para endpoints acessíveis publicamente.

- b. Para FIPS ativado, mantenha a caixa de seleção FIPS habilitado endpoint desmarcada.

 Note

FIPS-enabled endpoints não são compatíveis com servidores FTP.

- c. Escolha Próximo.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

6. Na página Escolher domínio, escolha o serviço AWS de armazenamento que você deseja usar para armazenar e acessar seus dados pelo protocolo selecionado.
- Escolha o Amazon S3 para armazenar e acessar seus arquivos como objetos no protocolo selecionado.
 - Escolha o Amazon EFS para armazenar e acessar seus arquivos em seu sistema de arquivos Amazon EFS usando o protocolo selecionado.

Escolha Próximo.

7. Em Configuração de detalhes adicionais, faça o seguinte:

- a. Para registro em log, especifique um grupo de logs existente ou crie um novo (a opção padrão).

The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains a 'Logging' section. Under 'Log group', it instructs to 'Choose the CloudWatch log group where your events will be delivered in a structured JSON format'. There are two radio buttons: 'Create a new log group' (unselected) and 'Choose an existing log group' (selected). Below the radio buttons is a text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. Under 'Logging role', it instructs to 'Choose the IAM role that will be used to deliver events to your CloudWatch logs'. There are two radio buttons: 'Create a new role' (unselected) and 'Choose an existing role' (unselected). At the bottom, a blue information box states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Se você escolher Criar grupo de registros, o CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) abrirá a página Criar grupo de registros. Para obter detalhes, consulte [Criar um grupo de CloudWatch registros em Registros](#).

- b. (Opcional) Para Fluxos de trabalho gerenciados, escolha IDs de fluxo de trabalho (e uma função correspondente) que o Transfer Family deve assumir ao executar o fluxo de trabalho. É possível escolher um fluxo de trabalho para executar em um upload completo e outro para executar em um upload parcial. Para saber mais sobre como processar seus arquivos usando fluxos de trabalho gerenciados, consulte [AWS Transfer Family fluxos de trabalho gerenciados](#).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

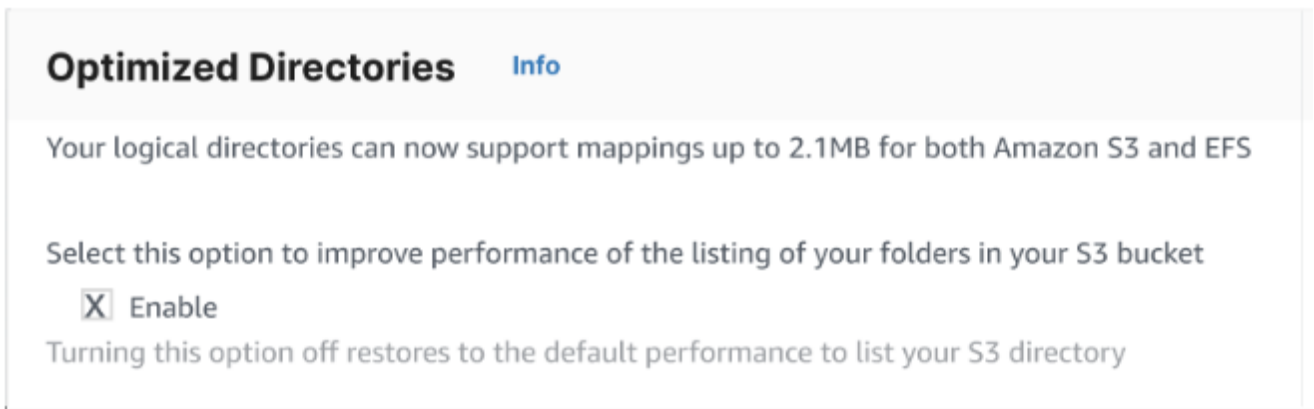
- c. Para Opções de algoritmo criptográfico, escolha uma política de segurança que contenha os algoritmos criptográficos habilitados para uso pelo seu servidor.

Note

O Transfer Family atribui a política de segurança mais recente ao seu servidor FTP. No entanto, como o protocolo FTP não usa criptografia, os servidores FTP não usam nenhum dos algoritmos de política de segurança. A menos que seu servidor também use o protocolo FTPS ou SFTP, a política de segurança permanece sem uso.

- d. Em Chave do host do servidor, mantenha-a em branco.
- e. (Opcional) Em Tags, para Chave e Valor, insira uma ou mais tags como pares de valor-chave e escolha Adicionar tag.
- f. Você pode otimizar o desempenho dos seus diretórios do Amazon S3. Por exemplo, suponha que você acesse seu diretório inicial e tenha 10.000 subdiretórios. Em outras palavras, seu bucket do Amazon S3 tem 10.000 pastas. Nesse cenário, se você executar o comando `ls` (list), a operação de lista levará entre seis e oito minutos. No entanto, se você otimizar seus diretórios, essa operação levará apenas alguns segundos.

Quando você cria seu servidor usando o console, os diretórios otimizados são habilitados por padrão. Se você criar seu servidor usando a API, esse comportamento não será ativado por padrão.



- g. Escolha Próximo.
- h. (Opcional) Você pode configurar AWS Transfer Family servidores para exibir mensagens personalizadas, como políticas organizacionais ou termos e condições, para seus usuários finais. Você também pode exibir a Mensagem do Dia (MOTD) personalizada para usuários que se autenticaram com sucesso.

Em Exibir banner, na caixa de texto Pre-authentication Exibir banner, insira a mensagem de texto que você deseja exibir para seus usuários antes da autenticação e, na caixa de texto Post-authentication Exibir banner, insira o texto que você deseja exibir para seus usuários após a autenticação bem-sucedida.

- i. (Opcional) É possível configurar as seguintes opções adicionais.
- SetStat opção: habilite essa opção para ignorar o erro gerado quando um cliente tenta usar SETSTAT em um arquivo que você está carregando em um bucket do Amazon S3. Para obter detalhes adicionais, consulte a SetStatOption documentação no [ProtocolDetails](#)tópico.
 - Retomada da sessão TLS: fornece um mecanismo para retomar ou compartilhar uma chave secreta negociada entre o controle e a conexão de dados para uma sessão FTPS. Para obter detalhes adicionais, consulte a TlsSessionResumptionMode documentação no [ProtocolDetails](#)tópico.
 - IP Passivo: indica o modo passivo, para protocolos FTP e FTPS. Insira um único endereço IPv4, como o endereço IP público de um firewall, roteador ou balanceador de carga. Para obter detalhes adicionais, consulte a PassiveIp documentação no [ProtocolDetails](#)tópico.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. Em Revisar e criar, revise as suas escolhas.

- Se você quiser editar algum deles, escolha Editar ao lado da etapa.

 Note

Você deve revisar cada etapa após a etapa que você escolheu editar.

- Se você não tiver alterações, escolha Criar servidor para criar seu servidor. Você será direcionado à página Servidores, exibida a seguir, onde seu novo servidor estará listado.

Pode levar alguns minutos até que o status de seu novo servidor mude para Online. Nesse momento, seu servidor poderá realizar operações de arquivo para seus usuários.

Próximas etapas - Para a próxima etapa, continue em [Trabalhar com provedores de identidade personalizados](#) para configurar usuários.

Crie um servidor em uma VPC (virtual private cloud).

Você pode hospedar o endpoint do seu servidor em uma nuvem privada virtual (VPC) para usar na transferência de dados de e para um bucket do Amazon S3 ou arquivo do Amazon EFS sem usar a internet pública.

Note

Depois de 19 de maio de 2021, você não poderá criar um servidor usando `EndpointType=VPC_ENDPOINT` sua AWS conta se ela ainda não tiver feito isso antes de 19 de maio de 2021. Se você já criou servidores `EndpointType=VPC_ENDPOINT` em sua AWS conta em ou antes de 21 de fevereiro de 2021, você não será afetado. Após essa data, use `EndpointType=VPC`. Para obter mais informações, consulte [the section called “Interromper o uso do VPC_ENDPOINT”](#).

Se você usa a Amazon Virtual Private Cloud (Amazon VPC) para hospedar seus AWS recursos, você pode estabelecer uma conexão privada entre sua VPC e um servidor. Você pode usar esse servidor em seguida para transferir dados do seu cliente de e para o bucket do Amazon S3 sem usar endereçamento IP público ou exigir um gateway da internet.

Usando o Amazon VPC, você pode lançar AWS recursos em uma rede virtual personalizada. Você pode usar uma VPC para controlar as configurações de rede, como o intervalo de endereços IP, sub-redes, tabelas de rotas e gateways de rede. Para obter mais informações sobre VPC, consulte [O que é a VPC da Amazon?](#) no Guia do usuário da VPC da Amazon .

Na próxima seção, você pode encontrar instruções sobre como conectar sua VPC a um servidor. Como visão geral, você faz isso da seguinte maneira:

1. Configure um servidor usando um endpoint da VPC.
2. Conecte-se ao seu servidor usando um cliente que está dentro da sua VPC, por meio do endpoint da VPC. Isso permite que você transfira dados que estão armazenados em seu bucket do Amazon S3 pelo seu cliente usando AWS Transfer Family. Você pode realizar essa transferência mesmo que a rede esteja desconectada da internet pública.
3. Além disso, se você optar por tornar o endpoint do seu servidor voltado para a Internet, poderá associar endereços IP elásticos ao seu endpoint. Isso permite que clientes fora da sua VPC se conectem ao seu servidor. Você pode usar grupos de segurança da VPC para controlar o acesso a usuários autenticados cujas solicitações são originadas apenas de endereços permitidos.

 Note

AWS Transfer Family suporta endpoints de pilha dupla, permitindo que seu servidor se comunique por IPv4 e IPv6. Para ativar o suporte de pilha dupla, selecione a opção Ativar endpoint de pilha dupla de DNS ao criar seu VPC endpoint. Observe que tanto a VPC quanto as sub-redes devem ser configuradas para suportar IPv6 antes que você possa usar esse recurso. Dual-stack o suporte é particularmente útil quando você tem clientes que precisam se conectar usando qualquer um dos protocolos.

Para obter informações sobre endpoints de servidor de pilha dupla (IPv4 e IPv6), consulte [Suporte IPv6 para servidores Transfer Family](#)

Tópicos

- [Crie um endpoint de servidor que possa ser acessado apenas em sua VPC](#)
- [Criar um endpoint voltado para a internet para seu servidor](#)
- [Altere o tipo de endpoint para o seu servidor](#)
- [Interromper o uso do VPC_ENDPOINT](#)
- [Limitando o acesso ao VPC endpoint para servidores Transfer Family](#)
- [Recursos adicionais de rede](#)
- [Atualização do tipo de endpoint AWS Transfer Family do servidor de VPC_ENDPOINT para VPC](#)

Crie um endpoint de servidor que possa ser acessado apenas em sua VPC

No procedimento a seguir, você cria um endpoint de servidor acessível apenas aos recursos dentro da sua VPC.

Para criar um endpoint de servidor dentro de uma VPC

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores e escolha Criar servidor.
3. Em Escolher protocolos, selecione um ou mais protocolos e escolha Avançar. Para obter mais informações sobre protocolos, consulte [Etapa 2: criar um SFTP-enabled servidor](#).
4. Em Escolher um provedor de identidade, escolha Serviço gerenciado para armazenar identidades e chaves de usuário e AWS Transfer Family, em seguida, escolha Avançar.

Este procedimento usa a opção gerenciada por serviço. Se escolher Personalizado, você fornecerá um endpoint do Amazon API Gateway e um perfil (IAM) do AWS Identity and Access Management para acessar o endpoint. Ao fazer isso, você poderá integrar seu serviço de diretório para autenticar e autorizar seus usuários. Para saber mais sobre como trabalhar com provedores de identidade personalizada, consulte [Trabalhar com provedores de identidade personalizados](#).

5. Em Escolha um endpoint, faça o seguinte:

- a. Em Tipo de endpoint, escolha o tipo de endpoint Hospedado em VPC para hospedar o endpoint do seu servidor.
- b. Em Acesso, escolha Interno para tornar seu endpoint acessível apenas aos clientes que usam os endereços IP privados do endpoint.

Para obter detalhes sobre a opção Voltado para a internet, consulte [Criar um endpoint voltado para a internet para seu servidor](#). Um servidor que é criado em uma VPC para acesso interno não oferece suporte a nomes de host personalizados.

- c. Para VPC, escolha um ID da VPC existente ou escolha Criar uma VPC para criar uma nova VPC.
- d. Na seção Zonas de disponibilidade, escolha até três Zonas de Disponibilidade e sub-redes associadas.
- e. Na seção Grupos de segurança, escolha uma ou mais IDs de grupo de segurança existentes ou escolha Criar um grupo de segurança para criar um grupo de segurança. Para obter mais informações sobre grupos de segurança da VPC, consulte [Grupos de segurança](#) no Guia do usuário da Amazon Virtual Private Cloud. Para criar um grupo de segurança, consulte [Criando um grupo de segurança](#) no Guia do usuário da Amazon Virtual Private Cloud.

 Note

Sua VPC vem automaticamente com um grupo de segurança padrão. Se você não especificar um grupo de segurança ou grupos diferentes ao lançar o servidor, associaremos o grupo de segurança padrão ao seu servidor.

- Para as regras de entrada do grupo de segurança, você pode configurar o tráfego SSH para usar as portas 22, 2222, 22000 ou qualquer combinação. A porta 22 é configurada

por padrão. Para usar a porta 2222 ou a porta 22000, você adiciona uma regra de entrada ao seu grupo de segurança. Para o tipo, escolha TCP personalizado e, em seguida, insira um **2222** ou **22000** para Intervalo de portas e, para a origem, insira o mesmo intervalo CIDR que você tem para sua regra de porta SSH 22.

- Para as regras de entrada do grupo de segurança, configure o tráfego FTP e FTPS para usar o intervalo de portas para o canal de controle e **21 8192-8200** para o canal de dados.

 Note

Você também pode usar a porta 2223 para clientes que precisam de ACKs TCP “piggy-back” ou a capacidade do pacote final do handshake tridirecional TCP também conter dados.

Alguns softwares cliente podem ser incompatíveis com a porta 2223: por exemplo, um cliente que exige que o servidor envie a string de identificação SFTP antes que o cliente o faça.

[VPC](#) > [Security Groups](#) > [sg-\[redacted\]-default](#) > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- f. (Opcional) Para FIPS ativado, marque a caixa de seleção Endpoint habilitado para FIPS para assegurar que o endpoint esteja em conformidade com os Padrões Federais de Processamento de Informações (FIPS).

 Note

FIPS-enabled endpoints estão disponíveis somente nas AWS regiões da América do Norte. Para saber as regiões disponíveis, consulte [Endpoints e cotas do AWS Transfer Family](#) em Referência geral da AWS. Para obter mais informações, consulte [FIPS – Padrão federal de processamento de informações 140-2](#).

- g. Escolha Próximo.
6. Em Configuração adicional, faça o seguinte:
 - a. Para CloudWatch registrar, escolha uma das seguintes opções para permitir que a Amazon CloudWatch registre sua atividade de usuário:
 - Crie uma nova função para permitir que o Transfer Family crie automaticamente o perfil do IAM, desde que você tenha as permissões certas para criar uma nova função. O perfil do IAM criado é chamado `AWSTransferLoggingAccess`.
 - Escolha a partir de uma função existente para selecionar um perfil do IAM existente da sua conta. Em Função de registro em log, escolha a função. Esse perfil do IAM deve incluir uma política de confiança com o Serviço definido como `transfer.amazonaws.com`.

Para obter mais informações sobre CloudWatch registro em log, consulte [Configurar função de CloudWatch registro](#).

 Note

- Você não pode ver a atividade do usuário final CloudWatch se não especificar uma função de registro.
- Se você não quiser configurar uma função de CloudWatch registro, selecione Escolher uma função existente, mas não selecione uma função de registro.

- b. Para Opções de algoritmo criptográfico, escolha uma política de segurança que contenha os algoritmos criptográficos habilitados para uso pelo seu servidor.

 Note

Por padrão, a política de segurança do `TransferSecurityPolicy-2024-01` é anexada ao seu servidor, a menos que você escolha uma diferente.

Para obter mais informações sobre as políticas de segurança, consulte [Políticas de segurança para AWS Transfer Family servidores](#).

- c. (Opcional: esta seção é somente para migrar usuários de um SFTP-enabled servidor existente.) Em Chave de host do servidor, insira uma chave privada RSA, ED25519 ou ECDSA que será usada para identificar seu servidor quando os clientes se conectarem a ele por SFTP.
 - d. (Opcional) Em Tags, para Chave e Valor, insira uma ou mais tags como pares de valor-chave e escolha Adicionar tag.
 - e. Escolha Próximo.
7. Em Revisar e criar, revise as suas escolhas. Se você:
- Se você quiser editar algum deles, escolha Editar ao lado da etapa.

 Note

Você deve revisar cada etapa após a etapa que você escolheu editar.

- Se você não tiver alterações, escolha Criar servidor para criar seu servidor. Você será direcionado à página Servidores, exibida a seguir, onde seu novo servidor estará listado.

Pode levar alguns minutos até que o status de seu novo servidor mude para Online. Nesse ponto, seu servidor pode realizar operações com arquivos, mas primeiro você precisa criar um usuário. Para obter detalhes sobre a criação de usuários, consulte [Gerenciando usuários para endpoints de servidor](#).

Criar um endpoint voltado para a internet para seu servidor

No procedimento a seguir, crie um endpoint do servidor. Esse endpoint pode ser acessado pela internet apenas para clientes cujos endereços IP de origem são permitidos no grupo de segurança padrão da sua VPC. Além disso, ao usar endereços IP elásticos para tornar seu endpoint voltado

para a internet, seus clientes podem usar o endereço IP elástico para permitir acesso ao seu endpoint em seus firewalls.

 Note

Apenas SFTP e FTPS podem ser usados em um endpoint hospedado em uma VPC voltado para a internet.

Para criar um endpoint voltado para a internet

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores e escolha Criar servidor.
3. Em Escolher protocolos, selecione um ou mais protocolos e escolha Avançar. Para obter mais informações sobre protocolos, consulte [Etapa 2: criar um SFTP-enabled servidor](#).
4. Em Escolher um provedor de identidade, escolha Serviço gerenciado para armazenar identidades e chaves de usuário e AWS Transfer Family, em seguida, escolha Avançar.

Este procedimento usa a opção gerenciada por serviço. Se escolher Personalizado, você fornecerá um endpoint do Amazon API Gateway e um perfil (IAM) do AWS Identity and Access Management para acessar o endpoint. Ao fazer isso, você poderá integrar seu serviço de diretório para autenticar e autorizar seus usuários. Para saber mais sobre como trabalhar com provedores de identidade personalizada, consulte [Trabalhar com provedores de identidade personalizados](#).

5. Em Escolha um endpoint, faça o seguinte:
 - a. Em Tipo de endpoint, escolha o tipo de endpoint Hospedado em VPC para hospedar o endpoint do seu servidor.
 - b. Em Acesso, escolha Voltado para a internet para tornar seu endpoint acessível aos clientes pela internet.

 Note

Ao escolher Voltado para a internet, você pode escolher um endereço IP elástico existente em cada sub-rede ou sub-redes. Ou você pode acessar o console VPC (<https://console.aws.amazon.com/vpc/>) para alocar um ou mais novos endereços IP elásticos. Esses endereços podem ser de sua propriedade AWS ou de sua

propriedade. Você não pode associar endereços IP elásticos que já estão em uso com seu endpoint.

- c. (Opcional) Em Nome de host personalizado, escolha uma das seguintes:

 Note

Clientes que AWS GovCloud (US) precisam se conectar diretamente por meio do endereço IP elástico ou criar um registro de nome de host no Commercial Route 53 que aponte para seu EIP. Para obter mais informações sobre o uso do Route 53 para GovCloud endpoints, consulte [Configurando o Amazon Route 53 com seus AWS GovCloud \(US\) recursos](#) no Guia do AWS GovCloud (US) usuário.

- Alias de DNS do Amazon Route 53 — se o nome do host que você deseja usar estiver registrado no Route 53. Em seguida, você pode inserir o nome do host.
- Outro DNS - se o nome do host que você deseja usar estiver registrado em outro provedor DNS. Em seguida, você pode inserir o nome do host.
- Nenhum - para usar o endpoint do servidor e não um nome de host personalizado. O nome do host do servidor tem a forma de `server-id.server.transfer.region.amazonaws.com`.

 Note

Para clientes em AWS GovCloud (US), selecionar Nenhum não cria um nome de host nesse formato.

Para saber mais sobre como trabalhar com nomes de host personalizados, consulte [Trabalhar com nomes de host personalizados](#).

- d. Para VPC, escolha um ID da VPC existente ou escolha Criar uma VPC para criar uma nova VPC.
- e. Na seção Zonas de disponibilidade, escolha até três Zonas de Disponibilidade e sub-redes associadas. Para Endereços IPv4, escolha um Endereço IP elástico para cada sub-rede. Esse é o endereço IP que seus clientes podem usar para permitir o acesso ao seu endpoint em seus firewalls.

Dica: você deve usar uma sub-rede pública para suas zonas de disponibilidade ou primeiro configurar um gateway de internet se quiser usar uma sub-rede privada.

- f. Na seção Grupos de segurança, escolha uma ou mais IDs de grupo de segurança existentes ou escolha Criar um grupo de segurança para criar um grupo de segurança. Para obter mais informações sobre grupos de segurança da VPC, consulte [Grupos de segurança](#) no Guia do usuário da Amazon Virtual Private Cloud. Para criar um grupo de segurança, consulte [Criando um grupo de segurança](#) no Guia do usuário da Amazon Virtual Private Cloud.

 Note

Sua VPC vem automaticamente com um grupo de segurança padrão. Se você não especificar um grupo de segurança ou grupos diferentes ao lançar o servidor, associaremos o grupo de segurança padrão ao seu servidor.

- Para as regras de entrada do grupo de segurança, você pode configurar o tráfego SSH para usar as portas 22, 2222, 22000 ou qualquer combinação. A porta 22 é configurada por padrão. Para usar a porta 2222 ou a porta 22000, você adiciona uma regra de entrada ao seu grupo de segurança. Para o tipo, escolha TCP personalizado e, em seguida, insira um **2222** ou **22000** para Intervalo de portas e, para a origem, insira o mesmo intervalo CIDR que você tem para sua regra de porta SSH 22.
- Para as regras de entrada do grupo de segurança, configure o tráfego FTPS para usar o intervalo de portas **21** para o canal de controle e **8192-8200** para o canal de dados.

 Note

Você também pode usar a porta 2223 para clientes que precisam de ACKs TCP “piggy-back” ou a capacidade do pacote final do handshake tridirecional TCP também conter dados.

Alguns softwares cliente podem ser incompatíveis com a porta 2223: por exemplo, um cliente que exige que o servidor envie a string de identificação SFTP antes que o cliente o faça.

[VPC](#) > [Security Groups](#) > [sg-\[redacted\]-default](#) > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- g. (Opcional) Para FIPS ativado, marque a caixa de seleção Endpoint habilitado para FIPS para assegurar que o endpoint esteja em conformidade com os Padrões Federais de Processamento de Informações (FIPS).

 Note

FIPS-enabled os endpoints estão disponíveis somente nas AWS regiões da América do Norte. Para saber as regiões disponíveis, consulte [Endpoints e cotas do AWS Transfer Family](#) em Referência geral da AWS. Para obter mais informações, consulte [FIPS – Padrão federal de processamento de informações 140-2](#).

h. Escolha Próximo.

6. Em Configuração adicional, faça o seguinte:

a. Para CloudWatch registrar, escolha uma das seguintes opções para permitir que a Amazon CloudWatch registre sua atividade de usuário:

- Crie uma nova função para permitir que o Transfer Family crie automaticamente o perfil do IAM, desde que você tenha as permissões certas para criar uma nova função. O perfil do IAM criado é chamado `AWSTransferLoggingAccess`.
- Escolha a partir de uma função existente para selecionar um perfil do IAM existente da sua conta. Em Função de registro em log, escolha a função. Esse perfil do IAM deve incluir uma política de confiança com o Serviço definido como `transfer.amazonaws.com`.

Para obter mais informações sobre CloudWatch registro em log, consulte [Configurar função de CloudWatch registro](#).

 Note

- Você não pode ver a atividade do usuário final CloudWatch se não especificar uma função de registro.
- Se você não quiser configurar uma função de CloudWatch registro, selecione Escolher uma função existente, mas não selecione uma função de registro.

b. Para Opções de algoritmo criptográfico, escolha uma política de segurança que contenha os algoritmos criptográficos habilitados para uso pelo seu servidor.

Note

Por padrão, a política de segurança do `TransferSecurityPolicy-2024-01` é anexada ao seu servidor, a menos que você escolha uma diferente.

Para obter mais informações sobre as políticas de segurança, consulte [Políticas de segurança para AWS Transfer Family servidores](#).

- c. (Opcional: esta seção é somente para migrar usuários de um SFTP-enabled servidor existente.) Em Chave de host do servidor, insira uma chave privada RSA, ED25519 ou ECDSA que será usada para identificar seu servidor quando os clientes se conectarem a ele por SFTP.
- d. (Opcional) Em Tags, para Chave e Valor, insira uma ou mais tags como pares de valor-chave e escolha Adicionar tag.
- e. Escolha Próximo.
- f. (Opcional) Para Fluxos de trabalho gerenciados, escolha IDs de fluxo de trabalho (e uma função correspondente) que o Transfer Family deve assumir ao executar o fluxo de trabalho. É possível escolher um fluxo de trabalho para executar em um upload completo e outro para executar em um upload parcial. Para saber mais sobre como processar seus arquivos usando fluxos de trabalho gerenciados, consulte [AWS Transfer Family fluxos de trabalho gerenciados](#).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

W- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

W- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

7. Em Revisar e criar, revise as suas escolhas. Se você:

- Se você quiser editar algum deles, escolha Editar ao lado da etapa.

 Note

Você deve revisar cada etapa após a etapa que você escolheu editar.

- Se você não tiver alterações, escolha Criar servidor para criar seu servidor. Você será direcionado à página Servidores, exibida a seguir, onde seu novo servidor estará listado.

Você pode escolher o ID do servidor para consultar as configurações detalhadas do servidor que acabou de criar. Depois que a coluna Endereço IPv4 público for preenchida, os endereços IP elásticos que você forneceu serão associados com sucesso ao endpoint do seu servidor.

 Note

Quando seu servidor em uma VPC está on-line, somente as sub-redes podem ser modificadas e somente por meio da API. [UpdateServer](#) Você deve [parar o servidor](#) para adicionar ou alterar os endereços IP elásticos do endpoint do servidor.

Altere o tipo de endpoint para o seu servidor

Se você tem um servidor existente que pode ser acessado pela Internet (ou seja, tem um tipo de endpoint público), pode alterar o endpoint para um endpoint da VPC.

 Note

Se você tiver um servidor existente em uma VPC exibido como VPC_ENDPOINT, recomendamos modificá-lo para o novo tipo de endpoint da VPC. Com esse novo tipo de endpoint, você não precisa mais usar um Network Load Balancer (NLB) para associar endereços IP elásticos ao endpoint do seu servidor. Além disso, você pode usar grupos de segurança da VPC para restringir o acesso ao endpoint do seu servidor. No entanto, você pode continuar a usar o tipo de endpoint VPC_ENDPOINT conforme necessário.

O procedimento a seguir pressupõe que você tenha um servidor que usa o tipo de endpoint público atual ou o tipo VPC_ENDPOINT mais antigo.

Para alterar o tipo de endpoint para o seu servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores.
3. Marque a caixa de seleção da predefinição do servidor no qual você deseja alterar o tipo de endpoint.

 Important

Você deve interromper o servidor antes de alterar o endpoint.

4. Em Ações, escolha Interromper.
5. Na caixa de diálogo de confirmação exibida, escolha Parar para confirmar que quer interromper o servidor.

 Note

Antes de prosseguir para a próxima etapa, em Detalhes do endpoint, aguarde até que o Status do servidor mude para Offline; isso pode levar alguns minutos. Talvez você precise selecionar Atualizar na página dos Servidores para ver a alteração de status. Não será possível fazer edições até que o servidor esteja Offline.

6. Em Detalhes do endpoint, escolha Editar.
7. Em Editar configuração do endpoint, faça o seguinte:
 - a. Para Tipo de endpoint, selecione hospedado na VPC.
 - b. Para Ações, escolha uma das seguinte opções:
 - Interno para tornar seu endpoint acessível apenas aos clientes que usam os endereços IP privados do endpoint.
 - Voltado para a internet para tornar seu endpoint acessível aos clientes pela internet pública.

 Note

Ao escolher Voltado para a internet, você pode escolher um endereço IP elástico existente em cada sub-rede ou sub-redes. Ou você pode acessar o console da VPC (<https://console.aws.amazon.com/vpc/>) para alocar um ou mais novos

endereços IP elásticos. Esses endereços podem ser de sua propriedade AWS ou de sua propriedade. Você não pode associar endereços IP elásticos que já estão em uso com seu endpoint.

- c. (Opcional somente para acesso voltado para a Internet) Em Nome de host personalizado, escolha uma das seguintes opções:

- Alias de DNS do Amazon Route 53 — se o nome do host que você deseja usar estiver registrado no Route 53. Em seguida, você pode inserir o nome do host.
- Outro DNS - se o nome do host que você deseja usar estiver registrado em outro provedor DNS. Em seguida, você pode inserir o nome do host.
- Nenhum - para usar o endpoint do servidor e não um nome de host personalizado. O nome do host do servidor tem a forma de `serverId.server.transfer.regionId.amazonaws.com`.

Para saber mais sobre como trabalhar com nomes de host personalizados, consulte [Trabalhar com nomes de host personalizados](#).

- d. Para VPC, escolha um ID da VPC existente ou escolha Criar uma VPC para criar uma nova VPC.
- e. Na seção Zonas de disponibilidade, escolha até três Zonas de Disponibilidade e sub-redes associadas. Se a opção Voltado para a internet for escolhida, escolha também um endereço IP elástico para cada sub-rede.

 Note

Se você quiser o máximo de três zonas de disponibilidade, mas não houver disponibilidade suficiente, crie-as no console VPC () <https://console.aws.amazon.com/vpc/>.

Se você modificar as sub-redes ou os endereços IP elásticos, o servidor levará alguns minutos para ser atualizado. Você não pode salvar suas alterações até que a atualização do servidor seja concluída.

- f. Escolha Salvar.
8. Em Ações, escolha Iniciar e aguarde até que o status do servidor mude para Online; isso pode levar alguns minutos.

 Note

Se você alterou um tipo de endpoint público para um tipo de endpoint da VPC, observe que o Tipo de endpoint do seu servidor mudou para VPC.

O grupo de segurança padrão é anexado ao endpoint. Para alterar ou adicionar outros grupos de segurança, consulte [Criar grupos de segurança](#).

Interromper o uso do VPC_ENDPOINT

AWS Transfer Family interrompeu a capacidade de criar servidores com quatro EndpointType=VPC_ENDPOINT novas AWS contas. A partir de 19 de maio de 2021, AWS contas que não possuem AWS Transfer Family servidores com um tipo de endpoint não VPC_ENDPOINT poderão criar novos servidores com EndpointType=VPC_ENDPOINT. Se você já é proprietário de servidores que usam o tipo de endpoint VPC_ENDPOINT, recomendamos que você comece a usar o EndpointType=VPC o mais rápido possível. Para obter detalhes, consulte [Atualizar o tipo de endpoint AWS Transfer Family do servidor de VPC_ENDPOINT para VPC](#).

Lançamos o novo tipo de endpoint VPC no início de 2020. Para obter mais informações, consulte [AWS Transfer Family para SFTP oferece suporte a grupos de segurança de VPC e endereços IP elásticos](#). Esse novo endpoint é mais rico em recursos e econômico, além de não PrivateLink cobrar nada. Para obter mais informações, consulte [Preços do AWS PrivateLink](#).

Esse tipo de endpoint é funcionalmente equivalente ao tipo de endpoint anterior (VPC_ENDPOINT). Você pode anexar endereços IP elásticos diretamente ao endpoint para torná-lo voltado para a internet e usar grupos de segurança para filtragem de IP de origem. Para obter mais informações, consulte a postagem do blog [Use IP allow to protect your AWS Transfer Family for SFTP servers](#).

Você também pode hospedar esse endpoint em um ambiente VPC compartilhado. Para obter mais informações, consulte [AWS Transfer Family agora oferece suporte a ambientes VPC de serviços compartilhados](#).

Além do SFTP, você pode usar a VPC EndpointType para habilitar FTPS e FTP. Não planejamos adicionar esses recursos e FTPS/FTP suporte ao EndpointType=VPC_ENDPOINT. Também removemos esse tipo de endpoint como uma opção do AWS Transfer Family console.

Você pode alterar o tipo de endpoint do seu servidor usando o console Transfer Family, API AWS CLI, SDKs ou CloudFormation. Para alterar o tipo de endpoint do seu servidor, consulte [Atualização do tipo de endpoint AWS Transfer Family do servidor de VPC_ENDPOINT para VPC](#).

Se você tiver alguma dúvida, entre em contato com AWS Support nossa equipe de AWS contas.

 Note

Não planejamos adicionar esses recursos e suporte a FTPS ou FTP ao VPC_ENDPOINT. EndpointType Não estamos mais oferecendo isso como uma opção no console do AWS Transfer Family .

Se você tiver outras dúvidas, entre em contato conosco por meio da AWS Support equipe de sua conta.

Limitando o acesso ao VPC endpoint para servidores Transfer Family

Ao criar um AWS Transfer Family servidor com o tipo de endpoint VPC, seus usuários e diretores do IAM precisam de permissões para criar e excluir endpoints de VPC. No entanto, as políticas de segurança da sua organização podem restringir essas permissões. Você pode usar políticas do IAM para permitir a criação e exclusão de endpoints VPC especificamente para Transfer Family, mantendo as restrições para outros serviços.

 Important

A política do IAM a seguir permite que os usuários criem e excluam VPC endpoints somente para servidores Transfer Family, enquanto negam essas operações para outros serviços:

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource": ["*"],
  "Condition": {
    "ForAnyValue:StringNotLike": {
```

```

        "ec2:VpceServiceName": [
            "com.amazonaws.INPUT-YOUR-REGION.transfer.server.*"
        ],
        "StringNotLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/INPUT-YOUR-ROLE"
            ]
        }
    }
}

```

INPUT-YOUR-REGION Substitua por sua AWS região (por exemplo, **us-east-1**) e *INPUT-YOUR-ROLE* pela função do IAM à qual você deseja conceder essas permissões.

Recursos adicionais de rede

AWS Transfer Family fornece vários recursos avançados de rede que aprimoram a segurança e a flexibilidade ao usar configurações de VPC:

- Suporte ao ambiente VPC compartilhado — você pode hospedar seu endpoint do servidor Transfer Family em um ambiente VPC compartilhado. Para obter mais informações, consulte Como [usar endpoints hospedados em VPC em VPCs compartilhadas](#) com AWS Transfer Family
- Autenticação e segurança - Você pode usar um AWS Web Application Firewall para proteger seu endpoint do Amazon API Gateway. Para obter mais informações, consulte [Segurança AWS Transfer Family com o AWS Web Application Firewall e o Amazon API Gateway](#).

Atualização do tipo de endpoint AWS Transfer Family do servidor de VPC_ENDPOINT para VPC

Você pode usar a Console de gerenciamento da AWS, CloudFormation, ou a API Transfer Family para atualizar a API de um servidor EndpointType de VPC_ENDPOINT para VPC. Procedimentos detalhados e exemplos para usar cada um desses métodos para atualizar um tipo de endpoint de servidor são apresentados nas seções a seguir. Se você tiver servidores em várias AWS regiões e em várias AWS contas, poderá usar o script de exemplo fornecido na seção a seguir, com modificações, para identificar servidores usando o VPC_ENDPOINT tipo que você precisará atualizar.

Tópicos

- [Identificação de servidores usando o tipo de endpoint VPC_ENDPOINT](#)

- [Atualizando o tipo de endpoint do servidor usando o Console de gerenciamento da AWS](#)
- [Atualizando o tipo de endpoint do servidor usando CloudFormation](#)
- [Atualizando o servidor EndpointType usando a API](#)

Identificação de servidores usando o tipo de endpoint **VPC_ENDPOINT**

Você pode identificar quais servidores estão usando o VPC_ENDPOINT com o Console de gerenciamento da AWS.

Para identificar servidores usando o tipo de endpoint **VPC_ENDPOINT** usando o console

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. Escolha Servidores no painel de navegação para exibir a lista de servidores em sua conta nessa Região.
3. Classifique a lista de servidores pelo Tipo de endpoint para ver todos os servidores usando VPC_ENDPOINT.

Para identificar servidores **VPC_ENDPOINT** em várias AWS regiões e contas

Se você tiver servidores em várias AWS regiões e em várias AWS contas, poderá usar o script de exemplo a seguir, com modificações, para identificar servidores usando o tipo de VPC_ENDPOINT endpoint. O script de exemplo usa o Amazon EC2 [DescribeRegions](#) e as operações da [ListServers](#) API Transfer Family. Se você tiver muitas contas da AWS, poderá percorrê-las usando um perfil do IAM com acesso de auditor somente de leitura se você se autenticar usando perfis de sessão no seu provedor de identidade.

1. Veja a seguir um exemplo simples.

```
import boto3

profile = input("Enter the name of the AWS account you'll be working in: ")
session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2")

regions = ec2.describe_regions()

for region in regions['Regions']:
```

```
region_name = region['RegionName']
if region_name=='ap-northeast-3': #https://github.com/boto/boto3/issues/1943
    continue
transfer = session.client("transfer", region_name=region_name)
servers = transfer.list_servers()
for server in servers['Servers']:
    if server['EndpointType']=='VPC_ENDPOINT':
        print(server['ServerId'], region_name)
```

2. Depois que você tiver a lista dos servidores a serem atualizados, poderá usar um dos métodos descritos nas seções a seguir para atualizar o EndpointType para VPC.

Atualizando o tipo de endpoint do servidor usando o Console de gerenciamento da AWS

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores.
3. Marque a caixa de seleção da predefinição do servidor no qual você deseja alterar o tipo de endpoint.



Important

Você deve interromper o servidor antes de alterar o endpoint.

4. Em Ações, escolha Interromper.
5. Na caixa de diálogo de confirmação exibida, escolha Parar para confirmar que quer interromper o servidor.



Note

Antes de prosseguir para a próxima etapa, aguarde até que o Status do servidor mude para Offline; isso pode levar alguns minutos. Talvez você precise selecionar Atualizar na página dos Servidores para ver a alteração de status.

6. Depois que o status mudar para Offline, escolha o servidor para exibir a página de detalhes do servidor.
7. Na seção Detalhes do endpoint, escolha Editar.
8. Escolha VPC hospedada para o Tipo de endpoint.
9. Escolha Salvar.

10. Em Ações, escolha Iniciar e aguarde até que o status do servidor mude para Online; isso pode levar alguns minutos.

Atualizando o tipo de endpoint do servidor usando CloudFormation

Esta seção descreve como usar CloudFormation para atualizar um servidor EndpointType paraVPC. Use esse procedimento para os servidores Transfer Family que você implantou usando CloudFormation. Neste exemplo, o modelo de CloudFormation original usado para implantar o servidor do Transfer Family é mostrado a seguir:

```
AWS::Template::FormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC_ENDPOINT endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
      EndpointDetails:
        VpcEndpointId: !Ref VPCEndpoint
      EndpointType: VPC_ENDPOINT
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
  VPCEndpoint:
    Type: AWS::EC2::VPCEndpoint
    Properties:
      ServiceName: com.amazonaws.us-east-1.transfer.server
      SecurityGroupIds:
        - !Ref SecurityGroupId
      SubnetIds:
        - !Select [0, !Ref SubnetIds]
        - !Select [1, !Ref SubnetIds]
        - !Select [2, !Ref SubnetIds]
      VpcEndpointType: Interface
      VpcId: !Ref VpcId
```

O modelo é atualizado com as seguintes alterações:

- O `EndpointType` foi alterado para VPC.
- O recurso `AWS::EC2::VPCEndpoint` foi removido.
- O `SecurityGroupId`, o `SubnetIds` e o `VpcId` foram movidos para a seção `EndpointDetails` do recurso `AWS::Transfer::Server`,
- A propriedade `VpcEndpointId` de `EndpointDetails` foi removida.

O modelo atualizado é semelhante ao seguinte:

```
AWS TemplateFormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
      EndpointDetails:
        SecurityGroupIds:
          - !Ref SecurityGroupId
        SubnetIds:
          - !Select [0, !Ref SubnetIds]
          - !Select [1, !Ref SubnetIds]
          - !Select [2, !Ref SubnetIds]
        VpcId: !Ref VpcId
      EndpointType: VPC
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
```

Para atualizar o tipo de endpoint dos servidores Transfer Family implantados usando CloudFormation

1. Pare o servidor que você deseja atualizar usando as etapas a seguir.

- a. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
- b. No painel de navegação, selecione Servidores.
- c. Marque a caixa de seleção da predefinição do servidor no qual você deseja alterar o tipo de endpoint.

 Important

Você deve interromper o servidor antes de alterar o endpoint.

- d. Em Ações, escolha Interromper.
- e. Na caixa de diálogo de confirmação exibida, escolha Parar para confirmar que quer interromper o servidor.

 Note

Antes de prosseguir para a próxima etapa, aguarde até que o Status do servidor mude para Offline; isso pode levar alguns minutos. Talvez você precise selecionar Atualizar na página dos Servidores para ver a alteração de status.

2. Atualize a CloudFormation pilha

- a. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
- b. Escolha a pilha usada para criar o servidor do Transfer Family.
- c. Selecione Atualizar.
- d. Escolha Substituir modelo atual
- e. Faça o upload do novo modelo. CloudFormation Os conjuntos de alterações ajudam você a entender como as alterações do modelo afetarão os recursos em execução antes de implementá-las. Neste exemplo, o recurso do servidor de transferência será modificado e o recurso VPCendpoint será removido. O servidor do tipo endpoint da VPC cria um Endpoint da VPC em seu nome, substituindo o recurso VPCEndpoint original.

Depois de carregar o novo modelo, o conjunto de alterações será semelhante ao seguinte:

Change set preview				
Changes (2)				
Search changes				
Action	Logical ID	Physical ID	Resource type	Replacement
Modify	TransferServer	arn:aws:transfer:us-east-1:364810874344:server/s-6a7d04e12d494ec98	AWS::Transfer::Server	Conditional
Remove	VPCEndpoint	vpce-04e685f8702849573 ↗	AWS::EC2::VPCEndpoint	-

- f. Atualize a pilha.
3. Quando a atualização da pilha estiver concluída, navegue até o console de gerenciamento do Transfer Family em <https://console.aws.amazon.com/transfer/>.
4. Reinicie o servidor. Escolha o servidor no CloudFormation qual você atualizou e escolha Iniciar no menu Ações.

Atualizando o servidor EndpointType usando a API

Você pode usar o comando AWS CLI [describe-server](#) ou o comando da API [UpdateServer](#). O script de exemplo a seguir interrompe o servidor Transfer Family, atualiza o EndpointType, remove o VPC_ENDPOINT e inicia o servidor.

```
import boto3
import time

profile = input("Enter the name of the AWS account you'll be working in: ")
region_name = input("Enter the AWS Region you're working in: ")
server_id = input("Enter the AWS Transfer Server Id: ")

session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2", region_name=region_name)
transfer = session.client("transfer", region_name=region_name)

group_ids=[]

transfer_description = transfer.describe_server(ServerId=server_id)
```



```

if transfer_description['Server']['EndpointType']=='VPC_ENDPOINT':
    transfer_vpc_endpoint = transfer_description['Server']['EndpointDetails']
['VpcEndpointId']
    transfer_vpc_endpoint_descriptions =
ec2.describe_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
    for transfer_vpc_endpoint_description in
transfer_vpc_endpoint_descriptions['VpcEndpoints']:
        subnet_ids=transfer_vpc_endpoint_description['SubnetIds']
        group_id_list=transfer_vpc_endpoint_description['Groups']
        vpc_id=transfer_vpc_endpoint_description['VpcId']
        for group_id in group_id_list:
            group_ids.append(group_id['GroupId'])
    if transfer_description['Server']['State']=='ONLINE':
        transfer_stop = transfer.stop_server(ServerId=server_id)
        print(transfer_stop)
        time.sleep(300) #safe
        transfer_update =
transfer.update_server(ServerId=server_id,EndpointType='VPC',EndpointDetails={'SecurityGroupIds':group_ids})
        print(transfer_update)
        time.sleep(10)
        transfer_start = transfer.start_server(ServerId=server_id)
        print(transfer_start)
        delete_vpc_endpoint =
ec2.delete_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])

```

Trabalhar com nomes de host personalizados

O nome de host do servidor é o nome do host que seus usuários inserem nos seus clientes ao se conectarem ao seu servidor. Você pode usar um domínio personalizado que você registrou para o nome de host do seu servidor ao trabalhar com AWS Transfer Family. Por exemplo, é possível usar um nome de host personalizado, como `mysftpserver.mysubdomain.domain.com`.

Para redirecionar o tráfego do domínio personalizado registrado para o endpoint do servidor, é possível usar o Amazon Route 53 ou qualquer provedor de Sistema de Nomes de Domínio (DNS). O Route 53 é o serviço DNS que AWS Transfer Family oferece suporte nativo.

Tópicos

- [Usar o Amazon Route 53 como seu provedor de DNS.](#)
- [Uso de outros provedores de DNS](#)
- [Nomes de host personalizados para servidores que não são criados por console](#)

No console, é possível escolher uma destas opções para a configuração de um nome de host personalizado:

- Pseudônimo de DNS do Amazon Route 53 — se o nome do host que você deseja usar estiver registrado no Route 53. Em seguida, você pode inserir o nome do host.
- Outro DNS - se o nome do host que você deseja usar estiver registrado em outro provedor DNS. Em seguida, você pode inserir o nome do host.
- Nenhum - para usar o endpoint do servidor e não um nome de host personalizado.

Você define essa opção ao criar um novo servidor ou editar a configuração de um servidor existente. Para obter mais informações sobre como criar um novo servidor, consulte [Etapa 2: criar um SFTP-enabled servidor](#). Para obter mais informações sobre como editar a configuração de um servidor existente, consulte [Editar detalhes do servidor](#).

Para obter mais detalhes sobre como usar seu próprio domínio para o nome do host do servidor e como AWS Transfer Family usa o Route 53, consulte as seções a seguir.

Usar o Amazon Route 53 como seu provedor de DNS.

Ao criar um servidor, é possível usar o Amazon Route 53 como provedor de DNS. Antes de usar um domínio no Route 53, registre o domínio. Para obter mais informações, consulte [Como funciona o registro de domínio](#) no Guia do desenvolvedor do Amazon Route 53.

Quando você usa o Route 53 para fornecer roteamento DNS ao seu servidor, AWS Transfer Family usa o nome de host personalizado que você inseriu para extrair sua zona hospedada. Ao AWS Transfer Family extrair uma zona hospedada, três coisas podem acontecer:

1. Se você é novo no Route 53 e não tem uma zona hospedada, AWS Transfer Family adiciona uma nova zona hospedada e um CNAME registro. O valor desse registro CNAME é o nome de host do endpoint para o seu servidor. Um CNAME é um nome de domínio alternativo.
2. Se você tiver uma zona hospedada no Route 53 sem registros de CNAME, o AWS Transfer Family adicionará um registro CNAME à zona hospedada.
3. Se o serviço detectar que um registro CNAME já existe na zona hospedada, você receberá uma mensagem de erro indicando que um registro CNAME já existe. Nesse caso, altere o valor do registro de CNAME para o nome de host do seu servidor.

Para obter mais informações sobre zonas hospedadas no Route 53, consulte [Zona hospedada](#) no Guia do desenvolvedor do Amazon Route 53.

Uso de outros provedores de DNS

Ao criar um servidor, você também pode usar provedores de DNS diferentes do Amazon Route 53. Se você usar um provedor de DNS alternativo, precisará se certificar de que o tráfego do seu domínio é direcionado para o endpoint do servidor do .

Para isso, defina seu domínio para o nome de host do endpoint no servidor.

- Para endpoints IPv4, o nome do host tem a seguinte aparência no console:

`serverid.server.transfer.region.amazonaws.com`

- Para endpoints de pilha dupla, o nome do host tem a seguinte aparência no console:

`serverid.transfer-server.region.on.aws`

Note

Se seu servidor tiver um VPC endpoint, o formato do nome do host será diferente dos descritos acima. Para encontrar seu endpoint da VPC, selecione o VPC na página de detalhes do servidor e, em seguida, selecione o ID do endpoint da VPC no painel da VPC. O endpoint é o primeiro nome DNS dos listados.

Nomes de host personalizados para servidores que não são criados por console

Ao criar um servidor usando AWS Cloud Development Kit (AWS CDK) CloudFormation, ou por meio da CLI, você deve adicionar uma tag se quiser que o servidor tenha um nome de host personalizado. Ao criar um servidor Transfer Family ao usar o console, a marcação é feita automaticamente.

Note

Você também precisa criar um registro DNS para redirecionar o tráfego do seu domínio para o endpoint do servidor. Para obter detalhes, consulte Como [trabalhar com registros](#) no Guia do desenvolvedor do Amazon Route 53.

Use as seguintes chaves para seu nome de host personalizado:

- Adicione `transfer:customHostname` para exibir o nome de host personalizado no console.
- Se você não está usando o Route 53 como provedor de DNS, adicione `transfer:route53HostedZoneId`. Essa tag vincula o nome do host personalizado ao seu ID de zona hospedada do Route 53.

Para adicionar o nome de host personalizado, emita o seguinte comando da CLI.

```
aws transfer tag-resource --arn arn:aws:transfer:region:Conta da AWS:server/server-ID
--tags Key=transfer:customHostname,Value="custom-host-name"
```

Por exemplo:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:customHostname,Value="abc.example.com"
```

Se você estiver usando o Route 53, emita o comando a seguir para vincular seu nome de host personalizado ao ID da zona hospedada do Route 53.

```
aws transfer tag-resource --arn server-ARN:server/server-ID --tags
Key=transfer:route53HostedZoneId,Value=HOSTED-ZONE-ID
```

Por exemplo:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:route53HostedZoneId,Value=ABCDE1111222233334444
```

Assumindo os valores de exemplo do comando anterior, execute o comando a seguir para visualizar suas tags:

```
aws transfer list-tags-for-resource --arn arn:aws:transfer:us-
east-1:111122223333:server/s-1234567890abcdef0
```

```
"Tags": [
  {
    "Key": "transfer:route53HostedZoneId",
```

```
    "Value": "/hostedzone/ABCDE1111222233334444"
  },
  {
    "Key": "transfer:customHostname",
    "Value": "abc.example.com"
  }
]
```

Note

Suas zonas públicas hospedadas e suas IDs estão disponíveis no Amazon Route 53. Faça login no Console de gerenciamento da AWS e abra o console do Route 53 em <https://console.aws.amazon.com/route53/>.

Considerações sobre o Network Load Balancer de FTP e FTPS

Embora seja recomendável evitar balanceadores de carga de rede na frente dos AWS Transfer Family servidores, se sua implementação de FTP ou FTPS exigir um NLB ou NAT na rota de comunicação do cliente, siga estas recomendações:

- Para um NLB, use a porta 21 para verificações de integridade, em vez das portas 8192-8200.
- Para o AWS Transfer Family servidor, habilite a retomada da sessão TLS configurando.
`TlsSessionResumptionMode = ENFORCED`

Note

Esse é o modo recomendado, pois fornece segurança aprimorada:

- Exige que os clientes usem a retomada da sessão TLS para conexões subsequentes.
- Fornece garantias de segurança mais fortes, garantindo parâmetros de criptografia consistentes.
- Ajuda a evitar possíveis ataques de downgrade.
- Mantém a conformidade com os padrões de segurança e, ao mesmo tempo, otimiza o desempenho.

- Se possível, deixe de usar um NLB para aproveitar ao máximo os limites de AWS Transfer Family desempenho e conexão.

Para obter orientação adicional sobre alternativas de NLB, entre em contato com a equipe de gerenciamento de AWS Transfer Family produtos por meio do Support AWS . Para obter mais informações sobre como melhorar sua postura de segurança, consulte a postagem do blog [Seis dicas para melhorar a segurança do seu AWS Transfer Family servidor](#).

A orientação de segurança para NLBs é fornecida em. [Evite colocar NLBs e NATs na frente de AWS Transfer Family servidores](#)

Transferindo arquivos em um endpoint de servidor usando um cliente

Você transfere arquivos pelo AWS Transfer Family serviço especificando a operação de transferência em um cliente. AWS Transfer Family suporta os seguintes clientes:

- Oferecemos suporte à versão 3 do protocolo SFTP.
- OpenSSH (macOS e Linux)

Note

Esse cliente funciona somente com servidores habilitados para File Transfer Protocol (SFTP) da Secure Shell (SSH).

- WinSCP (Microsoft Windows somente)
- Cyberduck (Windows, MacOS e Linux)
- FileZilla (Windows, macOS e Linux)

As limitações a seguir se aplicam a cada cliente:

- O protocolo SCP não é suportado, pois é considerado inseguro. Você pode usar o comando OpenSSH scp conforme descrito em. [Usar o comando scp](#)
- O número máximo de sessões SFTP simultâneas e multiplexadas por conexão é 10.
- Para conexões inativas, o valor do tempo limite é 1800 segundos (30 minutos) para todos os protocolos (). SFTP/FTP/FTPS Se não houver atividade após esse período, o cliente poderá ser desconectado. Para conexões que não respondem:
 - O SFTP tem um tempo limite de 300 segundos (5 minutos) quando um cliente não responde completamente.

- O FTPS e o FTP têm um tempo limite de aproximadamente 10 minutos sem resposta, gerenciado pela biblioteca subjacente.
- O Amazon S3 e o Amazon EFS (devido ao protocolo NFSv4) exigem que os nomes dos arquivos estejam codificados. UTF-8 Usar uma codificação diferente pode levar a resultados inesperados. Para o Amazon S3, consulte as [Diretrizes de nomenclatura de chaves de objetos](#).
- Para o protocolo de Transferência de Arquivos SSL (FTPS), somente o modo explícito é compatível. O modo implícito não é compatível.
- Para o protocolo de Transferência de Arquivos (FTP) e FTPS, somente o modo passivo é compatível.
- Para FTP e FTPS, somente o modo STREAM é compatível.
- Para FTP e FTPS, somente o Image/Binary modo é suportado.
- Para FTP e FTPS, TLS - PROT C (desprotegido) TLS para a conexão de dados é o padrão, mas o PROT C não é suportado no protocolo FTPS. AWS Transfer Family Portanto, para FTPS, você precisa emitir PROT P para que sua operação de dados seja aceita.
- Se você estiver usando o Amazon S3 para o armazenamento do seu servidor e se o seu cliente tiver a opção de usar várias conexões para uma única transferência, certifique-se de desativar a opção. Caso contrário, uploads de arquivos grandes podem falhar de forma imprevisível. Observe que, se você estiver usando o Amazon EFS como back-end de armazenamento, o EFS não oferece suporte a várias conexões para uma única transferência.

Veja a seguir uma lista dos comandos disponíveis para FTP e FTPS:

Comandos disponíveis					
ABOR	FEAT	MLST	PASS	RETR	STOR
AUTH	LANG	MKD	PASV	RMD	STOU
COPO	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PROT	RNTO	SYST
DELE	MFMT	NOOP	PWD	SIZE	TYPE
EPSV	MLSD	OPTS	QUIT	STAT	USER

Note

APPE não é compatível.

No momento, as operações a seguir não são compatíveis para usuários que usam o diretório inicial lógico em servidores que usam o Amazon Elastic File System (Amazon EFS).

Comandos SFTP incompatíveis

SSH_FXP_R EADLINK	SSH_FXP_SYMLINK	SSH_FXP_STAT quando o arquivo solicitado é um symlink	SSH_FXP_R EALPATH quando o caminho solicitad o contém qualquer componente symlink

Gerar um par de chaves pública-privada.

Antes de transferir um arquivo, você deve ter um par de chaves pública-privada disponível. Se você ainda não gerou um par de chaves, consulte [Gere chaves SSH para usuários gerenciados por serviços](#).

Tópicos

- [SFTP/FTPS/FTP Comandos disponíveis](#)
- [Encontre seu endpoint da Amazon VPC](#)
- [Evitar erros setstat](#)
- [Usar OpenSSH](#)
- [Usar o WinSCP](#)
- [Usar o Cyberduck](#)
- [Use FileZilla](#)
- [Usar um cliente Perl](#)
- [Use o LFTP](#)
- [Processamento pós upload](#)
- [Mensagens SFTP](#)

SFTP/FTPS/FTP Comandos disponíveis

A tabela a seguir descreve os comandos disponíveis para AWS Transfer Family, para os protocolos SFTP, FTPS e FTP.

Note

A tabela menciona arquivos e diretórios do Amazon S3, que só oferece suporte a buckets e objetos: não há hierarquia. No entanto, você pode usar prefixos em nomes de chaves de objetos para sugerir uma hierarquia e organizar seus dados de forma semelhante às pastas. Esse comportamento é descrito em [Trabalhar com metadados de objetos](#) no Guia do usuário do Amazon Simple Storage Service.

SFTP/FTPS/FTP Comandos

Command	Amazon S3	Amazon EFS
cd	Compatível	Compatível
chgrp	Não compatível	Compatível (apenas com root ou owner)
chmod	Não compatível	Compatível (apenas com root)
chmtime	Não compatível	Compatível
chown	Não compatível	Compatível (apenas com root)
get	Compatível	Compatível (incluindo resolução de links simbólicos)
ln -s	Não compatível	Compatível
ls/dir	Compatível	Compatível
mkdir	Compatível	Compatível

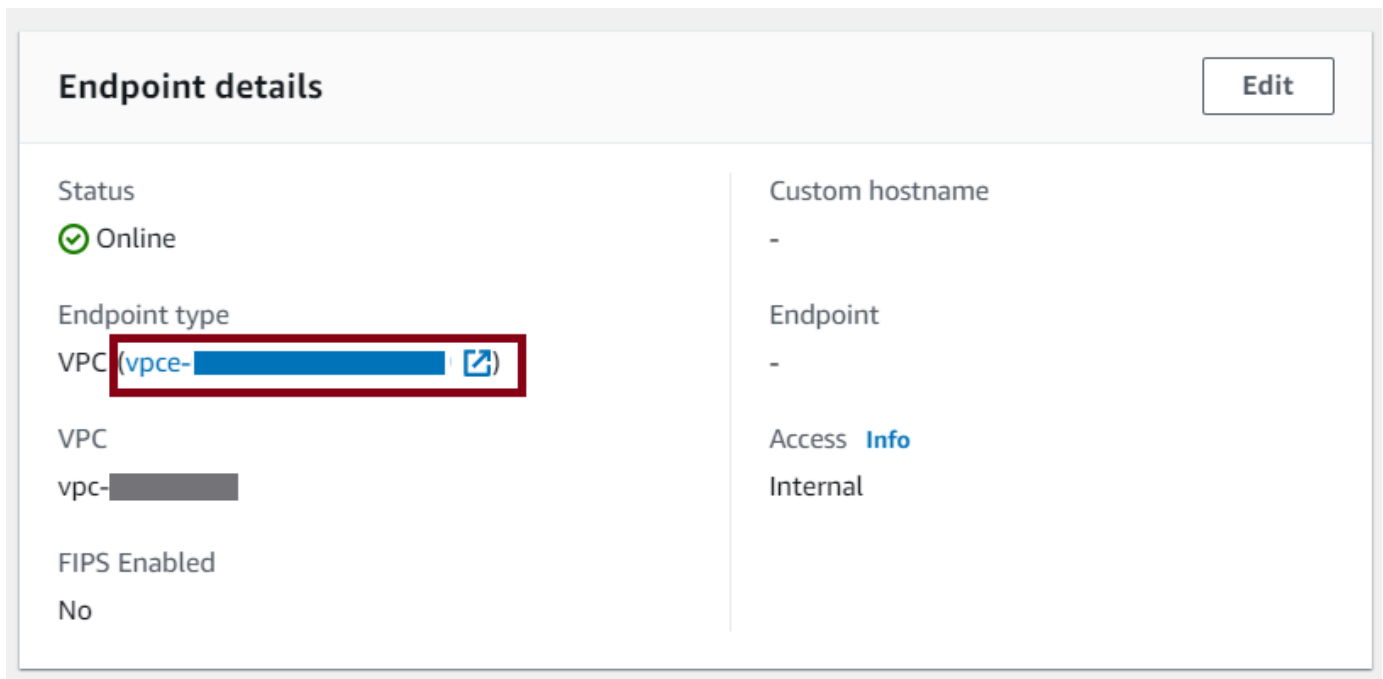
Command	Amazon S3	Amazon EFS
put	Compatível	Compatível
pwd	Compatível	Compatível
rename	Compatível somente com arquivos  Note A renomeação que substituiria um arquivo existente não é suportada.	Compatível  Note Não há suporte para renomear um arquivo ou diretório existente.
rm	Compatível	Compatível
rmdir	Compatível (somente diretórios vazios)	Compatível
version	Compatível	Compatível

Encontre seu endpoint da Amazon VPC

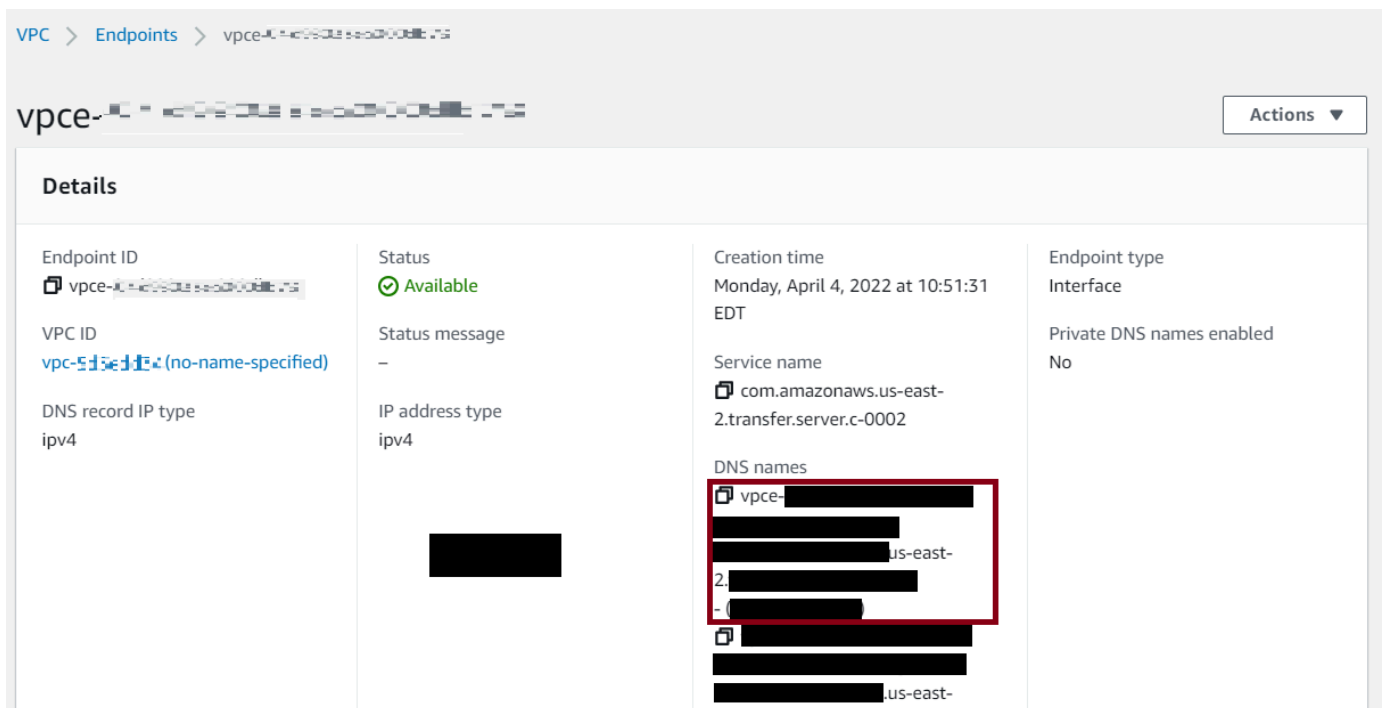
Se o tipo de endpoint do seu servidor Transfer Family para VPC, identificar o endpoint a ser usado para transferir arquivos não é simples. Nesse caso, use o procedimento a seguir para localizar o endpoint da Amazon VPC.

Para encontrar seu endpoint Amazon VPC

1. Navegue até a página de detalhes do seu servidor.
2. No painel de Detalhes do endpoint, selecione o VPC.



3. No painel do endpoint da Amazon VPC, selecione o ID do endpoint do VPC.
4. Na lista de Nomes de DNS, o endpoint do seu servidor é o primeiro listado.



Evitar erros `setstat`

Alguns clientes de transferência de arquivos SFTP podem tentar alterar os atributos de arquivos remotos, incluindo timestamp e permissões, utilizando comandos como SETSTAT ao carregar o arquivo. No entanto, esses comandos não são compatíveis com sistemas de armazenamento de objetos, como o Amazon S3. Devido a essa incompatibilidade, os uploads de arquivos desses clientes podem resultar em erros, mesmo quando o arquivo é carregado com êxito em outras circunstâncias.

- Quando você chama a API `CreateServer` ou `UpdateServer`, use a `ProtocolDetails` opção `SetStatOption` para ignorar o erro gerado quando o cliente tenta usar SETSTAT em um arquivo que você está carregando em um bucket do S3.
- Defina o valor como `ENABLE_NO_OP` para que o servidor do Transfer Family ignore o comando SETSTAT e carregue arquivos sem precisar fazer alterações no cliente SFTP.
- Observe que, embora a `SetStatOption ENABLE_NO_OP` configuração ignore o erro, ela gera uma entrada de registro em CloudWatch Logs, para que você possa determinar quando o cliente está fazendo uma chamada SETSTAT.

Para obter os detalhes da API dessa opção, consulte [ProtocolDetails](#).

Usar OpenSSH

Esta seção contém instruções para transferir arquivos da linha de comando usando o OpenSSH.

Note

Esse cliente funciona somente com um SFTP-enabled servidor.

Tópicos

- [Usar o OpenSSH](#)
- [Usar o comando scp](#)

Usar o OpenSSH

Para transferir arquivos AWS Transfer Family usando o utilitário de linha de comando OpenSSH

1. No Linux ou MacOS ou Windows, abra um terminal de comando.
2. No prompt, insira o seguinte comando:

```
sftp -i transfer-key sftp_user@service_endpoint
```

No comando anterior, *sftp_user* é o nome do usuário e *transfer-key* é a chave privada de SSH. Aqui *service_endpoint* está o endpoint do servidor, conforme mostrado no AWS Transfer Family console do servidor selecionado.

Note

Esse comando usa configurações que estão no `ssh_config` arquivo padrão. A menos que você tenha editado esse arquivo anteriormente, o SFTP usa a porta 22. Você pode especificar uma porta diferente (por exemplo, 2222) adicionando um `-P` sinalizador ao comando, da seguinte maneira.

```
sftp -P 2222 -i transfer-key sftp_user@service_endpoint
```

Como alternativa, se você sempre quiser usar a porta 2222 ou a porta 22000, poderá atualizar a porta padrão em seu `ssh_config` arquivo.

Um prompt `sftp` deve ser exibido.

3. (Opcional) Para visualizar o diretório inicial do usuário, digite o seguinte comando no prompt `sftp`:

```
pwd
```

4. Para carregar um arquivo do seu sistema de arquivos para o servidor Transfer Family, use o comando `put`. Por exemplo, para fazer o upload do `hello.txt` (supondo que o arquivo esteja no diretório atual do sistema de arquivos), execute o seguinte comando no prompt `sftp`:

```
put hello.txt
```

Uma mensagem semelhante à seguinte será exibida, indicando que a transferência de arquivos está em andamento ou foi concluída.

```
Uploading hello.txt to /amzn-s3-demo-bucket/home/sftp_user/hello.txt  
hello.txt 100% 127 0.1KB/s 00:00
```

Note

Depois de o servidor ser criado, poderá demorar alguns minutos para que o nome do host do endpoint do seu servidor possa ser resolvido pelo serviço de DNS em seu ambiente.

Usar o comando **scp**

O Transfer Family não suporta o protocolo SCP. No entanto, você pode usar o comando `scp` OpenSSH se precisar dessa funcionalidade.

A recomendação para usar o SCP sobre SFTP é usar o OpenSSH versão 9.0 ou posterior. No OpenSSH versão 9 e posterior, `scp` o comando usa como padrão o protocolo SFTP para transferências de arquivos em vez do protocolo SCP legado.

Important

Certifique-se de que seu servidor Transfer Family tenha sido configurado para usar o acesso a diretórios otimizado do S3.

Usar o WinSCP

Use as instruções a seguir para transferir arquivos a partir da linha de comando usando o WinSCP.

Note

Se você estiver usando o WinSCP 5.19, poderá se conectar diretamente ao Amazon S3 usando suas credenciais e arquivos. AWS upload/download Para obter mais detalhes, consulte [Conectar-se ao serviço Amazon S3](#).

Para transferir arquivos AWS Transfer Family usando o WinSCP

1. Abra o cliente WinSCP.
2. Na caixa de diálogo Login, em Protocolo de arquivo, escolha um protocolo: SFTP ou FTP.

Se você escolheu FTP, em Criptografia, selecione uma das seguintes opções:

- Sem criptografia para FTP
 - TLS/SSL Criptografia explícita para FTPS
3. Em Nome do host, insira o endpoint do servidor. O endpoint do servidor está localizado na página de Detalhes do servidor. Para obter mais informações, consulte [Exibir detalhes do servidor SFTP, FTPS e FTP](#).

Se seu servidor usa um endpoint do VPC, consulte [Encontre seu endpoint da Amazon VPC](#).

4. Em Número da porta, digite o seguinte:
 - **22** para SFTP
 - **21** para FTP/FTPS
5. Em Nome do usuário, insira o nome do usuário que você criou para seu provedor de identidade específico.

Dica: O nome de usuário deve ser um dos usuários que você criou ou configurou para seu provedor de identidade. AWS Transfer Family fornece os seguintes provedores de identidade:

- [Trabalhar com usuários gerenciados por serviços](#)
 - [Usando o AWS Directory Service para o Microsoft Active Directory](#)
 - [Trabalhar com provedores de identidade personalizados](#)
6. Escolha Avançado para abrir a caixa de diálogo Configurações avançadas do site. Na seção SSH, escolha Autenticação.
 7. Em Arquivo da chave privada, procure e selecione o arquivo de chave privada SSH no seu sistema de arquivos.

Se o WinSCP oferecer a conversão da sua chave privada SSH para o formato PPK, escolha OK.

8. Escolha OK para retornar à caixa de diálogo Login e escolha Salvar.
9. Na caixa de diálogo Salvar sessão como site, escolha OK para concluir a configuração da conexão.
10. Na caixa de diálogo Login, escolha Ferramentas e, em seguida, escolha Preferências.

11. Na caixa de diálogo Preferências, em Transferir, escolha Resistência.

Para a opção Habilitar transferência resume/transfer para nome de arquivo temporário para, escolha Desabilitar.

Important

Se você deixar essa opção ativada, ela aumentará os custos de upload, diminuindo substancialmente o desempenho do upload. Isso também pode levar a falhas no upload de arquivos grandes.

12. Em Transferir, escolha Segundo plano e desmarque a caixa de seleção Usar várias conexões para uma única transferência.

Dica: se você deixar essa opção selecionada, os carregamentos de arquivos grandes podem falhar de forma imprevisível. Por exemplo, uploads órfãos de várias partes que incorrem em cobranças do Amazon S3 podem ser criados. A corrupção silenciosa de dados também pode ocorrer.

13. Realize a transferência do seu arquivo.

Você pode usar métodos de arrastar e soltar para copiar arquivos entre as janelas de origem e destino. Você pode usar os ícones da barra de ferramentas para fazer upload/download, excluir, editar ou modificar as propriedades dos arquivos no WinSCP.

Note

Essa observação não se aplica se você estiver usando o Amazon EFS para armazenamento. Comandos que tentam alterar atributos de arquivos remotos, incluindo registros de data/hora, não são compatíveis com sistemas de armazenamento de objetos, como o Amazon S3. Portanto, se você estiver usando o Amazon S3 para armazenamento, certifique-se de desativar as configurações de marcação de tempo do WinSCP (ou use o `SetStatOption` conforme descrito em [Evitar erros setstat](#)) antes de realizar transferências de arquivos. Para isso, na caixa de diálogo Configurações de transferência do WinSCP, desabilite a opção de upload Definir permissões e a opção comum Preservar marcação de tempo.

Usar o Cyberduck

Use as instruções a seguir para transferir arquivos a partir da linha de comando usando o Cyberduck.

Para transferir arquivos AWS Transfer Family usando o Cyberduck

1. Abra o cliente [Cyberduck](#).
2. Escolha Abrir conexão.
3. Na caixa de diálogo Abrir conexão, escolha um protocolo: SFTP (SSH File Transfer Protocol), FTP-SSL(Explicit AUTH TLS) ou FTP (File Transfer Protocol).
4. Em Nome do servidor, insira o endpoint do servidor. O endpoint do servidor está localizado na página de Detalhes do servidor. Para obter mais informações, consulte [Exibir detalhes do servidor SFTP, FTPS e FTP](#).

Se seu servidor usa um endpoint do VPC, consulte [Encontre seu endpoint da Amazon VPC](#).

5. Em Número da porta, digite o seguinte:
 - **22** para SFTP
 - **21** para FTP/FTPS
6. Em Nome do usuário, insira o nome do usuário que você criou no [Gerenciando usuários para endpoints de servidor](#).
7. Se SFTP estiver selecionado, em Chave privada SSH, escolha ou insira a chave privada SSH.
8. Selecione Conectar.
9. Realize a transferência do seu arquivo.

Dependendo de onde estão seus arquivos, siga um destes procedimentos:

- Em seu diretório local (a origem), escolha os arquivos que você deseja transferir e arraste e solte-os no diretório do Amazon S3 (o destino).
- No diretório do Amazon S3 (a origem), escolha os arquivos que você deseja transferir e arraste e solte-os no seu diretório local (o destino).

Use FileZilla

Use as instruções a seguir para transferir arquivos usando FileZilla.

FileZilla Para configurar uma transferência de arquivos

1. Abra o FileZilla cliente.
2. Escolha Arquivo e, em seguida, selecione Gerenciador de sites.
3. Na caixa de diálogo Gerenciador de sites, escolha Novo site.
4. Na guia Geral, em Protocolo, escolha um protocolo: SFTP ou FTP.

Se você escolheu FTP, em Criptografia, selecione uma das seguintes opções:

- Usar somente FTP simples (sem segurança) — para FTP
 - Usar FTP explícito sobre TLS, se disponível — para FTPS
5. Em Nome do host, insira o protocolo que você está usando, seguido pelo endpoint do servidor. O endpoint do servidor está localizado na página de Detalhes do servidor. Para obter mais informações, consulte [Exibir detalhes do servidor SFTP, FTPS e FTP](#).
 - Se você estiver usando SFTP, digite: `sftp://hostname`
 - Se você estiver usando FTPS, digite: `ftps://hostname`

Certifique-se de *hostname* substituir pelo endpoint real do servidor.

Se seu servidor usa um endpoint do VPC, consulte [Encontre seu endpoint da Amazon VPC](#).

6. Em Número da porta, digite o seguinte:
 - **22** para SFTP
 - **21** para FTP/FTPS
7. Se SFTP estiver selecionado, em Tipo de logon, escolha Arquivo de chave.

Em Arquivo de chave, escolha ou insira a chave privada SSH.

8. Em Usuário, insira o nome do usuário que você criou no [Gerenciando usuários para endpoints de servidor](#).
9. Selecione Conectar.
10. Realize a transferência do seu arquivo.

 Note

Se você interromper uma transferência de arquivo em andamento, AWS Transfer Family poderá gravar um objeto parcial em seu bucket do Amazon S3. Se você interromper um upload, verifique se o tamanho do arquivo no bucket do S3 corresponde ao tamanho do arquivo do objeto de origem antes de continuar.

Usar um cliente Perl

Se você usa o cliente `Net::SFTP::Foreign` perl, você deve definir `queue_size` o. 1 Por exemplo:

```
my $sftp = Net::SFTP::Foreign->new('user@s-12345.server.transfer.us-east-2.amazonaws.com', queue_size => 1);
```

 Note

Essa solução alternativa é necessária para revisões de `Net::SFTP::Foreign` anteriores à [1.92.02](#).

Use o LFTP

O LFTP é um cliente FTP gratuito que permite aos usuários realizar transferências de arquivos por meio da interface de linha de comando da maioria das máquinas Linux.

Para downloads de arquivos grandes, o LFTP tem um problema conhecido com pacotes fora de ordem, fazendo com que a transferência do arquivo falhe.

Processamento pós upload

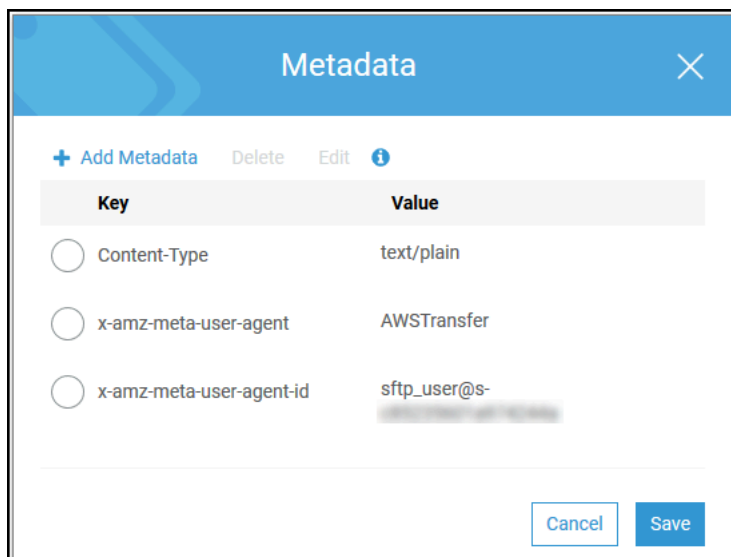
Você pode visualizar informações de processamento pós-upload, incluindo metadados de objetos do Amazon S3 e notificações de eventos.

Tópicos

- [Metadados de objetos do Amazon S3](#)
- [Notificações de eventos do Amazon S3](#)

Metadados de objetos do Amazon S3

Como parte dos metadados do seu objeto, você vê uma chave chamada `x-amz-meta-user-agent` cujo valor é `AWSTransfer` e `x-amz-meta-user-agent-id` cujo valor é `username@server-id`. O `username` é o usuário do Transfer Family que fez o upload do arquivo e o `server-id` é o servidor usado para o upload. Essas informações podem ser acessadas usando a [HeadObject](#) operação no objeto S3 dentro da função Lambda.



The screenshot shows the 'Metadata' window in the AWS console. It has a blue header with a close button. Below the header, there are buttons for '+ Add Metadata', 'Delete', 'Edit', and an information icon. A table lists the metadata:

Key	Value
☐ Content-Type	text/plain
☐ x-amz-meta-user-agent	AWSTransfer
☐ x-amz-meta-user-agent-id	sftp_user@s-

At the bottom right, there are 'Cancel' and 'Save' buttons.

Notificações de eventos do Amazon S3

Quando um objeto é carregado em seu bucket do S3 usando Transfer Family, o `RoleSessionName` está contido no campo Solicitante na [estrutura de notificação de eventos do S3](#) como `[AWS:Role Unique Identifier]/username.sessionid@server-id`. Por exemplo, a seguir está o conteúdo de um campo de exemplo de Solicitante de um log de acesso do S3 para um arquivo que foi copiado para o bucket do S3.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/  
username.sessionid@server-id
```

No campo Solicitante acima, ele mostra o perfil do IAM chamado `IamRoleName`. Para obter mais informações sobre a configuração de notificações de eventos do S3, consulte [Configurar notificações de eventos do Amazon S3](#) no Guia do desenvolvedor do Amazon Simple Storage Service. Para obter mais informações sobre identificadores exclusivos de funções AWS Identity and Access Management (IAM), consulte [Identificadores exclusivos](#) no Guia do AWS Identity and Access Management usuário.

Mensagens SFTP

Esta seção descreve as mensagens do lado do cliente que você pode receber durante ou após a transferência do arquivo SFTP ao usar um servidor Transfer Family. Para obter mais informações sobre qualquer evento SFTP, verifique os registros do cliente SFTP. Você pode usar essas informações para solucionar quaisquer erros ou encaminhá-las à sua equipe de rede para obter ajuda na identificação do problema.

Mensagens SFTP do lado do cliente

Atividade	Description
FALHA DE AUTENTICAÇÃO	O usuário falhou na autenticação. Isso pode ser qualquer tipo de falha de um provedor de identidade personalizado ou usuário gerenciado pelo serviço. Os detalhes do evento ajudam a esclarecer a causa raiz da falha.
CLOSE	Indica que um arquivo ou diretório aberto foi fechado com sucesso.
CONNECTED/DISCONNECTED	Indica sucesso e desconexões normais da conexão.
CRIAR_LINK SIMBÓLICO	Um link simbólico foi criado (com sucesso ou sem sucesso).
DELETE	Um arquivo foi excluído (com sucesso ou sem sucesso).
ERROR	Um erro geral e inesperado. A descrição associada contém informações que podem ajudar você ou seus administradores de rede a identificar o problema específico.
RAZÃO_DE_SAÍDA	Emitido quando um erro inesperado causou o encerramento da sua sessão de SFTP. A mensagem associada ao evento descreve a causa.

Atividade	Description
MKDIR	Um diretório foi criado (com sucesso ou sem sucesso).
OPEN	Um arquivo foi aberto para leitura ou gravação (com sucesso ou sem sucesso)
FECHAMENTO_PARCIAL	O cliente se desconectou do servidor enquanto um arquivo ainda estava aberto sem a mensagem CLOSE recebida. O Transfer Family armazena a parte recebida do arquivo (que na verdade pode ser o arquivo completo) e emite o evento PARTIAL_CLOSE para alertar o cliente sobre o problema. A integração de fluxos de trabalho também recebe um <code>onPartialClose</code> evento para tratar o arquivo adequadamente.
RENAME	Um arquivo foi renomeado (com sucesso ou sem sucesso)
RMDIR	Um diretório foi excluído (com sucesso ou sem sucesso)

Atividade	Description
SETSTAT	Os atributos de um arquivo são alterados (com ou sem sucesso).  Note O Transfer Family não oferece suporte ao SETSTAT se você estiver usando o Amazon S3 para armazenamento. A Evitar erros setstat seção fornece detalhes sobre como evitar SetStat erros, desativando a configuração. Isso evita que você receba uma <code>fail unsupported error</code> : em vez disso, você recebe uma <code>success but do nothing</code> mensagem.
FALHA NO RESUMO DO TLS	O servidor está configurado para impor a retomada da sessão TLS e o cliente não oferece suporte a ela.

Gerenciando usuários para endpoints de servidor

Nas seções a seguir, você encontrará informações sobre como adicionar usuários usando AWS Transfer Family AWS Directory Service for Microsoft Active Directory ou um provedor de identidade personalizado.

Como parte das propriedades de cada usuário, você também pode armazenar a chave pública Secure Shell (SSH) desse usuário. Isso é necessário para a autenticação baseada em chaves. A chave privada será armazenada localmente no computador do seu usuário. Quando o usuário envia uma solicitação de autenticação ao seu servidor usando um cliente, o servidor confirma que o usuário tem acesso à chave privada SSH associada. Em seguida, o servidor autentica o usuário com êxito.

 Note

Para implantação e gerenciamento automatizados de usuários com várias chaves SSH, consulte [Módulos Transfer Family Terraform](#).

Além disso, especifique um diretório da página inicial do usuário, ou o diretório inicial, e atribua um perfil (IAM) do AWS Identity and Access Management para o usuário. Opcionalmente, é possível fornecer uma política de sessão para limitar o acesso do usuário somente ao diretório do seu bucket do Amazon S3.

 Important

AWS Transfer Family bloqueia a autenticação de nomes de usuário com 1 ou 2 caracteres nos servidores SFTP. Além disso, também bloqueamos o nome de usuário `root`. A razão por trás disso é devido ao grande volume de tentativas mal-intencionadas de login por scanners de senha.

Amazon EFS versus Amazon S3

Características de cada opção de armazenamento:

- Para limitar o acesso: o Amazon S3 oferece suporte a políticas de sessão; o Amazon EFS oferece suporte a IDs POSIX de usuário, grupo e grupo secundário
- Ambas as public/private teclas de suporte
- Ambos dão suporte a diretórios iniciais
- Ambos dão suporte a diretórios lógicos

 Note

Para o Amazon S3, a maior parte do suporte para diretórios lógicos é via API/CLI. É possível usar a caixa de seleção Restrito no console para bloquear um usuário em seu diretório inicial, mas não pode especificar uma estrutura de diretório virtual.

Diretórios lógicos

Se você estiver especificando valores de diretório lógico para seu usuário, o parâmetro usado dependerá do tipo de usuário.

- Para usuários gerenciados por serviços, forneça valores de diretório lógico em `HomeDirectoryMappings`.
- Para usuários de provedores de identidade personalizados, forneça valores de diretório lógico em `HomeDirectoryDetails`.

AWS Transfer Family suporta a especificação de um `HomeDirectory` valor ao usar o `LOGICAL HomeDirectoryType`. Isso se aplica aos usuários do `Service Managed`, ao acesso ao `Active Directory` e às implementações do `Provedor de Identidade Personalizado`, onde `HomeDirectoryDetails` são fornecidos na resposta.

Important

Ao especificar um `HomeDirectory` com `LOGICAL HomeDirectoryType`, o valor deve ser mapeado para um de seus mapeamentos lógicos de diretório. O serviço valida isso durante a criação e as atualizações do usuário para evitar configurações que não funcionariam.

Comportamento padrão do

Por padrão, se não for especificado, o `HomeDirectory` é definido como `"/` para o modo `LÓGICO`. Esse comportamento permanece inalterado e permanece compatível com as definições de usuário existentes.

- Certifique-se de mapear sua entrada `HomeDirectory` para uma entrada e não para um alvo. Consulte mais detalhes em [Regras para usar diretórios lógicos](#).
- Para obter detalhes sobre como um diretório virtual é estruturado, consulte [Estrutura do diretório virtual](#).

Considerações sobre provedores de identidade personalizados

Ao usar um provedor de identidade personalizado, agora você pode especificar um `HomeDirectory` na resposta ao usar o `LOGICAL HomeDirectoryType`. A chamada da `TestIdentityProvider API`

produzirá resultados corretos quando o IDP personalizado especificar um HomeDirectory no modo LÓGICO.

Exemplo de resposta personalizada do IDP com HomeDirectory e LOGICAL HomeDirectoryType:

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-user-role",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectory": "/marketing",
  "HomeDirectoryDetails": "[{\"Entry\":\"\\\\\\\\\", \"Target\":\"\\\\\\\\/bucket/home\\\\\\\\\"}, {\"Entry\":\"\\\\\\\\/marketing\\\\\\\\\", \"Target\":\"\\\\\\\\/marketing-bucket/campaigns\\\\\\\\\"}]"
}
```

Cotas de grupo do Active Directory

AWS Transfer Family tem um limite padrão de 100 grupos do Active Directory por servidor. Se seu caso de uso exigir mais de 100 grupos, considere usar uma solução de provedor de identidade personalizada, conforme descrito em [Simplifique a autenticação do Active Directory com um provedor de identidade personalizado para AWS Transfer Family](#).

Esse limite se aplica aos servidores que usam os seguintes provedores de identidade:

- AWS Directory Service para Microsoft Active Directory
- AWS Directory Service para serviços de domínio Entra ID

Se você precisar solicitar um aumento do limite de serviço, consulte as [AWS service \(Serviço da AWS\) cotas](#) no Referência geral da AWS. Se seu caso de uso exigir mais de 100 grupos, considere usar uma solução de provedor de identidade personalizada, conforme descrito em [Simplifique a autenticação do Active Directory com um provedor de identidade personalizado para AWS Transfer Family](#).

Para obter informações sobre solução de problemas relacionadas aos limites de grupos do Active Directory, consulte [Limites de grupos do Active Directory excedidos](#).

Tópicos

- [Trabalhar com usuários gerenciados por serviços](#)
- [Trabalhar com provedores de identidade personalizados](#)
- [Usando o AWS Directory Service para o Microsoft Active Directory](#)
- [Usando o AWS Directory Service para serviços de domínio Entra ID](#)

Trabalhar com usuários gerenciados por serviços

É possível adicionar usuários gerenciados por serviços do Amazon S3 ou do Amazon EFS ao seu servidor, dependendo da configuração de domínio do servidor. Para obter mais informações, consulte [Configurando um endpoint de servidor SFTP, FTPS ou FTP](#).

Se você usar um tipo de identidade gerenciada por serviço, adicione usuários ao seu servidor habilitado para SFTP. Ao fazer isso, cada nome de usuário deve ser único no servidor.

Para adicionar programaticamente um usuário gerenciado pelo serviço, veja o [exemplo](#) da API. [CreateUser](#)

Note

Para usuários gerenciados por serviços, há um limite de 2.000 entradas de diretório lógico. Para obter informações sobre o uso de diretórios lógicos, consulte [Como usar diretórios lógicos para simplificar suas estruturas de diretórios do Transfer Family](#).

Tópicos

- [Adicionar usuários gerenciados por serviços do Amazon S3](#)
- [Adicionar usuários gerenciados por serviços do Amazon EFS](#)
- [Gerenciar usuários gerenciados por serviços](#)

Adicionar usuários gerenciados por serviços do Amazon S3

Note

Se você quiser configurar um bucket Amazon S3 com várias contas, siga as etapas mencionadas neste artigo do Knowledge Center: [Como configuro meu AWS Transfer Family servidor para usar um bucket do Amazon Simple Storage Service que está em outra AWS conta?](#) .

Para adicionar um usuário gerenciado por serviços do Amazon S3 ao seu servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/> e selecione Servidores no painel de navegação.

2. Na página Servidores, escolha a caixa de seleção ao lado do servidor para o qual você deseja adicionar um usuário.
3. Escolha Adicionar usuário.
4. Na seção Configuração do usuário, em Nome de usuário, insira o nome de usuário. Esse nome de usuário deve ter, no mínimo, 3 e, no máximo 100 caracteres. Você pode usar os seguintes caracteres no nome de usuário: a—z, 0—9 A-Z, sublinhado '_', hífen '-', ponto '.' e sinal de arroba '@'. O nome de usuário não pode começar com um hífen '-', ponto '.' ou com o sinal '@'.
5. Para For Acesso, selecione o perfil do IAM que você criou anteriormente e que fornece acesso ao seu bucket do Amazon S3.

Você criou esse perfil do IAM usando o procedimento em [Criar uma política e um perfil do IAM](#). Esse perfil do IAM inclui uma política do IAM que fornece acesso ao seu bucket do Amazon S3. Também inclui uma relação de confiança com o AWS Transfer Family serviço, definida em outra política do IAM. Se você precisar de um controle de acesso refinado para seus usuários, consulte a postagem do blog [Enhance data access with an Amazon AWS Transfer Family S3](#).

6. (Opcional) Para Política, selecione uma das seguintes ações:
 - Nenhum
 - Política existente
 - Selecione uma política do IAM: permite que você escolha uma política de sessão existente. Escolha Exibir para ver um objeto JSON contendo os detalhes da política.
 - Auto-generate política baseada na pasta inicial: gera uma política de sessão para você. Escolha Exibir para ver um objeto JSON contendo os detalhes da política.

 Note

Se você escolher a Auto-generate política com base na pasta base, não selecione Restrito para esse usuário.

Para saber mais sobre as políticas de sessão [Criar uma política e um perfil do IAM](#), consulte [Criar uma política de sessão de um bucket do Amazon S3](#), ou [Abordagens dinâmicas de gerenciamento de permissões](#).

7. Para o diretório inicial, escolha o bucket do Amazon S3 para armazenar os dados a serem transferidos usando. AWS Transfer Family Insira o caminho no diretório home que o usuário acessa quando faz login usando seu cliente.

Se você deixar esse parâmetro em branco, o diretório `root` do seu bucket do Amazon S3 será usado. Nesse caso, certifique-se de que seu perfil do IAM fornece acesso a esse `root` diretório.

 Note

Recomendamos que você escolha um caminho de diretório que contenha o nome do usuário, o que permite que você efetivamente use uma política de sessão. A política de sessão limita o acesso do usuário no bucket do Amazon S3 para o diretório home do usuário.

8. (Opcional) Em Restrito, marque a caixa de seleção para que seus usuários não possam acessar nada fora dessa pasta e não possam ver o bucket ou o nome da pasta do Amazon S3.

 Note

Atribuir ao usuário um diretório inicial e restringir o usuário a esse diretório inicial deve ser suficiente para bloquear o acesso do usuário à pasta designada. Se você precisar aplicar mais controles, use uma política de sessão.

Se você selecionar Restrito para esse usuário, não poderá selecionar a Auto-generate política com base na pasta base, pois a pasta base não é um valor definido para usuários restritos.

9. Para chave pública SSH, insira a parte da chave pública SSH do par de chaves SSH.

Sua chave é validada pelo serviço antes que você possa adicionar o novo usuário.

 Note

Para obter instruções sobre como gerar um par de chaves SSH, consulte [Gere chaves SSH para usuários gerenciados por serviços](#).

10. (Opcional) Em Chave e Valor, insira uma ou mais tags como pares de chave/valor e escolha Adicionar tag.
11. Escolha Adicionar para adicionar o novo usuário ao servidor que você escolheu.

O novo usuário será exibido na seção Usuários da página Detalhes do servidor.

Próximas etapas - Para a próxima etapa, continue em [Transferindo arquivos em um endpoint de servidor usando um cliente](#).

Adicionar usuários gerenciados por serviços do Amazon EFS

O Amazon EFS usa o modelo de permissão de arquivo da Portable Operating System Interface (POSIX) para representar a propriedade do arquivo.

- Para obter mais detalhes sobre a propriedade de arquivos do Amazon EFS, consulte [Propriedade do arquivo do Amazon EFS](#).
- Para obter mais detalhes sobre a configuração de diretórios para seus usuários do EFS, consulte [Configurar usuários do Amazon EFS para Transfer Family](#).

Para adicionar um usuário gerenciado por serviços do Amazon EFS ao seu servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/> e selecione Servidores no painel de navegação.
2. Na página Servidores, selecione o servidor do Amazon EFS ao qual você deseja adicionar um usuário.
3. Escolha Adicionar usuário para exibir a página Adicionar usuário.
4. Na seção Configuração de usuários, use as seguintes configurações.
 - a. Esse Nome de usuário deve ter, no mínimo, 3 e, no máximo 100 caracteres. Você pode usar os seguintes caracteres no nome de usuário: a—z,, 0—9 A-Z, sublinhado '_', hífen '-', ponto '.', e no sinal "@". O nome de usuário não pode começar com hífen '-', ponto final '.' ou o sinal de arroba "@".
 - b. Para ID de usuário e ID de grupo, observe o seguinte:
 - Para o primeiro usuário que você criar, recomendamos que você insira um valor de ID **0** de ID de grupo e ID de usuário. Isso concede ao usuário privilégios de administrador para o Amazon EFS.
 - Para usuários adicionais, insira o ID de usuário POSIX e o ID do grupo do usuário. Esses IDs são usados para todas as operações do Amazon Elastic File System realizadas pelo usuário.
 - Para ID de usuário e ID de grupo, não use nenhum zero à esquerda. Por exemplo, **12345** é aceitável, mas **012345** não é.

- c. (Opcional) Para IDs de grupo secundário, insira um ou mais IDs de grupo POSIX adicionais para cada usuário, separados por vírgulas.
- d. Para Acesso, escolha o perfil do IAM que:
 - Concede ao usuário acesso apenas aos recursos do Amazon EFS (sistemas de arquivos) que você deseja que ele acesse.
 - Define quais operações do sistema de arquivos o usuário pode ou não realizar.

Recomendamos que você use a função do IAM para a seleção do sistema de arquivos do Amazon EFS com acesso e read/write permissões de montagem. Por exemplo, a combinação das duas políticas AWS gerenciadas a seguir, embora bastante permissiva, concede as permissões necessárias para seu usuário:

- AmazonElasticFileSystemClientFullAccess
- AWSTransferConsoleFullAccess

Para obter mais informações, consulte a publicação do blog: [Suporte do AWS Transfer Family para Amazon Elastic File System](#).

- e. Para o Diretório inicial, faça o seguinte:
 - Escolha o sistema de arquivos do Amazon EFS que você deseja usar para armazenar os dados a serem transferidos usando AWS Transfer Family.
 - Decida se deseja definir o diretório inicial como Restrito. Definir o diretório inicial como Restrito tem os seguintes efeitos:
 - Os usuários do Amazon EFS não podem acessar nenhum arquivo ou diretório fora dessa pasta.
 - Os usuários do Amazon EFS não conseguem ver o nome do sistema de arquivos do Amazon EFS (fs-xxxxxxx).

 Note

Quando você seleciona a opção Restrito, os links simbólicos não são resolvidos para os usuários do Amazon EFS.

- (Opcional) Insira o caminho para o diretório inicial no qual você deseja que os usuários estejam quando fizerem login usando o cliente.

Se você não especificar um diretório inicial, o diretório raiz do seu sistema de arquivos Amazon EFS será usado. Nesse caso, certifique-se de que seu perfil do IAM fornece acesso a esse diretório .

5. Para chave pública SSH, insira a parte da chave pública SSH do par de chaves SSH.

Sua chave é validada pelo serviço antes que você possa adicionar o novo usuário.

 Note

Para obter instruções sobre como gerar um par de chaves SSH, consulte [Gere chaves SSH para usuários gerenciados por serviços](#).

6. (Opcional) Insira qualquer tag para o usuário. Para Chave and Valor, insira uma ou mais tags como pares de chave/valor e escolha Adicionar tag.
7. Escolha Adicionar para adicionar o novo usuário ao servidor que você escolheu.

O novo usuário será exibido na seção Usuários da página Detalhes do servidor.

Problemas possíveis de encontrar ao usar o SFTP pela primeira vez no servidor do Transfer Family:

- Se você executar o comando `sftp` e o prompt não aparecer, é possível encontrar a seguinte mensagem:

```
Couldn't canonicalize: Permission denied
```

```
Need cwd
```

Nesse caso, aumente as permissões da política para a função do seu usuário. Você pode adicionar uma política AWS gerenciada, como `AmazonElasticFileSystemClientFullAccess`.

- Se você entrar `pwd` no `sftp` prompt para visualizar o diretório inicial do usuário, poderá ver a seguinte mensagem, onde ***USER-HOME-DIRECTORY*** está o diretório inicial do usuário SFTP:

```
remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
```

Nesse caso, você deve conseguir navegar até o diretório pai (`cd . .`) e criar o diretório inicial do usuário (`mkdir username`).

Próximas etapas - Para a próxima etapa, continue em [Transferindo arquivos em um endpoint de servidor usando um cliente](#).

Gerenciar usuários gerenciados por serviços

Nesta seção, é possível encontrar informações sobre como visualizar uma lista de usuários, como editar detalhes do usuário e como adicionar uma chave pública SSH.

- [Exibir uma lista de usuários](#)
- [Exibir ou editar detalhes do usuário](#)
- [Exclusão de um usuário](#)
- [Adicionar chave pública SSH](#)
- [Excluir chave pública SSH](#)

Para encontrar uma lista de seus usuários

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. Selecione Servidores no painel de navegação para exibir a página Servidores.
3. Escolha o identificador na coluna ID do servidor para ver a página Detalhes do servidor.
4. Em Usuários, veja uma lista de usuários.

Para visualizar ou editar detalhes do usuário

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. Selecione Servidores no painel de navegação para exibir a página Servidores.
3. Escolha o identificador na coluna ID do servidor para ver a página Configuração do servidor.
4. Em Usuários, escolha um nome de usuário para ver a página de Detalhes do usuário.

É possível alterar as propriedades do usuário nessa página escolhendo Editar.

5. Na página Detalhes do usuário, escolha Editar ao lado de Configuração do usuário.

Edit configuration

User configuration

Access [Info](#)
User's IAM role for Amazon S3 access

Admin ▼

Policy [Info](#)
Scope down policy to apply to the user

☒ None
☐ Existing policy
☐ Select a policy from IAM

[View](#)

Home directory
User's login directory

Choose an S3 bucket ▼

Enter optional folder

☐ Restricted [Info](#)

Cancel Save

6. Na página Editar configuração, para Acesso, escolha o perfil do IAM que você criou antes e que fornece acesso ao seu bucket do Amazon S3.

Você criou esse perfil do IAM usando o procedimento em [Criar uma política e um perfil do IAM](#). Esse perfil do IAM inclui uma política do IAM que fornece acesso ao seu bucket do Amazon S3. Também inclui uma relação de confiança com o AWS Transfer Family serviço, definida em outra política do IAM.

7. (Opcional) Para Política, escolha uma das seguintes opções:
- Nenhum
 - Política existente
 - Selecionar uma política do IAM: permite que você escolha uma política de sessão existente. Escolha Exibir para ver um objeto JSON contendo os detalhes da política.

Para saber mais sobre as políticas de sessão, consulte [Criar uma política e um perfil do IAM](#). Para saber mais sobre como criar uma política de sessão, consulte [Criar uma política de sessão de um bucket do Amazon S3](#).

8. Para o diretório inicial, escolha o bucket do Amazon S3 para armazenar os dados a serem transferidos usando AWS Transfer Family. Insira o caminho no diretório home que o usuário acessa quando faz login usando seu cliente.

Se você deixar esse parâmetro em branco, o diretório root do seu bucket do Amazon S3 será usado. Nesse caso, certifique-se de que seu perfil do IAM fornece acesso a esse root diretório.

 Note

Recomendamos que você escolha um caminho de diretório que contenha o nome do usuário, o que permite que você efetivamente use uma política de sessão. A política de sessão limita o acesso do usuário no bucket do Amazon S3 para o diretório home do usuário.

9. (Opcional) Em Restrito, marque a caixa de seleção para que seus usuários não possam acessar nada fora dessa pasta e não possam ver o bucket ou o nome da pasta do Amazon S3.

 Note

Ao designar ao usuário um diretório inicial e restringir o usuário a esse diretório inicial, isso deve ser suficiente para bloquear o acesso do usuário à pasta designada. Se você precisar aplicar mais controles, use uma política de sessão.

10. Escolha Salvar para salvar as alterações.

Para excluir um usuário

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. Selecione Servidores no painel de navegação para exibir a página Servidores.
3. Escolha o identificador na coluna ID do servidor para ver a página Configuração do servidor.
4. Em Usuários, escolha um nome de usuário para ver a página de Detalhes do usuário.
5. Na página Detalhes do usuário, escolha Excluir à direita do nome de usuário.
6. Na caixa de diálogo de confirmação exibida, insira a palavra **delete** e escolha Excluir para confirmar que deseja excluir o usuário.

O usuário é excluído e removido da lista de usuários .

Para adicionar uma chave pública SSH para um usuário

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores.
3. Escolha o identificador na coluna ID do servidor para ver a página Configuração do servidor.
4. Em Usuários, escolha um nome de usuário para ver a página de Detalhes do usuário.
5. Escolha Add SSH public key (Adicionar chave pública SSH) para adicionar uma nova chave pública SSH a um usuário.

 Note

As chaves SSH são usadas somente por servidores habilitados para File Transfer Protocol (SFTP) da Secure Shell (SSH). Para obter informações sobre como gerar um par de chaves SSH, consulte [Gere chaves SSH para usuários gerenciados por serviços](#).

6. Em chave pública SSH, insira a parte da chave pública SSH do par de chaves SSH.

Sua chave é validada pelo serviço antes que você possa adicionar o novo usuário. O formato da chave SSH é `ssh-rsa string`. Para gerar um par de chaves SSH, consulte [Gere chaves SSH para usuários gerenciados por serviços](#).

7. Escolha Adicionar chave.

Para excluir uma chave pública SSH para um usuário

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores.
3. Escolha o identificador na coluna ID do servidor para ver a página Configuração do servidor.
4. Em Usuários, escolha um nome de usuário para ver a página de Detalhes do usuário.
5. Para excluir uma chave pública, marque a caixa de seleção da chave SSH e escolha Excluir.

Trabalhar com provedores de identidade personalizados

AWS Transfer Family oferece várias opções para provedores de identidade personalizados autenticarem e autorizarem usuários para transferências seguras de arquivos. Aqui estão as principais abordagens:

- [Solução personalizada de provedor de identidade](#)—Este tópico descreve a solução de provedor de identidade personalizada da Transfer Family, usando um kit de ferramentas hospedado em GitHub

 Note

Para a maioria dos casos de uso, essa é a opção recomendada. Especificamente, se você precisar oferecer suporte a mais de 100 grupos do Active Directory, a solução personalizada do provedor de identidade oferece uma alternativa escalável sem limitações de grupo. Essa solução é descrita na postagem do blog [Simplifique a autenticação do Active Directory com um provedor de identidade personalizado para AWS Transfer Family](#).

- [Usando para integrar seu provedor de identidade](#)—Este tópico descreve como usar uma AWS Lambda função para apoiar um método do Amazon API Gateway.

Você pode fornecer uma interface RESTful com um único método do Amazon API Gateway. O Transfer Family chama esse método para se conectar ao seu provedor de identidade, que autentica e autoriza seus usuários a acessar o Amazon S3 ou o Amazon EFS. Use essa opção se precisar de uma API RESTful para integrar seu provedor de identidade ou se quiser usá-la para aproveitar seus recursos AWS WAF para solicitações de bloqueio geográfico ou limitação de taxa. Para obter detalhes, consulte [Usando para integrar seu provedor de identidade](#).

- [Abordagens dinâmicas de gerenciamento de permissões](#)—Este tópico descreve abordagens para gerenciar dinamicamente as permissões do usuário usando políticas de sessão.

Para autenticar seus usuários, é possível usar seu provedor de identidade existente com AWS Transfer Family. Você integra seu provedor de identidade usando uma função AWS Lambda, que autentica e autoriza seus usuários a acessarem o Amazon S3 ou o Amazon Elastic File System (Amazon EFS). Para obter detalhes, consulte [Usando AWS Lambda para integrar seu provedor de identidade](#). Você também pode acessar CloudWatch gráficos de métricas como o número de arquivos e bytes transferidos no AWS Transfer Family Management Console, oferecendo um único painel para monitorar as transferências de arquivos usando um painel centralizado.

- O Transfer Family fornece uma postagem no blog e um workshop que orientam você na criação de uma solução de transferência de arquivos. Essa solução usa AWS Transfer Family SFTP/FTPS endpoints gerenciados e Amazon Cognito e DynamoDB para gerenciamento de usuários.

A postagem do blog está disponível em [Usando o Amazon Cognito como provedor de identidade com AWS Transfer Family o Amazon S3](#). Você pode ver os detalhes do workshop [aqui](#).

 Note

Para provedores de identidade personalizados, o nome de usuário deve ter no mínimo 3 e no máximo 100 caracteres. Você pode usar os seguintes caracteres no nome de usuário: a—z, 0—9 A-Z, sublinhado '_', hífen '-', ponto '.' e sinal de arroba '@'. O nome de usuário não pode começar com um hífen '-', ponto '.' ou com o sinal '@'.

Ao implementar um provedor de identidade personalizado, considere as seguintes práticas recomendadas:

- Implante a solução na mesma Conta da AWS região dos seus servidores Transfer Family.
- Implemente o princípio do menor privilégio ao configurar as funções e políticas do IAM.
- Use recursos como lista de permissões de IP e registro padronizado para aumentar a segurança.
- Teste minuciosamente seu provedor de identidade personalizado em um ambiente que não seja de produção antes da implantação.

Tópicos

- [Solução personalizada de provedor de identidade](#)
- [Usando AWS Lambda para integrar seu provedor de identidade](#)
- [Usando para integrar seu provedor de identidade](#)
- [Usando vários métodos de autenticação](#)
- [Suporte IPv6 para provedores de identidade personalizados](#)

Solução personalizada de provedor de identidade

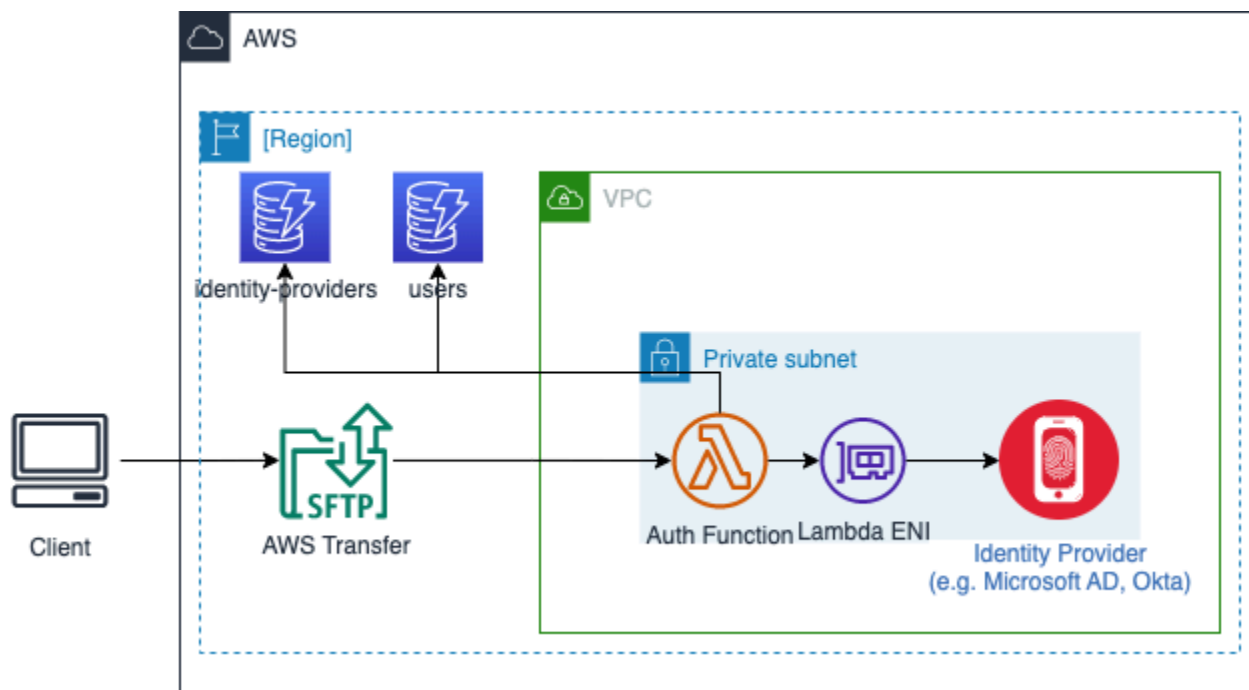
A solução de provedor de identidade AWS Transfer Family personalizada é uma solução modular de provedor de identidade personalizada que resolve muitos casos de uso comuns de autenticação e autorização que as empresas têm ao implementar o serviço. Essa solução fornece uma base reutilizável para a implementação de provedores de identidade personalizados com configuração granular por sessão por usuário e separa a lógica de autenticação e autorização, oferecendo uma base flexível e fácil de manter para vários casos de uso.

Com a solução AWS Transfer Family personalizada de provedor de identidade, você pode abordar casos de uso comuns de autenticação e autorização corporativa. Essa solução modular oferece:

- Uma base reutilizável para implementar provedores de identidade personalizados
- Configuração granular de sessão por usuário
- Lógica separada de autenticação e autorização

Detalhes de implementação do kit de ferramentas de identidade personalizado

A solução fornece uma base flexível e sustentável para vários casos de uso. Para começar, revise o kit de ferramentas em <https://github.com/aws-samples/toolkit-for-aws-transfer-family> e siga as instruções de implantação na seção [Introdução](#).



Note

Se você já usou modelos e exemplos de provedores de identidade personalizados, considere adotar essa solução. No futuro, os módulos específicos do fornecedor padronizarão essa solução. A manutenção contínua e os aprimoramentos de recursos serão aplicados a essa solução.

Essa solução contém padrões padrão para implementar um provedor personalizado que considera os detalhes, incluindo o registro e onde armazenar os metadados adicionais da sessão necessários AWS Transfer Family, como o `HomeDirectoryDetails` parâmetro. Essa solução fornece uma base reutilizável para a implementação de provedores de identidade personalizados com

configuração granular por sessão por usuário e separa a lógica de autenticação do provedor de identidade da lógica reutilizável que cria uma configuração que é retornada à Transfer Family para concluir a autenticação e estabelecer configurações para a sessão.

O código e os recursos de suporte para essa solução estão disponíveis em <https://github.com/aws-samples/toolkit-for-aws-transfer-family>.

O kit de ferramentas contém os seguintes recursos:

- Um [AWS Serverless Application Model](#) modelo que provisiona os recursos necessários. Opcionalmente, implante e configure o Amazon API Gateway para incorporar AWS WAF, conforme descrito na postagem do blog [Protegendo AWS Transfer Family com o AWS Web Application Firewall e o Amazon API Gateway](#).
- Um esquema do [Amazon DynamoDB](#) para armazenar metadados de configuração sobre provedores de identidade, incluindo configurações de sessão do usuário, como, e. `HomeDirectoryDetails Role Policy`
- Uma abordagem modular que permite adicionar novos provedores de identidade à solução no futuro, como módulos.
- Recuperação de atributos: opcionalmente, recupere a função do IAM e os atributos do perfil POSIX (UID e GID) de provedores de identidade compatíveis, incluindo AD, LDAP e Okta.
- Suporte para vários provedores de identidade conectados a um único servidor Transfer Family e vários servidores Transfer Family usando a mesma implantação da solução.
- Built-in Verificação da lista de permissões de IP, como listas de permissões de IP que podem ser configuradas opcionalmente por usuário ou por provedor de identidade.
- Registro detalhado com nível de registro configurável e suporte de rastreamento para auxiliar na solução de problemas.

Antes de começar a implantar a solução de provedor de identidade personalizada, você precisa ter os seguintes AWS recursos.

- Uma Amazon Virtual Private Cloud (VPC) com sub-redes privadas, com conectividade com a Internet por meio de um gateway NAT ou de um endpoint de gateway do DynamoDB.
- Permissões apropriadas do IAM para realizar as seguintes tarefas:
 - Implante o `custom-idp.yaml` CloudFormation modelo,
 - Crie AWS CodePipeline projetos
 - Crie AWS CodeBuild projetos

- Crie funções e políticas do IAM

Important

Você deve implantar a solução na mesma Conta da AWS e Região da AWS que contenha seus servidores Transfer Family de destino.

Provedores de identidade compatíveis

A lista a seguir contém detalhes dos provedores de identidade compatíveis com a solução de provedor de identidade personalizada.

Fornecedor	Fluxos de senhas	Fluxos de chave pública	Multi-factor	Recuperação de atributos	Detalhes
Active Directory e LDAP	Sim	Sim	Não	Sim	A verificação do usuário pode ser realizada como parte do fluxo de autenticação de chave pública.
Argon2 (hash local)	Sim	Não	Não	Não	Os hashes Argon2 são armazenados no registro do usuário para casos de uso de autenticação “local” baseada em senha.

Fornecedor	Fluxos de senhas	Fluxos de chave pública	Multi-factor	Recuperação de atributos	Detalhes
Amazon Cognito	Sim	Não	Sim*	Não	Time-based One-Time Somente autenticação multifatorial baseada em senha (TOTP). * SMS-based O MFA não é suportado.
Insira o ID (antigo Azure AD)	Sim	Não	Não	Não	
Okta	Sim	Sim	Yes (Sim)	Sim	TOTP-based Somente MFA.
Chave pública	Não	Sim	Não	Não	As chaves públicas são armazenadas no registro do usuário no DynamoDB.
Secrets Manager	Sim	Sim	Não	Não	

Usando AWS Lambda para integrar seu provedor de identidade

Este tópico descreve como criar uma AWS Lambda função que se conecta ao seu provedor de identidade personalizado. Você pode usar qualquer provedor de identidade personalizado, como

Okta, Secrets Manager ou um armazenamento de dados personalizado que inclua lógica de autorização e autenticação. OneLogin

Para a maioria dos casos de uso, a forma recomendada de configurar um provedor de identidade personalizado é usar [Solução personalizada de provedor de identidade](#) o.

 Note

Antes de criar um servidor Transfer Family que usa o Lambda como provedor de identidade, você deve criar a função. Para obter um exemplo de função do Lambda, consulte [Exemplo de funções do Lambda](#). Ou você pode implantar uma CloudFormation pilha que usa um dos [Modelos de função do Lambda](#). Além disso, certifique-se de que sua função do Lambda use uma política baseada em recursos que confie no Transfer Family. Para visualizar um exemplo de política, consulte [Exemplo de política baseada em recursos do Lambda](#).

1. Abra o [console do AWS Transfer Family](#).
2. Escolha Criar servidor para abrir a página Criar servidor. Em Escolher um provedor de identidade, escolha Provedor de identidade personalizado, conforme mostrado na captura de tela a seguir.

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel

Previous

Next

Note

A escolha dos métodos de autenticação só estará disponível se você habilitar o SFTP como um dos protocolos do seu servidor Transfer Family.

3. Certifique-se de que o valor padrão, Usar AWS Lambda para conectar seu provedor de identidade, esteja selecionado.
4. Para a AWS Lambda Função, insira o nome da sua função do Lambda.

5. Preencha as caixas restantes e escolha Criar servidor. Para obter detalhes sobre as etapas restantes para criar um servidor, consulte [Configurando um endpoint de servidor SFTP, FTPS ou FTP](#).

Exemplo de política baseada em recursos do Lambda

Você deve ter uma política que faça referência ao servidor Transfer Family e aos ARNs do Lambda. Por exemplo, é possível usar a política a seguir com sua função do Lambda que se conecta ao seu provedor de identidade. A política tem um JSON de escape como uma string.

```
"Policy":
"{\"Version\":\"2012-10-17\",
  \"Id\":\"default\",
  \"Statement\":[
    {\"Sid\":\"AllowTransferInvocation\",
     \"Effect\":\"Allow\",
     \"Principal\":{\"Service\":\"transfer.amazonaws.com\"},
     \"Action\":\"lambda:InvokeFunction\",
     \"Resource\":\"arn:aws:lambda:region:123456789012:function:my-lambda-auth-
function\",
     \"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
\"arn:aws:transfer:region:123456789012:server/server-id\"}}}}
]}"
```

Note

No exemplo de política acima, substitua cada uma *user input placeholder* por suas próprias informações.

Estrutura de mensagens de evento

A estrutura da mensagem de evento do servidor SFTP enviada para a função do Lambda do autorizador para um IDP personalizado é a seguinte.

```
{
  "username": "value",
  "password": "value",
  "protocol": "SFTP",
```

```
"serverId": "s-abcd123456",  
"sourceIp": "192.168.0.100"  
}
```

Onde username e password são os valores das credenciais de login enviadas ao servidor.

Por exemplo, insira o seguinte comando para se conectar:

```
sftp bobusa@server_hostname
```

A senha será solicitada:

```
Enter password:  
mysecretpassword
```

É possível verificar isso na sua função do Lambda imprimindo o evento passado de dentro da função do Lambda. A aparência deve ser semelhante ao exemplo a seguir.

```
{  
  "username": "bobusa",  
  "password": "mysecretpassword",  
  "protocol": "SFTP",  
  "serverId": "s-abcd123456",  
  "sourceIp": "192.168.0.100"  
}
```

A estrutura do evento é semelhante para FTP e FTPS: a única diferença é que esses valores são usados para o parâmetro `protocol`, em vez de SFTP.

Funções do Lambda para autenticação

Para implementar diferentes estratégias de autenticação, edite a função do Lambda. Para ajudá-lo a atender às necessidades do seu aplicativo, você pode implantar uma CloudFormation pilha. Para obter mais informações sobre o Lambda, consulte o [Guia do AWS Lambda desenvolvedor](#) ou Como criar funções do [Lambda](#) com. Node.js

Tópicos

- [Valores do Lambda válidos](#)
- [Exemplo de funções do Lambda](#)
- [Testar a configuração](#)

- [Modelos de função do Lambda](#)

Valores do Lambda válidos

A tabela a seguir descreve os detalhes dos valores que o Transfer Family aceita para funções Lambda que são usadas para provedores de identidade personalizados.

Valor	Description	Obrigatório
Role	Especifica o nome do recurso da Amazon (ARN) do perfil do IAM que controla o acesso dos seus usuários ao bucket do Amazon S3 ou ao sistema de arquivos do Amazon EFS. As políticas anexadas a essa função determinam o nível de acesso que você deseja fornecer aos usuários durante a transferência de arquivos para dentro e para fora de seu sistema de arquivos do Amazon S3 ou Amazon EFS. O perfil do IAM também deve conter uma relação de confiança que permite o servidor acesse os recursos quando estiver servindo as solicitações de transferência dos usuários. Para obter informações sobre como estabelecer um relacionamento de confiança, consulte Estabelecer um relacionamento de confiança.	Obrigatório

Valor	Description	Obrigatório
PosixProfile	A identidade POSIX completa, incluindo ID de usuário (Uid), ID de grupo (Gid) e quaisquer IDs de grupos secundários (SecondaryGids), que controla o acesso de seus usuários aos sistemas de arquivos do Amazon EFS. As permissões POSIX definidas em arquivos e diretórios em seu sistema de arquivos determinam o nível de acesso que os usuários obtêm ao transferir arquivos para dentro e para fora de seus sistemas de arquivos do Amazon EFS.	Necessário para armazenamento secundário do Amazon EFS
PublicKeys	Uma lista de valores de chave pública SSH que são válidos para esse usuário. Uma lista vazia indica que esse não é um login válido. Não deve ser devolvido durante a autenticação por senha.	Opcional

Valor	Description	Obrigatório
Policy	Uma política de sessão para seu usuário, para que você possa usar o mesmo perfil do IAM do entre vários usuários. Esta política delimita o acesso do usuário a partes do bucket do Amazon S3. Para obter mais informações sobre o uso de políticas de sessão com provedores de identidade e personalizados, consulte os exemplos de políticas de sessão neste tópico.	Opcional

Valor	Description	Obrigatório
HomeDirectoryType	O tipo de diretório (pasta) inicial que você deseja que o diretório inicial dos usuários seja quando eles fizerem login no servidor. • Se você configurá-lo como PATH, o usuário vê os caminhos absolutos do bucket do Amazon S3 ou do EFS como estão em seus clientes de protocolo de transferência de arquivos. • Se você configurá-lo como LOGICAL, será necessário o fornecer mapeamentos no parâmetro HomeDirectoryDetails para tornar os caminhos do Amazon S3 ou do Amazon EFS visíveis para os usuários.	Opcional

Valor	Description	Obrigatório
HomeDirectoryDetails	Mapeamentos de diretório lógicos que especificam quais caminhos e chaves do Amazon S3 devem estar visíveis para o usuário e como você deseja torná-los visíveis. Você precisa especificar o par Entry e Target, onde Entry mostra como o caminho se tornou visível e Target é o caminho real do Amazon S3 ou Amazon EFS.	Obrigatório se HomeDirectoryType tiver um valor de LOGICAL

Valor	Description	Obrigatório
HomeDirectory	O diretório inicial de um usuário quando ele faz login no servidor usando o cliente. O formato depende do seu back-end de armazenamento: • Para o Amazon S3: / bucket-name/user-home-directory Exemplo: /amzn-s3-demo-bucket/users/john • Para o Amazon EFS: / fs-12345/user-home-directory Exemplo: /fs-faa1a123/users/john  Important O nome do bucket ou o ID do sistema de arquivos do Amazon EFS devem ser incluídos no caminho. A omissão dessas informações resultará em erros de “Arquivo não encontrado” durante as transferências de arquivos.	Opcional

Note

`HomeDirectoryDetails` O é uma representação em string de um mapa JSON. Isso contrasta com `PosixProfile`, que é um objeto de mapa JSON real e `PublicKeys` que é uma matriz JSON de strings. Veja os exemplos de código para obter detalhes específicos do idioma.

⚠ HomeDirectory Requisitos de formato

Ao usar o `HomeDirectory` parâmetro, certifique-se de incluir o formato completo do caminho:

- Para armazenamento no Amazon S3: sempre inclua o nome do bucket no formato `/bucket-name/path`
- Para armazenamento no Amazon EFS: sempre inclua o ID do sistema de arquivos no formato `/fs-12345/path`

Uma causa comum de erros de “Arquivo não encontrado” é omitir o nome do bucket ou o ID do sistema de arquivos EFS do `HomeDirectory` caminho. `HomeDirectory` Definir como apenas `/` sem o identificador de armazenamento fará com que a autenticação seja bem-sucedida, mas as operações de arquivo falhem.

Exemplo de funções do Lambda

Esta seção apresenta alguns exemplos de funções do Lambda, tanto em NodeJS quanto em Python.

Note

Nesses exemplos, o usuário, a função, o perfil POSIX, a senha e os detalhes do diretório inicial são todos exemplos e devem ser substituídos pelos valores reais.

Logical home directory, NodeJS

A função de exemplo do NodeJS a seguir fornece os detalhes de um usuário que tem um [diretório inicial lógico](#).

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
  // check the value of the server ID, only that it is provided.
  if (event.serverId !== "" && event.username == 'example-user') {
    var homeDirectoryDetails = [
      {
        Entry: "/",
        Target: "/fs-faa1a123"
      }
    ];
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
      // authenticated if and only if the Role field is not blank
      PosixProfile: {"Gid": 65534, "Uid": 65534}, // Required for EFS access, but
      // not needed for S3
      HomeDirectoryDetails: JSON.stringify(homeDirectoryDetails),
      HomeDirectoryType: "LOGICAL",
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
      // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
      // authentication failure
      response = {};
    }
  } else {
    // Return HTTP status 200 but with no role in the response to indicate
    // authentication failure
    response = {};
  }
  callback(null, response);
};
```

Path-based home directory, NodeJS

A função de exemplo do NodeJS a seguir fornece os detalhes de um usuário que tem um diretório inicial baseado no caminho.

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
  check the value of the server ID, only that it is provided.
  // There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
  (e.g., "127.0.0.1") to further restrict logins.
  if (event.serverId !== "" && event.username == 'example-user') {
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
      authenticated if and only if the Role field is not blank
      Policy: '', // Optional, JSON stringified blob to further restrict this user's
      permissions
      // HomeDirectory format depends on your storage backend:
      // For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
      users/john')
      // For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
      HomeDirectory: '/my-transfer-bucket/users/example-user' // S3 example -
      replace with your bucket name
      // HomeDirectory: '/fs-faa1a123/users/example-user' // EFS example - uncomment
      for EFS
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
      // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
      authentication failure
      response = {};
    }
  } else {
```

```
// Return HTTP status 200 but with no role in the response to indicate
authentication failure
response = {};
}
callback(null, response);
};
```

Logical home directory, Python

A função de exemplo do Python a seguir fornece os detalhes de um usuário que tem um [diretório inicial lógico](#).

```
# GetUserConfig Python Lambda with LOGICAL HomeDirectoryDetails
import json

def lambda_handler(event, context):
    print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

    response = {}

    # Check if the username presented for authentication is correct. This doesn't
    # check the value of the server ID, only that it is provided.
    if event['serverId'] != '' and event['username'] == 'example-user':
        homeDirectoryDetails = [
            {
                'Entry': '/',
                'Target': '/fs-faa1a123'
            }
        ]
        response = {
            'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
            # be authenticated if and only if the Role field is not blank
            'PosixProfile': {"Gid": 65534, "Uid": 65534}, # Required for EFS access, but
            # not needed for S3
            'HomeDirectoryDetails': json.dumps(homeDirectoryDetails),
            'HomeDirectoryType': "LOGICAL"
        }

    # Check if password is provided
    if event.get('password', '') == '':
        # If no password provided, return the user's SSH public key
        response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
```



```

    # Check if password is correct
    elif event['password'] != 'Password1234':
        # Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {}
    else:
        # Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {}

    return response

```

Path-based home directory, Python

A função de exemplo do Python a seguir fornece os detalhes de um usuário que tem um diretório inicial baseado no caminho.

```

# GetUserConfig Python Lambda with PATH HomeDirectory

def lambda_handler(event, context):
    print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

    response = {}

    # Check if the username presented for authentication is correct. This doesn't
    # check the value of the server ID, only that it is provided.
    # There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
    # (e.g., "127.0.0.1") to further restrict logins.
    if event['serverId'] != '' and event['username'] == 'example-user':
        response = {
            'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
            # be authenticated if and only if the Role field is not blank
            'Policy': '', # Optional, JSON stringified blob to further restrict this
            # user's permissions
            # HomeDirectory format depends on your storage backend:
            # For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
            # users/john')
            # For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
            'HomeDirectory': '/my-transfer-bucket/users/example-user', # S3 example -
            # replace with your bucket name
            # 'HomeDirectory': '/fs-faa1a123/users/example-user', # EFS example -
            # uncomment for EFS
            'HomeDirectoryType': "PATH" # Not strictly required, defaults to PATH

```

```
}

# Check if password is provided
if event.get('password', '') == '':
    # If no password provided, return the user's SSH public key
    response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
    # Check if password is correct
    elif event['password'] != 'Password1234':
        # Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {}
    else:
        # Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {}

return response
```

Testar a configuração

Depois de criar seu provedor de identidade personalizado, você deve testar sua configuração.

Console

Para testar sua configuração usando o AWS Transfer Family console

1. Abra o [console do AWS Transfer Family](#).
2. Na página Servidores, escolha seu novo servidor, escolha Ações e escolha Testar.
3. Insira o texto para Nome de usuário e Senha que você definiu ao implantar a CloudFormation pilha. Se você manteve as opções padrão, o nome de usuário é `myuser` e a senha é `MySuperSecretPassword`.
4. Escolha o protocolo do servidor e insira o endereço IP do IP de origem, se você os definiu ao implantar a CloudFormation pilha.

CLI

Para testar sua configuração usando a AWS CLI

1. Execute o comando [test-identity-provider](#). Substitua cada *user input placeholder* por suas próprias informações, conforme descrito nas etapas subsequentes.

```
aws transfer test-identity-provider --server-id s-1234abcd5678efgh --user-  
name myuser --user-password MySuperSecretPassword --server-protocol FTP --  
source-ip 127.0.0.1
```

2. Insira o ID do servidor.
3. Insira o nome de usuário e a senha que você definiu ao implantar a CloudFormation pilha. Se você manteve as opções padrão, o nome de usuário é `myuser` e a senha é `MySuperSecretPassword`.
4. Insira o protocolo do servidor e o endereço IP de origem, se você os tiver definido ao implantar a CloudFormation pilha.

Se a autenticação do usuário for bem-sucedida, o teste retornará uma resposta de HTTP `Status Code: 200`, uma string vazia `Message: ""` (que, caso contrário, conterá um motivo para a falha) e um campo `Response`.

Note

No exemplo de resposta abaixo, o campo `Response` é um objeto JSON que foi “stringificado” (convertido em uma string JSON simples que pode ser usada dentro de um programa) e contém os detalhes das funções e permissões do usuário.

```
{
  "Response": "{\\\"Policy\\\":\\\"{\\\"Version\\\":\\\"2012-10-17\\\",\\\"Statement\\\":  
[\\\"Sid\\\":\\\"ReadAndListAllBuckets\\\",\\\"Effect\\\":\\\"Allow\\\",\\\"Action\\\":  
[\\\"s3:ListAllMybuckets\\\",\\\"s3:GetBucketLocation\\\",\\\"s3:ListBucket\\\",  
\\\"s3:GetObjectVersion\\\",\\\"s3:GetObjectVersion\\\"],\\\"Resource\\\":\\\"*\\\"]}\\\",  
\\\"Role\\\":\\\"arn:aws:iam::000000000000:role/MyUserS3AccessRole\\\",\\\"HomeDirectory\\\":\\\"/  
\\\"}\\\",  
  \"StatusCode\": 200,  
  \"Message\": \"\"  
}
```

Modelos de função do Lambda

Você pode implantar uma CloudFormation pilha que usa uma função Lambda para autenticação. Fornecemos vários modelos que autenticam e autorizam seus usuários usando credenciais de login. Você pode modificar esses modelos ou AWS Lambda códigos para personalizar ainda mais o acesso do usuário.

Note

Você pode criar um FIPS-enabled AWS Transfer Family servidor CloudFormation especificando uma política de FIPS-enabled segurança em seu modelo. As políticas de segurança disponíveis estão descritas em [Políticas de segurança para AWS Transfer Family servidores](#)

Para criar uma CloudFormation pilha para usar na autenticação

1. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. Siga as instruções para implantar uma CloudFormation pilha a partir de um modelo existente em [Seleção de um modelo de pilha no Guia](#) do AWS CloudFormation usuário.
3. Use um dos modelos a seguir para criar uma função do Lambda para usar na autenticação no Transfer Family.

- [Modelo de pilha clássico \(Amazon Cognito\)](#)

Um modelo básico para criar um AWS Lambda para uso como provedor de identidade personalizado em AWS Transfer Family. Ele se autentica no Amazon Cognito para autenticação baseada em senha, e as chaves públicas são retornadas de um bucket do Amazon S3 se a autenticação baseada em chave pública for usada. Após a implantação, é possível modificar o código da função do Lambda para fazer algo diferente.

- [AWS Secrets Manager modelo de pilha](#)

Um modelo básico usado AWS Lambda com um AWS Transfer Family servidor para integrar o Secrets Manager como um provedor de identidade. Ele se autentica com base em uma entrada AWS Secrets Manager do formato `aws/transfer/server-id/username`. Além disso, o segredo deve conter os pares de valores-chave de todas as propriedades do usuário retornadas ao Transfer Family. Após a implantação, é possível modificar o código da função do Lambda para fazer algo diferente.

- [Modelo de pilha Okta](#): um modelo básico usado AWS Lambda com um AWS Transfer Family servidor para integrar o Okta como um provedor de identidade personalizado.
- [Okta-mfa modelo de pilha](#): um modelo básico usado AWS Lambda com um AWS Transfer Family servidor para integrar o Okta, com a autenticação multifator, como um provedor de identidade personalizado.
- [Modelo do Azure Active Directory](#): os detalhes dessa pilha estão descritos na postagem do blog [Autenticando AWS Transfer Family com o Azure Active Directory e. AWS Lambda](#)

Depois que a pilha for implantada, você poderá ver detalhes sobre ela na guia Saídas no console. CloudFormation

A implantação de uma dessas pilhas é a maneira mais fácil de integrar um provedor de identidade personalizado ao fluxo de trabalho do Transfer Family.

Usando para integrar seu provedor de identidade

Este tópico descreve como usar uma AWS Lambda função para apoiar um método do API Gateway. Use essa opção se precisar de uma API RESTful para integrar seu provedor de identidade ou se quiser usá-la para aproveitar seus recursos AWS WAF para solicitações de bloqueio geográfico ou limitação de taxa.

Para a maioria dos casos de uso, a forma recomendada de configurar um provedor de identidade personalizado é usar [Solução personalizada de provedor de identidade](#) o.

Limitações ao usar um API Gateway para integrar seu provedor de identidade

- Essa configuração não aceita domínios personalizados.
- Essa configuração não é compatível com um URL privado do API Gateway.

Se precisar de um desses, é possível usar o Lambda como provedor de identidade, sem o API Gateway. Para obter detalhes, consulte [Usando AWS Lambda para integrar seu provedor de identidade](#).

Autenticação usando um método do API Gateway

É possível criar um método API Gateway para ser usado como provedor de identidade para o Transfer Family. Essa abordagem fornece uma maneira altamente segura de criar e fornecer APIs.

Com o API Gateway, você pode criar um endpoint HTTPS para que todas as operações de entrada da API sejam transmitidas com maior segurança. Para obter mais detalhes sobre o serviço do API Gateway, consulte o [Guia do desenvolvedor do API Gateway](#).

O API Gateway oferece um método de autorização chamado `AWS_IAM`, que fornece a mesma autenticação baseada em AWS Identity and Access Management (IAM) AWS usada internamente. Se você ativar a autenticação com `AWS_IAM`, somente chamadores com permissões explícitas para chamar uma API poderão acessar o método API Gateway dessa API.

Para usar o método do API Gateway como provedor de identidade personalizado para o Transfer Family, ative o IAM para o método do API Gateway. Como parte desse processo, você fornece um perfil do IAM com permissões para o Transfer Family usar seu gateway.

 Note

Para melhorar a segurança, é possível configurar um firewall para aplicações Web. O AWS WAF é um firewall para aplicações Web que permite monitorar as solicitações HTTP e HTTPS que são encaminhadas ao Amazon API Gateway. Para obter detalhes, consulte [Adicione um firewall da aplicação web](#).

 Não habilite o armazenamento em cache do API Gateway

Não habilite o armazenamento em cache para seu método API Gateway ao usá-lo como um provedor de identidade personalizado para Transfer Family. O armazenamento em cache é impróprio e inválido para solicitações de autenticação porque:

- Cada solicitação de autenticação é exclusiva e requer uma resposta ativa, não uma resposta em cache
- O armazenamento em cache não oferece benefícios, pois o Transfer Family nunca envia solicitações duplicadas ou repetidas para o API Gateway.
- A ativação do armazenamento em cache fará com que o API Gateway responda com dados incompatíveis, resultando em respostas inválidas às solicitações de autenticação

Para usar seu método API Gateway para autenticação personalizada com o Transfer Family

1. Crie uma CloudFormation pilha. Para fazer isso:

 Note

Os modelos de pilha foram atualizados para usar BASE64-encoded senhas: para obter detalhes, consulte [Melhorias nos CloudFormation modelos](#).

- a. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
- b. Siga as instruções para implantar uma CloudFormation pilha a partir de um modelo existente em [Seleção de um modelo de pilha no Guia](#) do AWS CloudFormation usuário.
- c. Use um dos modelos básicos a seguir para criar um método API Gateway suportado por AWS Lambda para uso como provedor de identidade personalizado no Transfer Family.

- [Modelo básico de pilha](#)

Por padrão, seu método API Gateway é usado como um provedor de identidade personalizado para autenticar um único usuário em um único servidor usando uma chave ou senha SSH (Secure Shell) codificada. Após a implantação, é possível modificar o código da função do Lambda para fazer algo diferente.

- [AWS Secrets Manager modelo de pilha](#)

Por padrão, seu método API Gateway é autenticado em uma entrada no Secrets Manager do formato `aws/transfer/server-id/username`. Além disso, o segredo deve conter os pares de valores-chave de todas as propriedades do usuário retornadas ao Transfer Family. Após a implantação, é possível modificar o código da função do Lambda para fazer algo diferente. Para obter mais informações, consulte a postagem do blog [Habilitar a autenticação por senha para AWS Transfer Family uso AWS Secrets Manager](#).

- [Modelo de pilha Okta](#)

Seu método API Gateway se integra ao Okta como um provedor de identidade personalizado no Transfer Family. Para obter mais informações, consulte a postagem de blog [Usar o Okta como provedor de identidade com AWS Transfer Family](#).

A implantação de uma dessas pilhas é a maneira mais fácil de integrar um provedor de identidade personalizado ao fluxo de trabalho do Transfer Family. Cada pilha usa a função do Lambda para oferecer suporte ao seu método de API com base no API Gateway. Em seguida, é possível usar seu método de API como um provedor de identidade personalizado no Transfer

Family. Por padrão, a função do Lambda autentica um único usuário chamado `myuser` com uma senha de `MySuperSecretPassword`. Após a implantação, é possível editar essas credenciais ou atualizar o código da função do Lambda para fazer algo diferente.

 Important

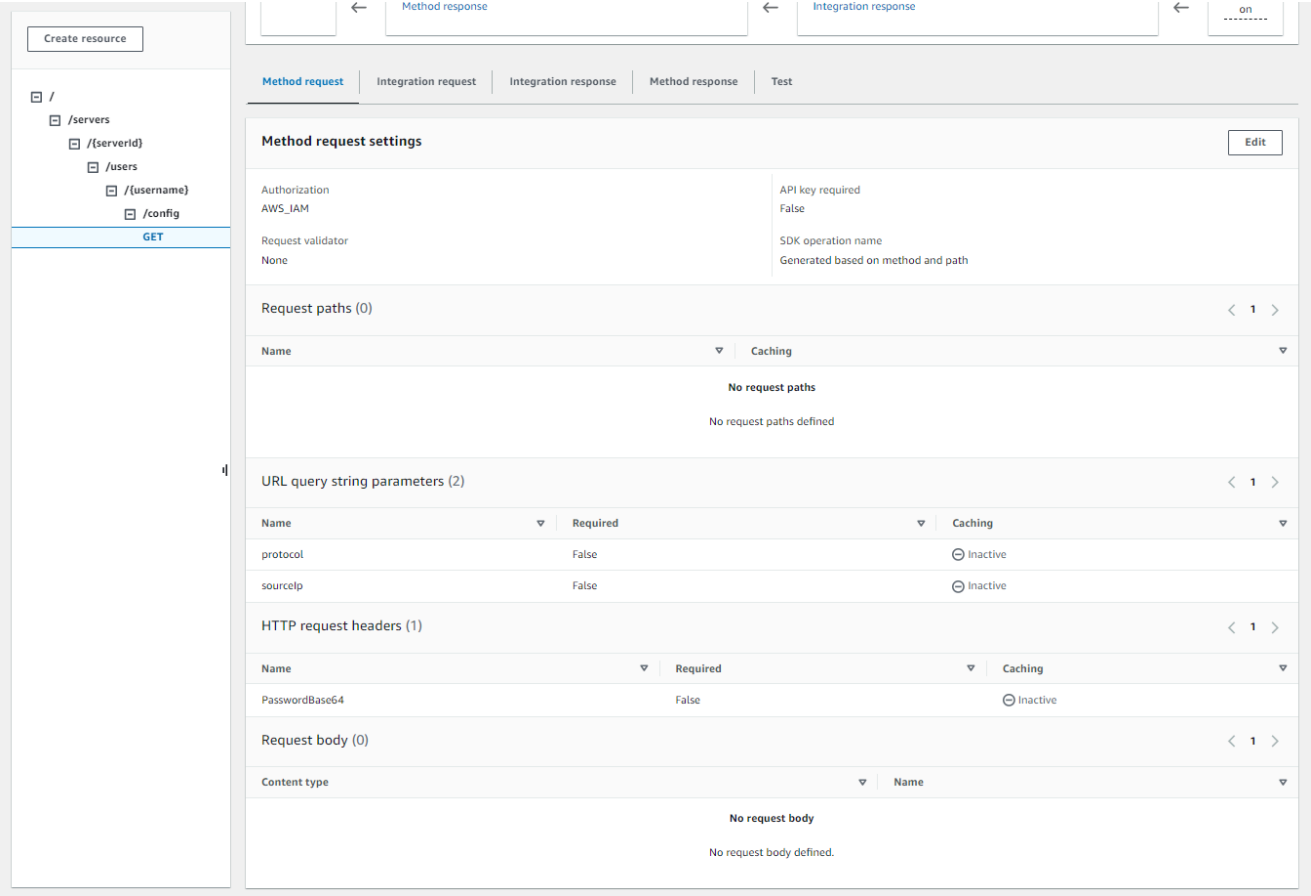
Recomendamos que você edite as credenciais padrão de usuário e senha.

Depois que a pilha for implantada, você poderá ver detalhes sobre ela na guia Saídas no console. CloudFormation Esses detalhes incluem o nome do recurso da Amazon (ARN) da pilha, o ARN do perfil do IAM que a pilha criou e o URL do seu novo gateway.

 Note

Se você estiver usando a opção de provedor de identidade personalizado para habilitar a autenticação baseada em senha para seus usuários e ativar o registro de solicitações e respostas fornecido pelo API Gateway, o API Gateway registrará as senhas dos seus usuários no Amazon Logs. CloudWatch Não recomendamos usar esse log em seu ambiente de produção. Para obter mais informações, consulte [Configurar o registro de CloudWatch API no API Gateway](#) no Guia do desenvolvedor do API Gateway.

2. Verifique a configuração do método API Gateway para seu servidor. Para fazer isso:
 - a. Abra o console do API Gateway em <https://console.aws.amazon.com/apigateway/>.
 - b. Escolha a API de modelo básico do Transfer Custom Identity Provider que o CloudFormation modelo gerou. Talvez seja necessário selecionar sua região para ver seus gateways.
 - c. No painel Recursos, escolha OBTER. A captura de tela a seguir mostra a configuração correta do método.



Neste ponto, seu API gateway está pronto para ser implantado.

3. Escolha Ações e Implantar API. Para o Estágio de implantação, escolha prod e Implantar.

Depois que o método API Gateway for implantado com sucesso, veja seu desempenho em Estágios > Detalhes do estágio, conforme mostrado na captura de tela a seguir.

 Note

Copie o endereço do URL de invocação que aparece na parte superior da tela. Talvez você precise dele para a próxima etapa.

API Gateway > APIs > Transfer Custom Identity Provider basic template API > Stages

Stages

Stage actions ▼ Create stage

prod

Stage details info

Stage name: prod

API cache: ☐ Inactive

Rate: 10000

Burst: 5000

Web ACL: -

Client certificate: -

Invoke URL: <https://execute-api.us-east-1.amazonaws.com/prod>

Active deployment: t8aqrn on December 12, 2023, 10:49 (UTC-05:00)

Logs and tracing info

CloudWatch logs: Error and info logs

Detailed metrics: ☐ Inactive

X-Ray tracing: ☐ Inactive

Custom access logging: ☐ Inactive

Stage variables (0/0)

Find resources

Name	Value
No variables	

No variables associated with the stage.

Manage variables

4. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
5. Uma Transfer Family deveria ter sido criada para você quando você criou a pilha. Caso contrário, configure seu servidor usando essas etapas.
 - a. Escolha Criar servidor para abrir a página Criar servidor. Em Escolher um provedor de identidade, escolha Personalizado e, em seguida, selecione Usar Amazon API Gateway para se conectar ao seu provedor de identidade, conforme mostrado na captura de tela a seguir.

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

☐ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☒ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

Provide an Amazon API Gateway URL

Role
IAM role for the service to invoke your Amazon API Gateway URL

- b. Na caixa de texto Fornecer um URL do Amazon API Gateway, cole o endereço do URL de invocação do endpoint do API Gateway que você criou na etapa 3 deste procedimento.
- c. Em Role, escolha a função do IAM que foi criada pelo CloudFormation modelo. Essa função permite que o Transfer Family invoque seu método de gateway de API.

A função de invocação contém o nome da CloudFormation pilha que você selecionou para a pilha que você criou na etapa 1. Tem o seguinte formato: *CloudFormation-stack-name-TransferIdentityProviderRole-ABC123DEF456GHI*.

- d. Preencha as caixas restantes e escolha Criar servidor. Para obter detalhes sobre as etapas restantes para criar um servidor, consulte [Configurando um endpoint de servidor SFTP, FTPS ou FTP](#).

Implementar seu método do API Gateway

Para criar um provedor de identidade personalizado para o Transfer Family, seu método API Gateway deve implementar um único método que tenha um caminho de recurso de `/servers/{serverId}/users/{username}/config`. Os valores `serverId` e `username` são originados do caminho de recurso RESTful. Além disso, adicione `sourceIp` e `protocol` como Parâmetros de sequência de caracteres de consulta do URL na solicitação de método, conforme mostrado na imagem a seguir.

The screenshot displays the AWS API Gateway console interface for configuring a GET method. On the left, a sidebar shows the resource tree with the path `/servers/{serverId}/users/{username}/config` selected. The main area shows the 'Method request settings' for the GET method. Key settings include: Authorization set to 'AWS_IAM', Request validator set to 'None', API key required set to 'False', and SDK operation name set to 'Generated based on method and path'. Below these settings, the 'Request paths' section is empty, indicating 'No request paths defined'. The 'URL query string parameters' section lists two parameters: 'protocol' and 'sourceIp', both of which are not required and have caching set to 'Inactive'.

Note

O nome de usuário deve ter no mínimo 3 e no máximo 100 caracteres. Você pode usar os seguintes caracteres no nome de usuário: a—z, 0—9 A-Z, sublinhado '_', hífen '-', ponto '.' e sinal de arroba '@'. O nome de usuário não pode começar com um hífen '-', ponto '.' ou com o sinal '@'.

Se o Transfer Family tentar uma autenticação de senha para o usuário, o serviço fornecerá um campo de cabeçalho `Password:`. Na ausência de um cabeçalho `Password:`, o Transfer Family tenta a autenticação por chave pública para autenticar seu usuário.

Ao usar um provedor de identidade para autenticar e autorizar usuários finais, além de validar suas credenciais, é possível permitir ou negar solicitações de acesso com base nos endereços IP dos clientes usados por seus usuários finais. É possível usar esse atributo para garantir que os dados armazenados em seus buckets do S3 ou em seu sistema de arquivos Amazon EFS possam ser acessados por meio dos protocolos suportados somente a partir de endereços IP que você especificou como confiáveis. Para ativar esse atributo, você deve incluir `sourceIp` na sequência de caracteres de consulta.

Se você tiver vários protocolos habilitados para seu servidor, e quiser fornecer acesso usando o mesmo nome de usuário em vários protocolos, poderá fazer isso desde que as credenciais específicas para cada protocolo tenham sido configuradas no seu provedor de identidade. Para habilitar esse atributo, você deve incluir o valor `protocol` no caminho do recurso RESTful.

Seu método do API Gateway deve sempre retornar o código de status HTTP 200. Qualquer outro código de status HTTP indica um erro ao acessar a API.

Resposta de exemplo do Amazon S3

O corpo de resposta do exemplo é um documento JSON do seguinte formato para o Amazon S3.

```
{
  "Role": "IAM role with configured S3 permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
    "ssh-rsa public-key2"
  ],
  "Policy": "STS Assume role session policy",
  "HomeDirectory": "/amzn-s3-demo-bucket/path/to/home/directory"
}
```

Note

A política tem um JSON de escape como uma string. Por exemplo:

```
"Policy":
```

```
"{
  \"Version\": \"2012-10-17\",
  \"Statement\":
    [
      {\"Condition\":
        {\"StringLike\":
          {\"s3:prefix\":
            [\"user/*\", \"user/\"]}},
        \"Resource\": \"arn:aws:s3:::amzn-s3-demo-bucket\",
        \"Action\": \"s3:ListBucket\",
        \"Effect\": \"Allow\",
        \"Sid\": \"ListHomeDir\",
        {\"Resource\": \"arn:aws:s3:::*\",
          \"Action\": [\"s3:PutObject\",
            \"s3:GetObject\",
            \"s3:DeleteObjectVersion\",
            \"s3:DeleteObject\",
            \"s3:GetObjectVersion\",
            \"s3:GetObjectACL\",
            \"s3:PutObjectACL\"],
          \"Effect\": \"Allow\",
          \"Sid\": \"HomeDirObjectAccess\"]}
      }
    ]
}
```

O exemplo de resposta a seguir mostra que um usuário tem um tipo de diretório inicial lógico.

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\", \"Target\": \"/amzn-s3-demo-bucket1\"}]",
  "PublicKeys": ["" ]
}
```

Exemplo de resposta do Amazon EFS

O corpo de resposta do exemplo é um documento JSON do seguinte formato para o Amazon EFS.

```
{
  "Role": "IAM role with configured EFS permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
  ]
}
```

```

    "ssh-rsa public-key2"
  ],
  "PosixProfile": {
    "Uid": "POSIX user ID",
    "Gid": "POSIX group ID",
    "SecondaryGids": [Optional list of secondary Group IDs],
  },
  "HomeDirectory": "/fs-id/path/to/home/directory"
}

```

O campo `Role` indica que ocorreu uma autenticação bem-sucedida. Ao fazer a autenticação por senha (quando você fornece um cabeçalho `Password:`), você não precisa fornecer chaves públicas SSH. Se um usuário não puder ser autenticado, por exemplo, se a senha estiver incorreta, seu método deverá retornar uma resposta sem um `Role` definido. Um exemplo dessa resposta é um objeto JSON vazio.

O exemplo de resposta a seguir mostra um usuário que tem um tipo de diretório inicial lógico.

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"/\", \"Target\": \"/faa1a123\"}]",
  "PublicKeys": [""],
  "PosixProfile": {"Uid": "65534", "Gid": "65534"}
}

```

É possível incluir políticas de usuário na função do Lambda no formato JSON. Para obter mais informações sobre a configuração de políticas de usuário no Transfer Family, consulte [Gerenciar controles de acesso](#).

Função do Lambda padrão

Para implementar diferentes estratégias de autenticação, edite a função do Lambda que seu gateway usa. Para ajudá-lo a atender às necessidades do seu aplicativo, você pode usar os seguintes exemplos de funções Lambda em Node.js. Para obter mais informações sobre o Lambda, consulte o [Guia do AWS Lambda desenvolvedor](#) ou Como criar funções do [Lambda](#) com Node.js.

O exemplo a seguir da função do Lambda usa seu nome de usuário, senha (se você estiver executando a autenticação por senha), ID do servidor, protocolo e endereço IP do cliente. É possível usar uma combinação dessas entradas para pesquisar seu provedor de identidade e determinar se o login deve ser aceito.

 Note

Se você tiver vários protocolos habilitados para seu servidor e quiser fornecer acesso usando o mesmo nome de usuário em vários protocolos, poderá fazer isso desde que as credenciais específicas do protocolo tenham sido configuradas no seu provedor de identidade.

Para File Transfer Protocol (FTP), recomendamos manter credenciais separadas do Secure Shell (SFTP) e File Transfer Protocol (SFTP) e File Transfer Protocol (FTP). Recomendamos manter credenciais separadas para o FTP porque, diferentemente do SFTP e do FTPS, o FTP transmite as credenciais em texto não criptografado. Ao isolar as credenciais de FTP do SFTP ou FTPS, se as credenciais de FTP forem compartilhadas ou expostas, suas cargas de trabalho usando SFTP ou FTPS permanecerão seguras.

Essa função de exemplo retorna a função e os detalhes do diretório inicial lógico, junto com as chaves públicas (se ela realizar a autenticação por chave pública).

Ao criar usuários gerenciados por serviços, você define o diretório inicial, lógico ou físico. Da mesma forma, precisamos dos resultados da função do Lambda para transmitir a estrutura de diretórios física ou lógica desejada pelo usuário. Os parâmetros definidos dependem do valor do campo [HomeDirectoryType](#).

- `HomeDirectoryType` definido como `PATH` — o `HomeDirectory` campo deve então ser um prefixo absoluto do bucket do Amazon S3 ou um caminho absoluto do Amazon EFS que seja visível para seus usuários.
- `HomeDirectoryType` definido como `LOGICAL` — Não defina um campo `HomeDirectory`. Em vez disso, definimos um `HomeDirectoryDetails` campo que fornece os `Entry/Target` mapeamentos desejados, semelhantes aos valores descritos no [HomeDirectoryDetails](#) parâmetro para usuários gerenciados por serviços.

As funções de exemplo estão listadas em [Exemplo de funções do Lambda](#).

Função Lambda para uso com AWS Secrets Manager

Para usar AWS Secrets Manager como seu provedor de identidade, você pode trabalhar com a função Lambda no modelo de amostra CloudFormation . A função do Lambda consulta o serviço Secrets Manager com suas credenciais e, se for bem-sucedida, retorna um segredo designado. Para ter mais informações sobre o Secrets Manager, consulte o [Guia do usuário do AWS Secrets Manager](#).

Para baixar um CloudFormation modelo de amostra que usa essa função Lambda, acesse o bucket do [Amazon S3 fornecido](#) pela AWS Transfer Family

Melhorias nos CloudFormation modelos

Melhorias na interface do API Gateway foram feitas nos CloudFormation modelos publicados. Os modelos agora usam BASE64-encoded senhas com o API Gateway. Suas implantações existentes continuam funcionando sem esse aprimoramento, mas não permitem senhas com caracteres fora do conjunto básico de US-ASCII caracteres.

As alterações no modelo que habilitam esse recurso são as seguintes:

- O `GetUserConfigRequest` `AWS::ApiGateway::Method` recurso precisa ter esse `RequestTemplates` código (a linha em itálico é a linha atualizada)

```
RequestTemplates:
  application/json: |
    {
      "username": "$util.urlDecode($input.params('username'))",
      "password":
        "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll('\\"', '\"')",
      "protocol": "$input.params('protocol')",
      "serverId": "$input.params('serverId')",
      "sourceIp": "$input.params('sourceIp')"
    }
```

- O `RequestParameters` formulário do `GetUserConfig` recurso deve ser alterado para usar o `PasswordBase64` cabeçalho (a linha em itálico é a linha atualizada):

```
RequestParameters:
  method.request.header.PasswordBase64: false
  method.request.querystring.protocol: false
  method.request.querystring.sourceIp: false
```

Para verificar se o modelo da sua pilha é o mais recente

1. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. Na lista de pilhas, escolha sua pilha.
3. No painel de detalhes, escolha a guia Modelo.

4. Procure o seguinte:

- Pesquise RequestTemplates e verifique se você tem esta linha:

```
"password":  
  "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(  
    \\'',\"'\")",
```

- Pesquise RequestParameters e verifique se você tem esta linha:

```
method.request.header.PasswordBase64: false
```

Se você não vê as linhas atualizadas, edite sua pilha. Para obter detalhes sobre como atualizar sua CloudFormation pilha, consulte [Modificar um modelo de pilha](#) no AWS CloudFormation; Guia do usuário.

Usando vários métodos de autenticação

O servidor Transfer Family controla a lógica AND quando você usa vários métodos de autenticação. A Transfer Family trata isso como duas solicitações separadas para seu provedor de identidade personalizado: no entanto, seus efeitos são combinados.

Ambas as solicitações devem retornar com êxito com a resposta correta para permitir que a autenticação seja concluída. O Transfer Family exige que as duas respostas sejam completas, o que significa que elas contêm todos os elementos necessários (função, diretório inicial, política e perfil POSIX se você estiver usando o Amazon EFS para armazenamento). O Transfer Family também exige que a resposta da senha não inclua chaves públicas.

A solicitação de chave pública deve ter uma resposta separada do provedor de identidade. Esse comportamento permanece inalterado ao usar Senha OU Chave ou Senha E Chave.

O SSH/SFTP protocolo desafia o cliente de software primeiro com uma autenticação de chave pública e, em seguida, solicita uma autenticação por senha. Essa operação exige que ambas sejam bem-sucedidas antes que o usuário possa concluir a autenticação.

Para opções personalizadas de provedor de identidade, você pode especificar qualquer uma das opções a seguir sobre como autenticar.

- Senha OU chave — os usuários podem se autenticar com sua senha ou chave. Este é o valor padrão.

- **SOMENTE senha** — os usuários devem fornecer sua senha para se conectar.
- **SOMENTE CHAVE** — os usuários devem fornecer sua chave privada para se conectar.
- **Senha e chave** — os usuários devem fornecer a chave privada e a senha para se conectar. O servidor verifica a chave em primeiro lugar e, em seguida, se a chave for válida, o sistema solicitará uma senha. Se a chave privada fornecida não for correspondente à chave pública armazenada, a autenticação falhará.

Suporte IPv6 para provedores de identidade personalizados

AWS Transfer Family provedores de identidade personalizados oferecem suporte total às conexões IPv6. Ao implementar um provedor de identidade personalizado, sua função Lambda pode receber e processar solicitações de autenticação de clientes IPv4 e IPv6 sem nenhuma configuração adicional. A função Lambda recebe o endereço IP do cliente no `sourceIp` campo da solicitação, que pode ser um endereço IPv4 (por exemplo, `203.0.113.42`) ou um endereço IPv6 (por exemplo, `2001:db8:85a3:8d3:1319:8a2e:370:7348`). A implementação do seu provedor de identidade personalizado deve lidar com os dois formatos de endereço de forma adequada.

Important

Se seu provedor de identidade personalizado realizar IP-based validação ou registro, certifique-se de que sua implementação manipule adequadamente os formatos de endereço IPv6. Os endereços IPv6 são maiores que os endereços IPv4 e usam um formato de notação diferente.

Note

Ao lidar com endereços IPv6 em seu provedor de identidade personalizado, certifique-se de usar funções adequadas de análise de endereços IPv6 em vez de simples comparações de strings. Os endereços IPv6 podem ser representados em vários formatos canônicos (por exemplo, `fd00:b600::ec2` ou `fd00:b600:0:0:0:0:ec2`). Use bibliotecas de endereços IPv6 ou funções apropriadas em sua linguagem de implementação para validar e comparar corretamente os endereços IPv6.

Exemplo Tratamento de endereços IPv4 e IPv6 em um provedor de identidade personalizado

```
def lambda_handler(event, context):
    # Extract the source IP address from the request
    source_ip = event.get('sourceIp', '')

    # Log the client IP address (works for both IPv4 and IPv6)
    print(f"Authentication request from: {source_ip}")

    # Example of IP-based validation that works with both IPv4 and IPv6
    if is_ip_allowed(source_ip):
        # Continue with authentication
        # ...
    else:
        # Reject the authentication request
        return {
            "Role": "",
            "HomeDirectory": "",
            "Status": "DENIED"
        }
```

Para obter mais informações sobre a implementação de provedores de identidade personalizados, consulte [Usando AWS Lambda para integrar seu provedor de identidade](#).

Usando o AWS Directory Service para o Microsoft Active Directory

Você pode usar AWS Transfer Family para autenticar seus usuários finais de transferência de arquivos usando AWS Directory Service for Microsoft Active Directory. Ele permite a migração perfeita de fluxos de trabalho de transferência de arquivos que dependem da autenticação do Active Directory sem alterar as credenciais dos usuários finais ou precisar de um autorizador personalizado.

Com AWS Managed Microsoft AD, você pode fornecer acesso seguro a Directory Service usuários e grupos via SFTP, FTPS e FTP para dados armazenados no Amazon Simple Storage Service (Amazon S3) ou no Amazon Elastic File System (Amazon EFS). Se você usa o Active Directory para armazenar as credenciais de seus usuários, agora tem uma maneira mais fácil de habilitar transferências de arquivos para esses usuários.

Você pode fornecer acesso aos grupos do Active Directory AWS Managed Microsoft AD em seu ambiente local ou na AWS nuvem usando conectores do Active Directory. Você pode dar aos usuários que já estão configurados em seu ambiente Microsoft Windows, na AWS nuvem ou em sua

rede local, acesso a um AWS Transfer Family servidor que usa AWS Managed Microsoft AD como identidade. O blog AWS de armazenamento contém uma postagem que detalha uma solução para usar o Active Directory com o Transfer Family: [Simplifique a autenticação do Active Directory com um provedor de identidade personalizado para AWS Transfer Family](#).

 Note

- AWS Transfer Family não é compatível com Simple AD.
- O Transfer Family não é compatível com as configurações entre regiões do Active Directory: oferecemos suporte apenas às integrações do Active Directory que estejam na mesma região do servidor Transfer Family.
- O Transfer Family não suporta o uso de nenhum deles AWS Managed Microsoft AD nem do AD Connector para habilitar a autenticação multifator (MFA) para sua infraestrutura de RADIUS-based MFA existente.
- AWS Transfer Family não oferece suporte a regiões replicadas do Managed Active Directory.

Para usar AWS Managed Microsoft AD, você deve executar as seguintes etapas:

1. Crie um ou mais AWS Managed Microsoft AD diretórios usando o Directory Service console.
2. Use o console Transfer Family para criar um servidor que use AWS Managed Microsoft AD como provedor de identidade.
3. Configure o AWS Directory usando um conector do Active Directory.
4. Adicione acesso de um ou mais dos seus Directory Service grupos.
5. Embora não seja obrigatório, recomendamos que você teste e verifique o acesso do usuário.

Tópicos

- [Antes de começar a usar AWS Directory Service for Microsoft Active Directory](#)
- [Trabalhando com realms do Active Directory](#)
- [Escolhendo AWS Managed Microsoft AD como seu provedor de identidade](#)
- [Conectando-se ao Microsoft Active Directory local](#)
- [Como conceder acesso a grupos](#)

- [Testando usuários](#)
- [Como excluir o acesso ao servidor para um grupo](#)
- [Como se conectar ao servidor usando SSH \(Secure Shell\)](#)
- [Conectando-se AWS Transfer Family a um Active Directory autogerenciado usando florestas e relações de confiança](#)

Antes de começar a usar AWS Directory Service for Microsoft Active Directory

Note

AWS Transfer Family tem um limite padrão de 100 grupos do Active Directory por servidor. Se seu caso de uso exigir mais de 100 grupos, considere usar uma solução de provedor de identidade personalizada, conforme descrito em [Simplifique a autenticação do Active Directory com um provedor de identidade personalizado para AWS Transfer Family](#).

Forneça um identificador exclusivo para seus grupos do AD

Antes de poder usar AWS Managed Microsoft AD, você deve fornecer um identificador exclusivo para cada grupo em seu diretório do Microsoft AD. É possível usar o identificador de segurança (SID) de cada grupo para fazer isso. Os usuários do grupo que você associa têm acesso aos seus recursos do Amazon S3 ou do Amazon EFS por meio dos protocolos habilitados usando o AWS Transfer Family.

Use o seguinte PowerShell comando do Windows para recuperar o SID de um grupo, *YourGroupName* substituindo-o pelo nome do grupo.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select SamAccountName, ObjectSid
```

Note

Se você estiver usando AWS Directory Service como seu provedor de identidade `userPrincipalName` e `SamAccountName` tiver valores diferentes, AWS Transfer Family aceite o valor em `SamAccountName`. O Transfer Family não aceita o valor especificado em `userPrincipalName`.

Adicione Directory Service permissões à sua função

Você também precisa de permissões de Directory Service API para usar AWS Directory Service como seu provedor de identidade. As seguintes permissões são necessárias ou sugeridas:

- `ds:DescribeDirectories` é necessária para que o Transfer Family procure o diretório
- `ds:AuthorizeApplication` é necessária para adicionar autorização para o Transfer Family
- `ds:UnauthorizeApplication` é sugerida para remover todos os recursos criados provisoriamente, caso algo dê errado durante o processo de criação do servidor

Adicione essas permissões à função que você está usando para criar seus servidores do Transfer Family. Para obter detalhes sobre essas permissões, consulte [Permissões da API do Directory Service : referência de ações, recursos e condições](#).

Trabalhando com realms do Active Directory

Ao considerar como fazer com que seus usuários do Active Directory acessem os servidores AWS Transfer Family , tenha em mente o realm do usuário e o realm do grupo. Idealmente, o realm do usuário e o realm do grupo devem corresponder. Ou seja, tanto o usuário quanto o grupo estão no realm padrão, ou ambos estão no realm confiável. Se esse não for o caso, o usuário não poderá ser autenticado pelo Transfer Family.

É possível testar o usuário para garantir que a configuração esteja correta. Para obter detalhes, consulte [Testando usuários](#). Se houver um problema com o user/group território, você receberá o erro Nenhum acesso associado encontrado para grupos de usuários.

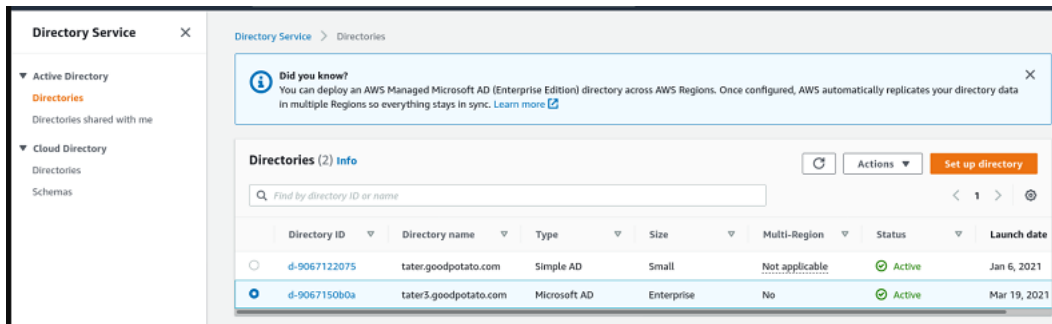
Escolhendo AWS Managed Microsoft AD como seu provedor de identidade

Esta seção descreve como usar AWS Directory Service for Microsoft Active Directory com um servidor.

Para usar AWS Managed Microsoft AD com Transfer Family

1. Faça login no Console de gerenciamento da AWS e abra o Directory Service console em <https://console.aws.amazon.com/directoryservicev2/>.

Use o Directory Service console para configurar um ou mais diretórios gerenciados. Para obter mais informações, consulte [AWS Managed Microsoft AD](#), no Guia do administrador do Directory Service .

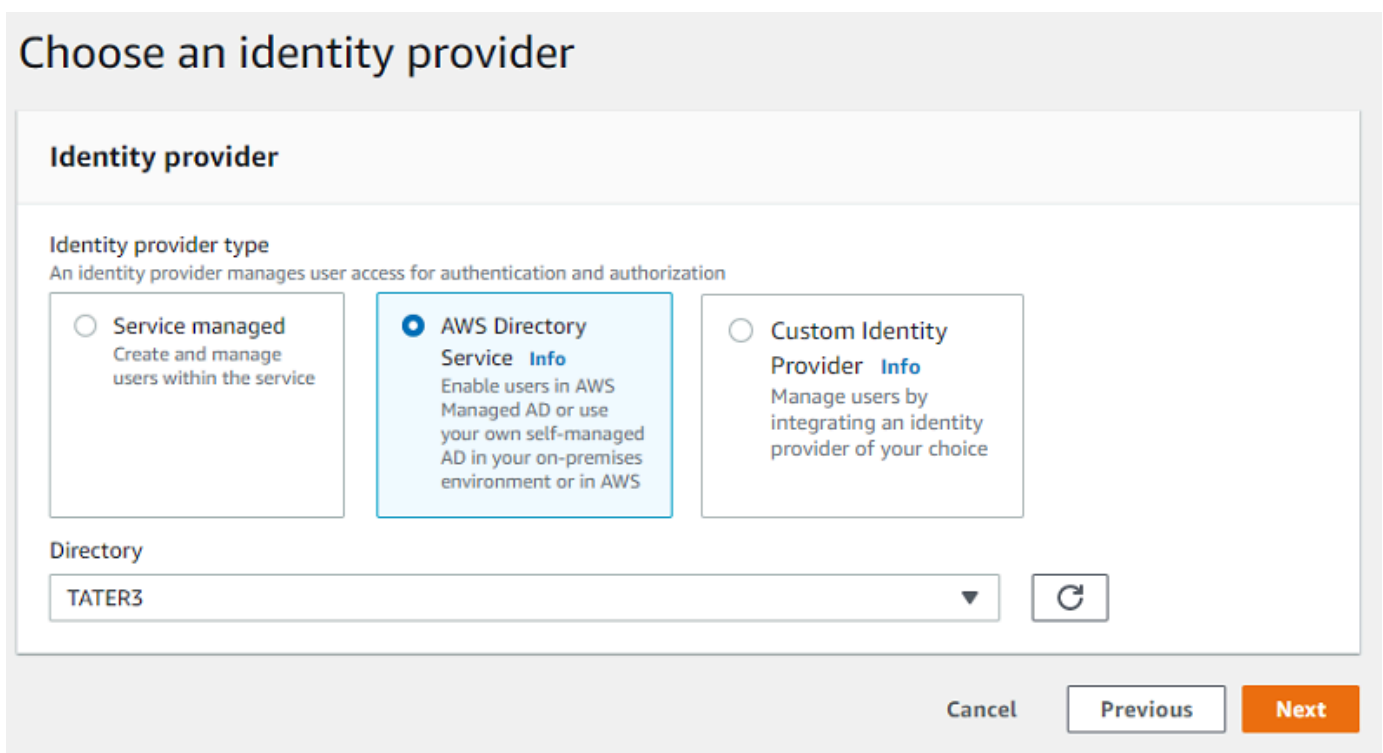


- Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/> e escolha Criar servidor.
- Na página Escolher protocolos, escolha um ou mais protocolos na lista.

Note

Se você selecionar FTPS, deverá fornecer o certificado AWS Certificate Manager .

- Em Escolher um provedor de identidade, escolha Directory Service AWS .



- A lista Diretórios contém todos os diretórios gerenciados que você configurou. Escolha um diretório da lista e escolha Próximo.

 Note

- Cross-Account e não há suporte para AWS Managed Microsoft AD diretórios compartilhados.
- Para configurar um servidor com o Directory Service como seu provedor de identidade, você precisa adicionar algumas Directory Service permissões. Para obter detalhes, consulte [Antes de começar a usar AWS Directory Service for Microsoft Active Directory](#).

6. Para concluir a criação do servidor, use um dos procedimentos a seguir:

- [Crie um SFTP-enabled servidor](#)
- [Crie um FTPS-enabled servidor](#)
- [Crie um FTP-enabled servidor](#)

Nesses procedimentos, continue com a etapa a seguir, escolhendo um provedor de identidade.

 Important

Você não pode excluir um diretório do Microsoft AD Directory Service se o tiver usado em um servidor Transfer Family. Primeiro, você deve excluir o servidor e, em seguida, excluir o diretório.

Conectando-se ao Microsoft Active Directory local

Esta seção descreve como configurar um AWS diretório usando um AD Connector

Para configurar seu AWS diretório usando o AD Connector

1. Abra o console do [Directory Service](#) e selecione Diretórios.
2. Selecione Configurar diretório.
3. Em tipo de diretório, escolha AD Connector.
4. Selecione um tamanho de diretório, selecione Avançar e, em seguida, selecione sua VPC e sub-redes.

5. Selecione Avançar e preencha os campos da seguinte forma:

- Nome DNS do diretório: insira o nome de domínio que você está usando para o Microsoft Active Directory.
- Endereços IP DNS: insira seus endereços IP do Microsoft Active Directory.
- Nome de usuário e senha da conta do servidor: insira os detalhes da conta de serviço a ser usada.

6. Preencha as telas para criar o serviço de diretório.

A próxima etapa é criar um servidor Transfer Family com o protocolo SFTP e o tipo de provedor de identidade do AWS Directory Service. Na lista suspensa Diretório, selecione o diretório que você adicionou no procedimento anterior.

Como conceder acesso a grupos

Depois de criar o servidor, você deve escolher quais grupos no diretório devem ter acesso para carregar e baixar arquivos usando os protocolos habilitados AWS Transfer Family. Você faz isso criando um acesso.

Note

AWS Transfer Family tem um limite padrão de 100 grupos do Active Directory por servidor. Se seu caso de uso exigir mais de 100 grupos, considere usar uma solução de provedor de identidade personalizada, conforme descrito em [Simplifique a autenticação do Active Directory com um provedor de identidade personalizado para AWS Transfer Family](#).

Note

Os usuários devem pertencer diretamente ao grupo ao qual você está concedendo acesso. Por exemplo, suponha que Bob seja um usuário e pertença ao Grupo A, e que o próprio Grupo A esteja incluído no Grupo B.

- Se você conceder acesso ao Grupo A, Bob terá acesso.
- Se você conceder acesso ao Grupo B (e não ao Grupo A), Bob não terá acesso.

Para conceder acesso a um grupo

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. Navegue até a página de detalhes do seu servidor.
3. Na seção Acessos, escolha Adicionar acesso.
4. Insira o SID do AWS Managed Microsoft AD diretório ao qual você deseja ter acesso ao servidor.

Note

Para obter informações sobre como encontrar o SID do seu grupo, consulte [the section called “Antes de começar a usar AWS Directory Service for Microsoft Active Directory”](#).

5. Para Access, escolha uma função AWS Identity and Access Management (IAM) para o grupo.
6. Na seção Política, escolha uma política. A configuração padrão é Nenhum.
7. Para o diretório inicial, escolha um bucket do Amazon S3 que corresponda ao diretório inicial do grupo.

Note

É possível limitar as partes do bucket que os usuários veem criando uma política de sessão. Por exemplo, para limitar os usuários à sua própria pasta no diretório / filetest, insira o texto a seguir na caixa.

```
/filetest/${transfer:UserName}
```

Para saber mais sobre como criar uma política de sessão, consulte [Criar uma política de sessão de um bucket do Amazon S3](#).

8. Escolha Adicionar para criar a associação.
9. Escolha seu servidor.
10. Escolha Adicionar acesso.
 - Insira o SID do grupo.

Note

Para obter informações sobre como encontrar o SID, consulte [the section called “Antes de começar a usar AWS Directory Service for Microsoft Active Directory”](#).

11. Escolha Adicionar acesso.

Na seção Acessos, os acessos para o servidor estão listados.

The screenshot displays the AWS Transfer Family console interface. At the top, the 'Endpoint configuration' section shows the 'Availability Zone' as 'us-east-1a', the 'Subnet ID' as 'subnet-...', and the 'Private IPv4 Address' as '172.31.80.36'. Below this, the 'Accesses (1)' section features a search bar, an 'Actions' dropdown menu, and an 'Associate access' button. A table lists the access details with columns for 'External Id', 'Home directory', and 'Role'. The table contains one entry: 'S-' for 'External Id', '/padbucket3' for 'Home directory', and 'ADGuy_S3_And_EFS' for 'Role'. The 'Additional details' section at the bottom includes 'Logging role' (Server activity not logged to Amazon CloudWatch), 'Server host key', 'Security Policy' (TransferSecurityPolicy-2018-11), and 'Domain' (Amazon S3). An 'Edit' button is located in the top right corner of the 'Additional details' section.

External Id	Home directory	Role
S-	/padbucket3	ADGuy_S3_And_EFS

Testando usuários

Você pode testar se um usuário tem acesso ao AWS Managed Microsoft AD diretório do seu servidor.

Note

Um usuário deve estar em exatamente um grupo (uma ID externa) listado na seção Acesso da página de Configuração do Endpoint. Se o usuário não estiver em nenhum grupo ou estiver em mais de um único grupo, esse usuário não receberá acesso.

Para testar se um usuário específico tem acesso

1. Na página de detalhes do servidor, escolha Ações e, em seguida, escolha Teste.
2. Para testar o provedor de identidade, insira as credenciais de login de um usuário que está em um dos grupos que tem acesso.
3. Escolha Testar.

Você vê um teste bem-sucedido do provedor de identidade, mostrando que o usuário selecionado recebeu acesso ao servidor.

Identity provider testing

User configuration [Info](#)

Username

Password

Response

```

{
  "Response": "
    {\"homeDirectory\":\"/padbucket3\", \"homeDirectoryDetails\":null, \"homeDirectoryType\":\"PATH\", \"posixProfile\",
    null, \"publicKeys\":null, \"role\":\"arn:aws:iam::195886157073:role/MDGuy_53_Amazon_EFS\", \"policy\":null, \"userName\":
    \"transferuser1\", \"identityProviderType\":null, \"userConfigMessage\":null}",
    "StatusCode": 200,
    "Message": ""
  }

```

Cancel
Test

Se o usuário pertencer a mais de um grupo que tenha acesso, você receberá a seguinte resposta.

```

"Response": "",
"StatusCode": 200,
"Message": "More than one associated access found for user's groups."

```

Como excluir o acesso ao servidor para um grupo

Para excluir o acesso ao servidor para um grupo

1. Na página de detalhes do servidor, escolha Ações e, em seguida, escolha Excluir acesso.
2. Na caixa de diálogo, confirme que deseja remover o acesso para este grupo.

Ao retornar à página de detalhes do servidor, você verá que o acesso para o grupo não está mais listado.

Como se conectar ao servidor usando SSH (Secure Shell)

Depois de configurar o servidor e os usuários, é possível se conectar ao servidor usando SSH e usar o nome de usuário totalmente qualificado para um usuário que tenha acesso.

```
sftp user@active-directory-domain@vpc-endpoint
```

Por exemplo: `transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-svc-987654zyxabc.us-east-1.vpce.amazonaws.com`.

Este formato tem como destino a pesquisa da federação, limitando a pesquisa de um Active Directory potencialmente grande.

Note

É possível especificar o nome de usuário simples. No entanto, neste caso, o código do Active Directory precisa pesquisar todos os diretórios na federação. Isso pode limitar a pesquisa e a autenticação pode falhar mesmo que o usuário tenha acesso.

Após a autenticação, o usuário fica localizado no diretório inicial que você especificou quando configurou o usuário.

Conectando-se AWS Transfer Family a um Active Directory autogerenciado usando florestas e relações de confiança

Directory Service tem as seguintes opções disponíveis para se conectar a um Active Directory autogerenciado:

- One-way a confiança na floresta (de saída AWS Managed Microsoft AD e entrada para o Active Directory local) funciona somente para o domínio raiz.
- Para domínios secundários, é possível usar um dos seguintes:
 - Use a confiança bidirecional entre o Active Directory local AWS Managed Microsoft AD e o Active Directory
 - Use confiança externa unidirecional para cada domínio secundário.

Ao se conectar ao servidor usando um domínio confiável, o usuário precisa especificar o domínio confiável, por exemplo, `transferuserexample@mycompany.com`.

Usando o AWS Directory Service para serviços de domínio Entra ID

Para clientes que precisam apenas de transferência por SFTP e não desejam gerenciar um domínio, existe o Simple Active Directory. Como alternativa, os clientes que desejam os benefícios do Active Directory e a alta disponibilidade em um serviço totalmente gerenciado podem usar o Microsoft AD gerenciado da AWS. Por fim, para clientes que desejam aproveitar a floresta existente do Active Directory para a transferência por SFTP, existe o Active Directory Connector.

Observe o seguinte:

- Para aproveitar sua floresta existente do Active Directory para atender às suas necessidades de transferência por SFTP, é possível usar o [Active Directory Connector](#).
- Se deseja os benefícios do Active Directory e a alta disponibilidade em um serviço totalmente gerenciado, é possível usar o AWS Directory Service for Microsoft Active Directory. Para obter detalhes, consulte [Usando o AWS Directory Service para o Microsoft Active Directory](#).

Este tópico descreve como usar um conector do Active Directory e os [serviços de domínio Entra ID \(anteriormente Azure AD\)](#) para autenticar usuários do SFTP Transfer com o Entra ID.

Tópicos

- [Antes de começar a usar o AWS Directory Service para o Entra ID Domain Services](#)
- [Etapa 1: Adicionar serviços de domínio Entra ID](#)
- [Etapa 2: Criar uma conta de serviço](#)
- [Etapa 3: Configurando o AWS diretório usando o AD Connector](#)
- [Etapa 4: Configurar o AWS Transfer Family servidor](#)

- [Etapa 5: Conceder acesso a grupos](#)
- [Etapa 6: Testar usuários](#)

Antes de começar a usar o AWS Directory Service para o Entra ID Domain Services

 Note

AWS Transfer Family tem um limite padrão de 100 grupos do Active Directory por servidor. Se seu caso de uso exigir mais de 100 grupos, considere usar uma solução de provedor de identidade personalizada, conforme descrito em [Simplifique a autenticação do Active Directory com um provedor de identidade personalizado para AWS Transfer Family](#).

Para AWS isso, você precisa do seguinte:

- Uma nuvem privada virtual (VPC) em uma AWS região em que você está usando seus servidores Transfer Family
- Pelo menos duas sub-redes privadas na VPC
- A VPC deve ter conectividade com a Internet
- Um gateway de cliente e um gateway privado virtual para conexão VPN site a site com o Microsoft Entra

Para o Microsoft Entra, você precisa do seguinte:

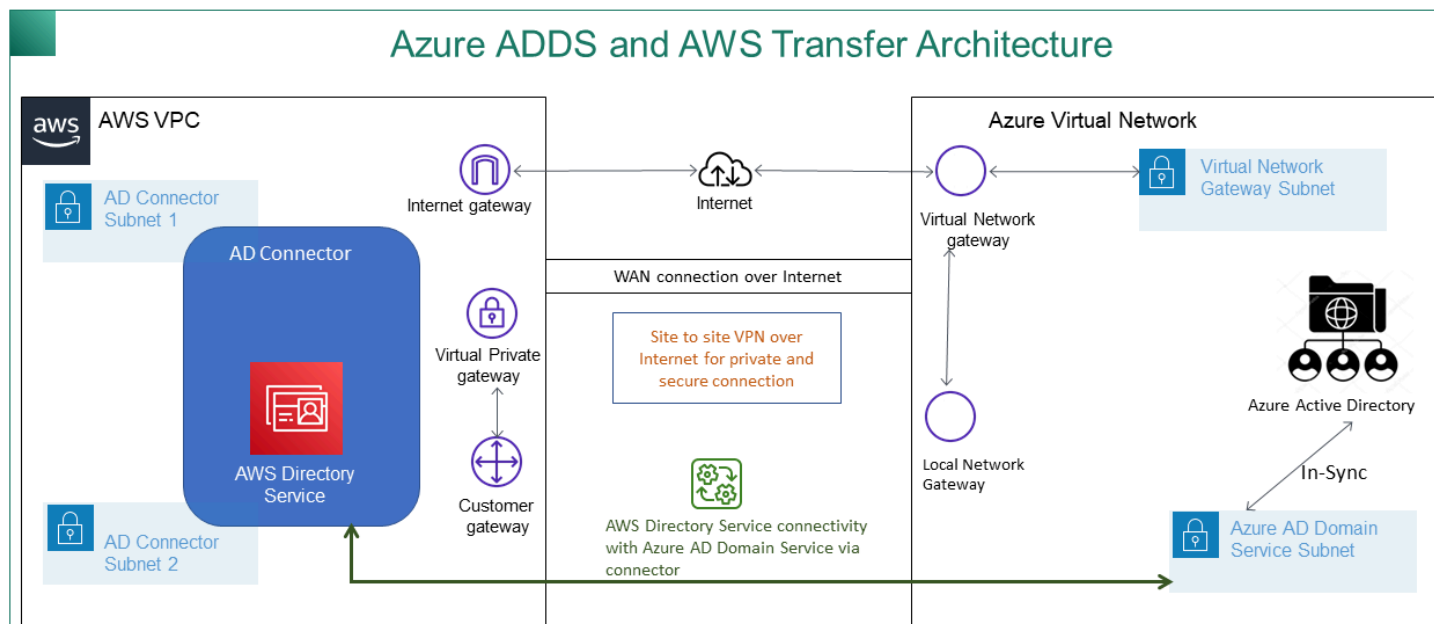
- Um serviço de domínio Entra ID e Active Directory
- Um grupo de recursos da Entra
- Uma rede virtual Entra
- Conectividade VPN entre sua Amazon VPC e seu grupo de recursos Entra

 Note

Isso pode ser feito por meio de túneis IPSEC nativos ou usando dispositivos VPN. Neste tópico, usamos túneis IPSEC entre um gateway de rede virtual Entra e um gateway de rede local. Os túneis devem ser configurados para permitir o tráfego entre seus endpoints do Entra Domain Service e as sub-redes que abrigam sua VPC. AWS

- Um gateway de cliente e um gateway privado virtual para conexão VPN site a site com o Microsoft Entra

O diagrama a seguir mostra a configuração necessária antes de começar.



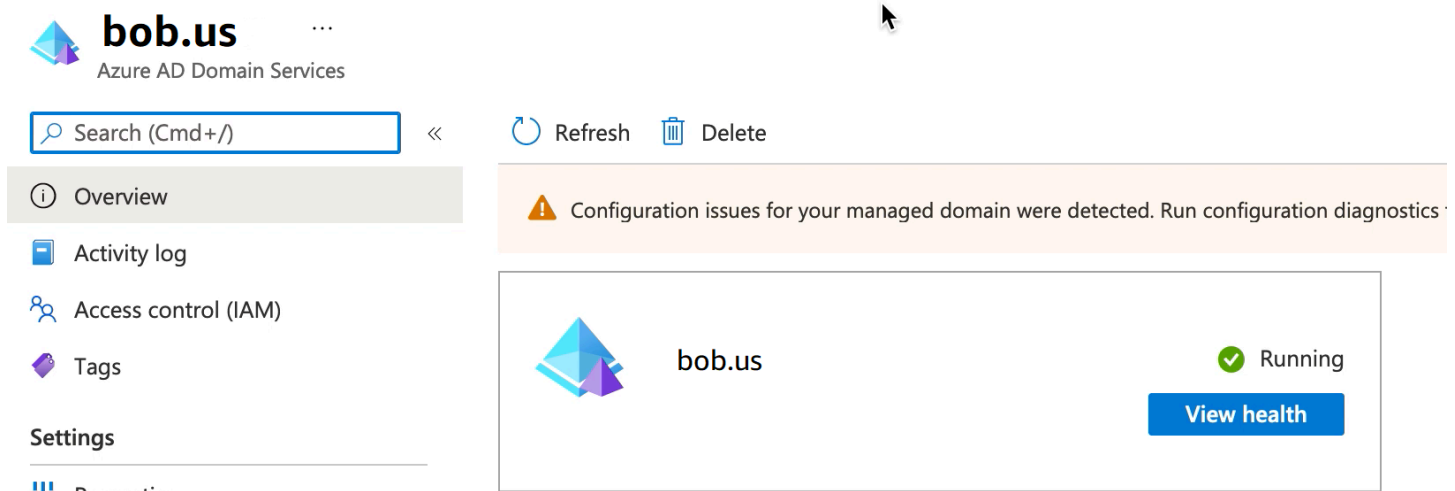
Etapa 1: Adicionar serviços de domínio Entra ID

O Entra ID não oferece suporte a instâncias de ingresso de domínio por padrão. Para realizar ações como o Domain Join e usar ferramentas como a Política de Grupo, os administradores devem habilitar os Serviços de Domínio Entra ID. Se você ainda não adicionou o Entra DS, ou sua implementação existente não está associada ao domínio que você deseja que seu servidor de transferência SFTP use, você deve adicionar uma nova instância.

Para obter informações sobre como habilitar os Serviços de Domínio Entra ID, consulte [Tutorial: Criar e configurar um domínio gerenciado do Microsoft Entra Domain Services](#).

Note

Ao habilitar o Entra DS, verifique se ele está configurado para o grupo de recursos e o domínio Entra ao qual você está conectando seu servidor de transferência SFTP.



bob.us
Azure AD Domain Services

Search (Cmd+/) << Refresh Delete

Overview
Activity log
Access control (IAM)
Tags
Settings
Diagnostics

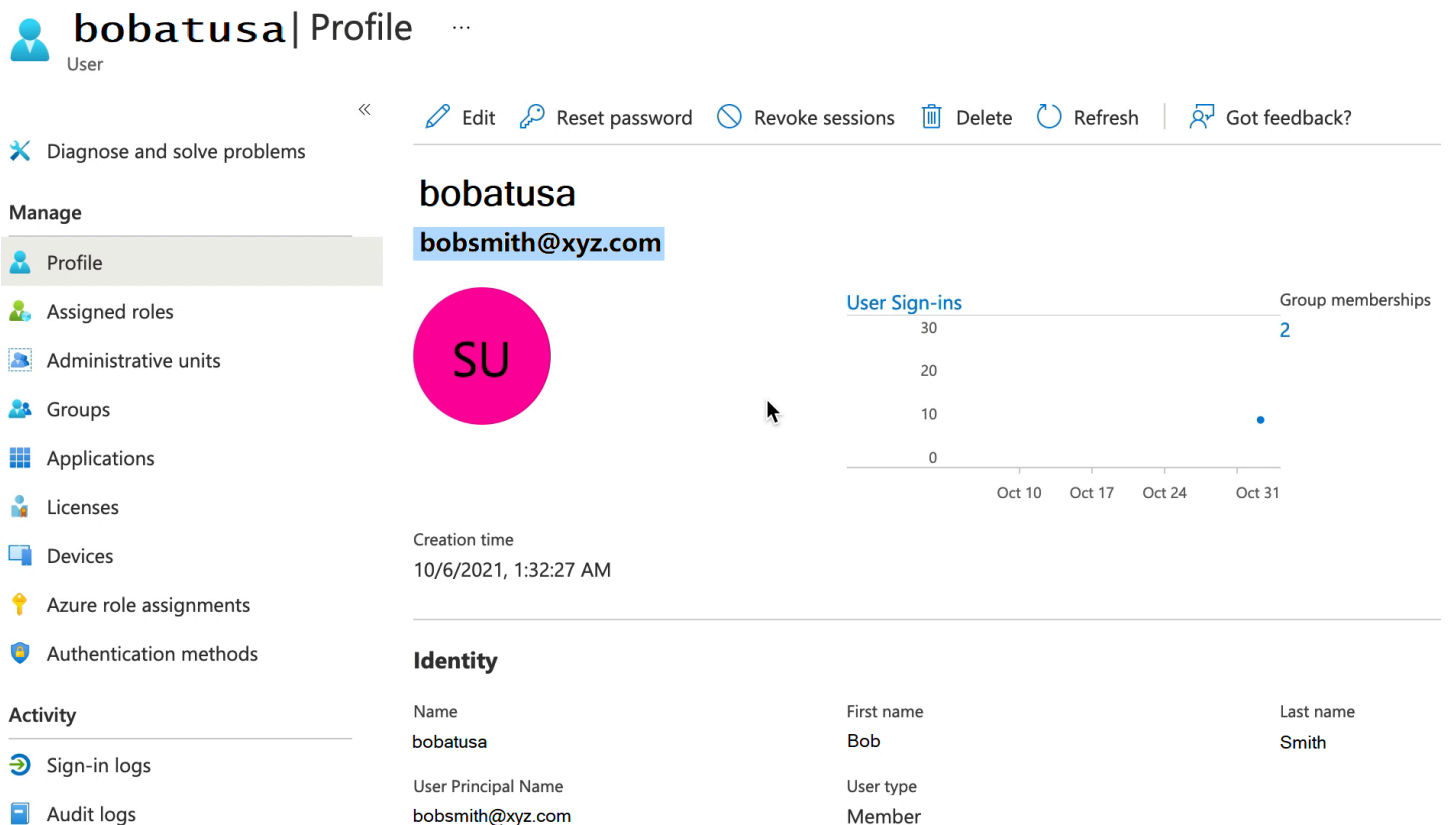
Configuration issues for your managed domain were detected. Run configuration diagnostics.

bob.us Running
[View health](#)

Etapa 2: Criar uma conta de serviço

O Entra deve ter uma conta de serviço que faça parte de um grupo de administradores no Entra DS. Essa conta é usada com o conector do AWS Active Directory. Certifique-se de que essa conta esteja sincronizada com o Entra DS.

[Home](#) > [Default Directory](#) > [Users](#) > [bobatusa](#)



bobatusa | Profile
User

« Edit Reset password Revoke sessions Delete Refresh Got feedback?

Diagnose and solve problems

Manage

- Profile
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Activity

- Sign-in logs
- Audit logs

bobatusa
bobsmith@xyz.com

SU

Creation time
10/6/2021, 1:32:27 AM

Identity

Name	First name	Last name
bobatusa	Bob	Smith

User Principal Name
bobsmith@xyz.com

User type
Member

User Sign-ins

Group memberships
2

Oct 10 Oct 17 Oct 24 Oct 31

Tip

Multi-factor a autenticação do Entra ID não é suportada pelos servidores Transfer Family que usam o protocolo SFTP. O servidor do Transfer Family não pode fornecer o token MFA depois que um usuário se autentica no SFTP. Certifique-se de desativar o MFA antes de tentar se conectar.

multi-factor authentication
users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)
Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users Multi-Factor Auth status: Any bulk update

☐	DISPLAY NAME ^	USER NAME	MULTI-FACTOR AUTH STATUS
☐	Christopher	admin@christopher.com	Disabled
☐	Robert	test@christopher.com	Disabled

Select a user

Etapa 3: Configurando o AWS diretório usando o AD Connector

Depois de configurar o Entra DS e criar uma conta de serviço com túneis VPN IPSEC entre sua AWS VPC e a rede virtual Entra, você pode testar a conectividade fazendo ping no endereço IP DNS do Entra DS de qualquer instância do EC2. AWS

Depois de verificar se a conexão está ativa, continue abaixo.

Para configurar seu AWS diretório usando o AD Connector

1. Abra o console do [Directory Service](#) e selecione Diretórios.
2. Selecione Configurar diretório.
3. Em tipo de diretório, escolha AD Connector.
4. Selecione um tamanho de diretório, selecione Avançar e, em seguida, selecione sua VPC e sub-redes.
5. Selecione Avançar e preencha os campos da seguinte forma:
 - Nome DNS do diretório: insira o nome de domínio que você está usando para o Entra DS.
 - Endereços IP DNS: insira seus endereços IP do Entra DS.

- Nome de usuário da conta do servidor e senha: insira os detalhes da conta de serviço que você criou na Etapa 2: Crie uma conta de serviço.

6. Preencha as telas para criar o serviço de diretório.

Agora, o status do diretório deve estar Ativo e está pronto para ser usado com um servidor de transferência SFTP.

Directory Service > Directories

 **Did you know?**
You can deploy an AWS Managed Microsoft AD (Enterprise Edition) directory across AWS Regions. Once configured, AWS automatically replicates your directory data in multiple Regions so everything stays in sync. [Learn more](#)

Directories (1) [Info](#)

 **Actions**  **Set up directory**

 Find by directory ID or name

 **1**  

	Directory ID	Directory name	Type	Size	Multi-Region	Status	Launch date
	d-906752c0d7		AD Connector	Small	Not applicable	 Active	Nov 3, 2021

Etapa 4: Configurar o AWS Transfer Family servidor

Crie um servidor Transfer Family com o protocolo SFTP e o tipo de provedor de identidade do AWS Directory Service. Na lista suspensa Diretórios, selecione o diretório que você adicionou na Etapa 3: Configurar o AWS Directory usando o AD Connector.

Note

Você não pode excluir um diretório do Microsoft AD no AWS Directory Service se o tiver usado em um servidor Transfer Family. Primeiro, você deve excluir o servidor e, em seguida, excluir o diretório.

Etapa 5: Conceder acesso a grupos

Depois de criar o servidor, você deve escolher quais grupos no diretório devem ter acesso para carregar e baixar arquivos usando os protocolos habilitados AWS Transfer Family. Você faz isso criando um acesso.

Note

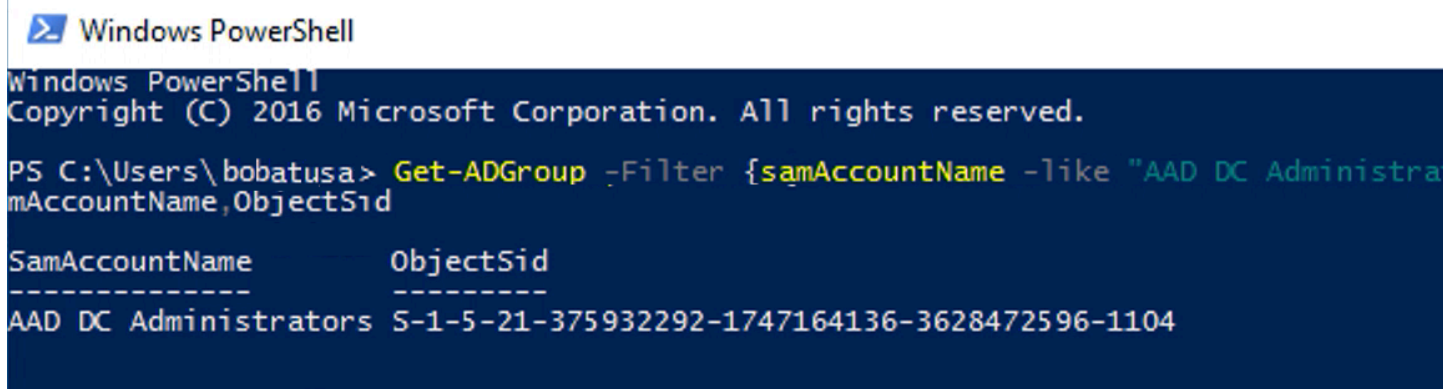
Os usuários devem pertencer diretamente ao grupo ao qual você está concedendo acesso. Por exemplo, suponha que Bob seja um usuário e pertença ao Grupo A, e que o próprio Grupo A esteja incluído no Grupo B.

- Se você conceder acesso ao Grupo A, Bob terá acesso.
- Se você conceder acesso ao Grupo B (e não ao Grupo A), Bob não terá acesso.

Para conceder acesso, você precisa recuperar o SID do grupo.

Use o seguinte PowerShell comando do Windows para recuperar o SID de um grupo, *YourGroupName* substituindo-o pelo nome do grupo.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select SamAccountName, ObjectSid
```



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\bobatusa> Get-ADGroup -Filter {samAccountName -like "AAD DC Administrators"} -Properties * | Select SamAccountName, ObjectSid

SamAccountName      ObjectSid
-----
AAD DC Administrators S-1-5-21-375932292-1747164136-3628472596-1104
```

Conceder acesso a grupos

1. Abra o <https://console.aws.amazon.com/transfer/>.
2. Navegue até a página de detalhes do servidor e, na seção Acessos, escolha Adicionar acesso.
3. Insira o SID que você recebeu da saída do procedimento anterior.
4. Para Access, escolha uma AWS Identity and Access Management função para o grupo.
5. Na seção Política, escolha uma política. O valor padrão é Nenhum.
6. Para o diretório inicial, escolha um bucket do Amazon S3 que corresponda ao diretório inicial do grupo.

7. Escolha Adicionar para criar a associação.

Os detalhes do servidor de transferência devem ser semelhantes aos seguintes:

Protocols	Identity provider
Protocols over which clients can connect to your server's endpoint SFTP	Identity provider type AWS Directory Service Directory ID d-123456789a

Accesses (1)
Actions ▾
Add access

< 1 >

☐	External Id	Home directory	Role
☐	S-1-5-21-375932292-1747164136-3628472596-1104	/usr/bin/sftp	sftp-user-role ↗

Etapa 6: Testar usuários

É possível testar ([Testando usuários](#)) se um usuário tem acesso ao diretório AWS Managed Microsoft AD do seu servidor. Um usuário deve estar em exatamente um grupo (uma ID externa) listado na seção Acesso da página de Configuração do Endpoint. Se o usuário não estiver em nenhum grupo ou estiver em mais de um único grupo, esse usuário não receberá acesso.

Como usar diretórios lógicos para simplificar suas estruturas de diretórios do Transfer Family

Os diretórios lógicos simplificam a estrutura de diretórios do AWS Transfer Family servidor. Com diretórios lógicos, você pode criar uma estrutura de diretórios virtuais com nomes fáceis de usar que os usuários navegam quando se conectam ao seu bucket do Amazon S3 ou ao sistema de arquivos do Amazon EFS. Isso impede que os usuários vejam os caminhos reais do diretório, os nomes dos buckets e os nomes do sistema de arquivos.

Note

Você deve usar políticas de sessão para que seus usuários finais possam realizar somente as operações que você permite que eles realizem.

Você deve usar diretórios lógicos para criar um diretório virtual fácil de usar para seus usuários finais e abstrair os nomes dos buckets. Os mapeamentos lógicos de diretórios só permitem que os usuários acessem seus caminhos lógicos e subdiretórios designados e proíbem caminhos relativos que atravessam as raízes lógicas.

O Transfer Family valida todos os caminhos que podem incluir elementos relativos e bloqueia ativamente a resolução desses caminhos antes de passarmos esses caminhos para o Amazon S3; isso impede que seus usuários ultrapassem seus mapeamentos lógicos. Embora o Transfer Family impeça que seus usuários finais acessem diretórios fora do diretório lógico, recomendamos que você também use funções ou políticas de sessão exclusivas para impor privilégios mínimos no nível de armazenamento.

Entendendo o chroot e a estrutura de diretórios

Uma operação chroot permite que você defina o diretório raiz de um usuário em qualquer local na sua hierarquia de armazenamento. Isso restringe os usuários ao diretório inicial ou raiz configurado, impedindo o acesso aos diretórios de nível superior.

Considere um caso em que um usuário do Amazon S3 esteja limitado a `amzn-s3-demo-bucket/home/${transfer:UserName}`. Sem o chroot, alguns clientes podem permitir que os usuários migrem para `/amzn-s3-demo-bucket/home`, exigindo um logout e um login para retornar ao diretório correto. Executar uma operação chroot evita esse problema.

Você pode criar estruturas de diretórios personalizadas em vários buckets e prefixos. Isso é útil se seu fluxo de trabalho exigir um layout de diretório específico que os prefixos de bucket sozinhos não podem fornecer. Você também pode se vincular a vários locais não contíguos no Amazon S3, semelhante à criação de um link simbólico em um sistema de arquivos Linux em que o caminho do diretório faz referência a um local diferente no sistema de arquivos.

Regras para usar diretórios lógicos

Esta seção descreve algumas regras e outras considerações sobre o uso de diretórios lógicos.

Limites de mapeamento

- Somente um mapeamento é permitido quando `Entry` é `"/` (nenhum caminho sobreposto é permitido).

- Os diretórios lógicos oferecem suporte a mapeamentos de até 2,1 MB para usuários personalizados de IDP e AD e 2.000 entradas para usuários gerenciados por serviços. Você pode calcular o tamanho dos mapeamentos da seguinte forma:
 1. Escreva um mapeamento típico no formato `{"Entry": "/entry-path", "Target": "/target-path"}`, onde *entry-path* e onde *target-path* estão os valores reais que você usará.
 2. Conte os caracteres dessa string e adicione um (1).
 3. Multiplique esse número pelo número aproximado de mapeamentos que você tem para o seu servidor.

Se o número estimado na etapa 3 for menor que 2,1 MB, seus mapeamentos estão dentro do limite aceitável.

Requisitos do caminho de destino

- Use a `${transfer:UserName}` variável se o caminho do bucket ou do sistema de arquivos tiver sido parametrizado com base no nome de usuário.
- Os destinos podem ser configurados para apontar para diferentes buckets ou sistemas de arquivos do Amazon S3, desde que a função IAM associada tenha as permissões necessárias para acessar esses locais de armazenamento.
- Todos os alvos devem começar com uma barra (/), mas não podem terminar com uma. Por exemplo, `/amzn-s3-demo-bucket/images` está correto, enquanto `amzn-s3-demo-bucket/images/` e não `/amzn-s3-demo-bucket/images/` está.

Considerações sobre armazenamento

- O Amazon S3 é um armazenamento de objetos em que as pastas existem apenas como um conceito virtual. Ao usar o armazenamento do Amazon S3, o Transfer Family relata prefixos como diretórios nas operações STAT, mesmo que não haja um objeto de zero byte com uma barra final. Um objeto adequado de zero bytes com uma barra final também é relatado como um diretório nas operações STAT. Esse comportamento é descrito em [Organização de objetos no console do Amazon S3 usando pastas](#) no Guia do usuário do Amazon Simple Storage Service.
- Para aplicativos que precisam distinguir entre arquivos e pastas, use o Amazon Elastic File System (Amazon EFS) como sua opção de armazenamento do Transfer Family.

- Se você estiver especificando valores de diretório lógico para seu usuário, o parâmetro usado dependerá do tipo de usuário:
 - Para usuários gerenciados por serviços, forneça valores de diretório lógico em `HomeDirectoryMappings`.
 - Para usuários de provedores de identidade personalizados, forneça valores de diretório lógico em `emHomeDirectoryDetails`.

Valores do diretório de usuários

- O parâmetro para especificar valores lógicos do diretório depende do seu tipo de usuário:
 - Para usuários gerenciados por serviços, forneça valores de diretório lógico em `HomeDirectoryMappings`.
 - Para usuários de provedores de identidade personalizados, forneça valores de diretório lógico em `emHomeDirectoryDetails`.
- Ao usar o `LOGICAL HomeDirectoryType`, você pode especificar um `HomeDirectory` valor para usuários do `Service Managed`, acesso ao `Active Directory` e implementações do `Provedor de Identidade Personalizado`, onde `HomeDirectoryDetails` eles são fornecidos na resposta. Se não for especificado, o `HomeDirectory` padrão é `/`.

Para obter detalhes sobre como implementar diretórios lógicos, consulte [Implementando diretórios lógicos](#).

Implementando diretórios lógicos

Important

Requisitos do diretório raiz

- Se você não estiver usando as configurações de otimização de desempenho do Amazon S3, seu diretório raiz deve existir na inicialização.
- Para o Amazon S3, isso significa criar um objeto de zero bytes que termina com uma barra (`/`).
- Para evitar esse requisito, considere ativar a otimização de desempenho do Amazon S3 ao criar ou atualizar seu servidor.

- Ao especificar um HomeDirectory com LOGICAL HomeDirectoryType, o valor deve ser mapeado para um de seus mapeamentos lógicos de diretório. O serviço valida isso durante a criação e as atualizações do usuário para evitar configurações que não funcionariam.

Configuração lógica do diretório inicial

Ao usar LOGICAL como seu HomeDirectoryType, observe o seguinte:

- O HomeDirectory valor deve corresponder a um dos mapeamentos de diretórios lógicos existentes.
- O sistema valida isso automaticamente durante a criação e as atualizações do usuário.
- Essa validação evita configurações que causariam problemas de acesso.

Habilitar diretórios lógicos

Para usar diretórios lógicos para um usuário, defina o HomeDirectoryType parâmetro como LOGICAL. Faça isso ao criar um novo usuário ou atualizar um usuário existente.

```
"HomeDirectoryType": "LOGICAL"
```

Habilitar **chroot** para usuários

Em chroot, crie uma estrutura de diretórios que consiste em um emparelhamento de Entry e Target para cada usuário. A entrada/representa a pasta raiz, enquanto o Target especifica a localização real em seu bucket ou sistema de arquivos.

Example for Amazon S3

```
[{"Entry": "/", "Target": "/amzn-s3-demo-bucket/jane"}]
```

Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

É possível usar um caminho absoluto, como no exemplo anterior, ou pode usar uma substituição dinâmica para o nome de usuário com `${transfer:UserName}`, como no exemplo a seguir.

```
[{"Entry": "/", "Target":  
"/amzn-s3-demo-bucket/${transfer:UserName}"}]
```

No exemplo anterior, o usuário está bloqueado em seu diretório raiz e não pode ficar maior na hierarquia.

Estrutura do diretório virtual

Para uma estrutura de diretório virtual, é possível criar vários emparelhamentos de Entry e Target, com destinos em qualquer lugar em seus buckets S3 ou sistemas de arquivos do EFS, inclusive em vários buckets ou sistemas de arquivos, desde que o mapeamento de perfis do IAM do usuário tenha permissões de acesso a eles.

No exemplo de estrutura virtual a seguir, quando o usuário faz login no AWS SFTP, ele está no diretório raiz com subdiretórios de/pics,/doc, e. /reporting /anotherpath/subpath/financials

Note

A menos que você opte por otimizar o desempenho dos diretórios do Amazon S3 (ao criar ou atualizar um servidor), o usuário ou o administrador precisará criar os diretórios, caso eles ainda não existam. Evitar esse problema é um motivo para considerar a otimização do desempenho do Amazon S3.

Para o Amazon EFS, você ainda precisa do administrador para criar os mapeamentos lógicos ou o / diretório.

```
[  
{"Entry": "/pics", "Target": "/amzn-s3-demo-bucket1/pics"},  
{"Entry": "/doc", "Target": "/amzn-s3-demo-bucket1/anotherpath/docs"},  
{"Entry": "/reporting", "Target": "/amzn-s3-demo-bucket2/Q1"},  
{"Entry": "/anotherpath/subpath/financials", "Target": "/amzn-s3-demo-bucket2/  
financials"}]
```

Note

Você só pode fazer upload de arquivos para as pastas específicas que mapear. Isso significa que, no exemplo anterior, você não pode fazer upload para diretórios /anotherpath ou

anotherpath/subpath; somente anotherpath/subpath/financials. Você também não pode mapear esses caminhos diretamente, pois caminhos com sobreposição não são permitidos.

Por exemplo, suponha que você crie os seguintes mapeamentos:

```
{
  "Entry": "/pics",
  "Target": "/amzn-s3-demo-bucket/pics"
},
{
  "Entry": "/doc",
  "Target": "/amzn-s3-demo-bucket/mydocs"
},
{
  "Entry": "/temp",
  "Target": "/amzn-s3-demo-bucket2/temporary"
}
```

Você só pode fazer upload de arquivos para esses buckets. Quando você se conecta pela primeira vez por meio de sftp, você é colocado no diretório raiz, /. Se você tentar fazer upload de um arquivo para esse diretório, o upload falhará. Os comandos a seguir mostram uma sequência de exemplo:

```
sftp> pwd
Remote working directory: /
sftp> put file
Uploading file to /file
remote open("/file"): No such file or directory
```

Para fazer upload para qualquer directory/sub-directory, você deve mapear explicitamente o caminho para o sub-directory.

Para obter mais informações sobre como configurar diretórios lógicos e chroot para seus usuários, incluindo um AWS CloudFormation modelo que você pode baixar e usar, consulte [Simplifique sua estrutura de AWS SFTP com chroot e diretórios lógicos](#) no blog de armazenamento. AWS

Configurar exemplos de diretórios lógicos

Neste exemplo, criamos um usuário e atribuímos dois diretórios lógicos. O comando a seguir cria um novo usuário (para um servidor do Transfer Family existente) com diretórios lógicos `pics` e `doc`.

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-
bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs
\"}]" \
  --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Se **marymajor** for um usuário existente e o tipo de seu diretório inicial for `PATH`, é possível alterá-lo para `LOGICAL` com um comando semelhante ao anterior.

```
aws transfer update-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-
bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs
\"}]"
```

Observe o seguinte:

- Se os diretórios `/amzn-s3-demo-bucket1/pics` e `/amzn-s3-demo-bucket2/test/mydocs` ainda não existem, o usuário (ou um administrador) precisa criá-los.

Note

Esses diretórios são criados automaticamente pelo servidor Transfer Family se você tiver configurado diretórios otimizados.

- Quando **marymajor** se conecta ao servidor e executa o `ls -l` comando, Mary vê o seguinte:

```
drwxr--r--  1      -      -      0 Mar 17 15:42 doc
```

```
drwxr--r--  1      -      -      0 Mar 17 16:04 pics
```

- **marymajor** não é possível criar nenhum arquivo ou diretório neste nível. No entanto, dentro de `pics` e `doc`, ela pode adicionar subdiretórios.
- Arquivos que Mary adiciona `pics` e `doc` são adicionados aos caminhos do Amazon S3 `/amzn-s3-demo-bucket1/pics` e `/amzn-s3-demo-bucket2/test/mydocs` respectivamente.
- Neste exemplo, especificamos dois compartimentos diferentes para ilustrar essa possibilidade. No entanto, é possível usar o mesmo bucket para vários ou todos os diretórios lógicos que você especifica para o usuário.

Este exemplo fornece uma configuração alternativa para um caminho inicial lógico.

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory /home/marymajor \
  --home-directory-mappings "[{\"Entry\":\"/home/marymajor/pics\", \"Target\":\"/amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/home/marymajor/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs\"}]" \
  --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Observe o seguinte:

- Os mapeamentos fornecem um caminho comum, `/home/marymajor`, que é a primeira parte dos dois caminhos lógicos. Em seguida, os arquivos podem ser adicionados às doc pastas `pics` e `doc`.
- Como no exemplo anterior, o diretório inicial, `/home/marymajor`, é somente para leitura.

Configure diretórios lógicos para o Amazon EFS

Se o seu servidor do Transfer Family usa o Amazon EFS, o diretório inicial do usuário deve ser criado com acesso de leitura e gravação antes que o usuário possa trabalhar em seu diretório inicial lógico. O usuário não pode criar esse diretório sozinho, pois não teria permissões para `mkdir` em seu diretório inicial lógico.

Se o diretório inicial do usuário não existir e ele executar um comando `ls`, o sistema responderá da seguinte forma:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Um usuário com acesso administrativo ao diretório pai precisa criar o diretório inicial lógico do usuário.

AWS Lambda Resposta personalizada

É possível usar diretórios lógicos com uma função do Lambda que se conecta ao seu provedor de identidade personalizado. Para fazer isso, em sua função do Lambda, você especifica o `HomeDirectoryType` como **LOGICAL** e adiciona os valores `Entry` e `Target` para o parâmetro `HomeDirectoryDetails`. Por exemplo:

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{"Entry": "\\", "Target": "\/amzn-s3-demo-bucket/
theRealFolder"}]"
```

O código seguinte é um exemplo de uma resposta de êxito de uma chamada de autenticação Lambda personalizado.

```
aws transfer test-identity-provider \
  --server-id s-1234567890abcdef0 \
  --user-name myuser
{
  "Url": "https://a1b2c3d4e5.execute-api.us-east-2.amazonaws.com/prod/servers/
s-1234567890abcdef0/users/myuser/config",
  "Message": "",
  "Response": "{\"Role\": \"arn:aws:iam::123456789012:role/bob-usa-role\",
    \"HomeDirectoryType\": \"LOGICAL\",
    \"HomeDirectoryDetails\": \"[{\\\"Entry\\\": \\\"\\\"/myhome\\\"\\\", \\\"
\\\"Target\\\": \\\"\\\"/amzn-s3-demo-bucket/theRealFolder\\\"}]\\\",
    \"PublicKeys\": \"[ssh-rsa myrsapubkey]\\\"}\",
  \"StatusCode\": 200
}
```

Note

A linha `"Url"`: é retornada somente se você estiver usando um método do API Gateway como seu provedor de identidade personalizado.

Acesse seus sistemas de arquivos FSx for NetApp ONTAP com Transfer Family

Sumário

- [Visão geral do](#)
- [Pré-requisitos](#)
 - [Requisitos do FSx para NetApp ONTAP](#)
 - [Permissões obrigatórias do IAM](#)
- [Como o armazenamento FSx funciona com o Transfer Family](#)
 - [Identidade do usuário do sistema de arquivos](#)
- [Criando um ponto de acesso S3 para FSx](#)
 - [Nomeação de pontos de acesso](#)
 - [Criando um ponto de acesso para FSx for ONTAP NetApp](#)
 - [Configurando permissões do sistema de arquivos](#)
- [Usando aliases de ponto de acesso S3 com FSx](#)
 - [Sobre aliases de pontos de acesso](#)
 - [Encontrando seu alias de ponto de acesso](#)
- [Configurando o Transfer Family para armazenamento FSx](#)
 - [Criar um perfil do IAM](#)
- [Gerenciando usuários para armazenamento FSx](#)
 - [Criar um usuário](#)
 - [Configurando vários mapeamentos de diretórios](#)
- [Configurando clientes de transferência de arquivos](#)
 - [Configuração WinSCP](#)
 - [Outros clientes SFTP](#)
- [Solução de problemas de armazenamento FSx](#)
 - [Problemas de operação de arquivos](#)

Visão geral do

O Transfer Family oferece suporte ao Amazon FSx for NetApp ONTAP por meio de pontos de acesso S3. O Amazon FSx for NetApp ONTAP é um serviço totalmente gerenciado que fornece armazenamento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, baseado no popular sistema de arquivos ONTAP. NetApp Quando você configura o Transfer Family com um sistema de arquivos FSx, seus usuários se conectam aos endpoints do Transfer Family usando clientes de transferência de arquivos padrão. O Transfer Family roteia as operações de arquivos por meio de um ponto de acesso S3 conectado ao seu volume FSx, enquanto seus dados permanecem no sistema de arquivos FSx. Para saber mais sobre o FSx for NetApp ONTAP, consulte O que é o [Amazon FSx for](#) ONTAP? NetApp

Essa integração permite que você:

- Transfira arquivos usando protocolos SFTP, FTPS ou FTP para armazenamento de arquivos de nível corporativo
- Acesse os mesmos dados por meio de vários protocolos (SFTP, NFS, SMB)
- Use recursos do FSx, como instantâneos, backups e hierarquização de dados

Important

Algumas operações de arquivo não são suportadas ao usar sistemas de arquivos FSx com Transfer Family, incluindo operações de renomeação e adição. Para operações de upload, os tamanhos dos arquivos são limitados a 5 GB. Para obter uma lista completa das limitações, consulte [Compatibilidade de pontos de acesso](#).

Pré-requisitos

Antes de configurar o Transfer Family com o Amazon FSx, você deve atender aos seguintes requisitos.

Requisitos do FSx para NetApp ONTAP

Para usar o FSx for NetApp ONTAP com Transfer Family, você precisa:

- Um FSx para sistema de arquivos NetApp ONTAP executando o ONTAP versão 9.17.1 ou posterior

- O sistema de arquivos e o ponto de acesso S3 na mesma região AWS
- A mesma AWS conta proprietária do sistema de arquivos e do ponto de acesso

Para saber mais, consulte [Introdução ao Amazon FSx for NetApp](#) ONTAP.

Permissões obrigatórias do IAM

Você pode configurar cada ponto de acesso do S3 com permissões e controles de rede distintos que o S3 aplica a qualquer solicitação feita usando esse ponto de acesso. Os pontos de acesso do S3 oferecem suporte às políticas de recursos do IAM que você pode usar para controlar o uso do ponto de acesso por recurso, usuário ou outras condições. Para que um aplicativo ou usuário acesse arquivos por meio de um ponto de acesso, tanto o ponto de acesso quanto o volume subjacente devem permitir a solicitação. Para obter mais informações, consulte as [políticas de pontos de acesso do IAM](#).

Os pontos de acesso do Amazon S3 para FSx usam um modelo de autorização de camada dupla que combina permissões do IAM com permissões no nível do sistema de arquivos. Essa abordagem garante que as solicitações de acesso aos dados sejam devidamente autorizadas tanto no nível do AWS serviço quanto no nível do sistema de arquivos subjacente.

Para que um aplicativo ou usuário acesse com êxito os dados por meio de um ponto de acesso, tanto a política de ponto de acesso do S3 quanto o volume FSx subjacente devem permitir a solicitação.

Para criar e configurar essa integração, você precisa das seguintes permissões:

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`
- `s3:PutAccessPointPolicy`(se estiver criando uma política de ponto de acesso opcional)

Como o armazenamento FSx funciona com o Transfer Family

Quando você configura o Transfer Family com um sistema de arquivos FSx, os seguintes componentes trabalham juntos para permitir transferências de arquivos:

1. Um usuário se conecta ao servidor Transfer Family usando um cliente SFTP, FTPS ou FTP.

2. O Transfer Family autentica o usuário usando identidades gerenciadas pelo serviço, um provedor de identidade personalizado ou AWS Directory Service for Microsoft Active Directory. Depois de autenticado, o Transfer Family assume a função do IAM associada ao usuário.
3. Para cada operação de arquivo, o Transfer Family atua como um cliente de API S3 padrão, fazendo solicitações ao S3 Access Point usando a função assumida do usuário no IAM e verifica as permissões em relação à política de ponto de acesso do S3.
4. O sistema de arquivos FSx verifica se o usuário do sistema de arquivos associado ao ponto de acesso tem permissão para realizar a operação solicitada. A operação do arquivo é então executada no volume FSx.

Para que uma operação de arquivo seja bem-sucedida, ambas as camadas de autorização devem permitir a solicitação.

 Note

Anexar um ponto de acesso S3 a um volume FSx não altera o comportamento do volume quando acessado diretamente por meio de NFS ou SMB. O acesso ao protocolo de arquivos existente continua funcionando inalterado.

Identidade do usuário do sistema de arquivos

Cada ponto de acesso usa uma identidade de usuário do sistema de arquivos que você especifica ao criar o ponto de acesso. Essa identidade autoriza todas as solicitações de acesso a arquivos feitas por meio desse ponto de acesso. O usuário do sistema de arquivos é uma conta de usuário no sistema de arquivos Amazon FSx subjacente. Se o usuário do sistema de arquivos tiver acesso somente para leitura, somente as solicitações de leitura feitas usando o ponto de acesso serão autorizadas e as solicitações de gravação serão bloqueadas. Se o usuário do sistema de arquivos tiver acesso de leitura e gravação, as solicitações de leitura e gravação no volume conectado feitas usando o ponto de acesso serão autorizadas.

Criando um ponto de acesso S3 para FSx

Antes de configurar o Transfer Family, você deve criar um ponto de acesso S3 conectado ao seu volume FSx. Os pontos de acesso S3 são endpoints de rede denominados que são conectados a uma fonte de dados, como um bucket ou volume Amazon FSx for ONTAP. Você pode criar e conectar um ponto de acesso a um FSx for NetApp ONTAP usando o console, a AWS CLI ou a

API do Amazon FSx. Depois de anexado, você pode usar as APIs de objeto do S3 para acessar seus dados de arquivo. Seus dados continuam residindo no sistema de arquivos do Amazon FSx e continuam diretamente acessíveis para suas workloads existentes. Você continua gerenciando seu armazenamento usando todos os recursos de gerenciamento de armazenamento do FSx for NetApp ONTAP, incluindo backups, instantâneos, cotas de usuários e grupos e compactação.

Para obter mais informações, consulte [Criar pontos de acesso](#).

Nomeação de pontos de acesso

Ao nomear seu ponto de acesso, siga estas diretrizes:

- Os nomes dos pontos de acesso devem ser exclusivos em sua AWS conta e região.
- Os nomes não podem terminar com `-ext-s3alias` (reservados para aliases).
- Evite incluir informações confidenciais nos nomes porque eles são publicados no DNS.

Para obter uma lista completa das regras de nomenclatura, consulte Regras de [nomenclatura, restrições e limitações dos pontos de acesso](#).

Criando um ponto de acesso para FSx for ONTAP NetApp

Use o procedimento a seguir para criar um ponto de acesso S3 para um volume FSx NetApp for ONTAP.

Para criar um ponto de acesso (console)

1. Abra o console do Amazon FSx em <https://console.aws.amazon.com/fsx/>
2. No painel de navegação, escolha Sistemas de arquivos.
3. Escolha seu FSx para o sistema de arquivos NetApp ONTAP.
4. Escolha a guia Volumes.
5. Selecione o volume que você deseja conectar.
6. Em Ações, escolha Criar ponto de acesso S3.
7. Em Nome do ponto de acesso, insira um nome descritivo (por exemplo, `transfer-family-ap`).
8. Para Tipo de identidade de usuário do sistema de arquivos, escolha uma das seguintes opções:
 - Identidade UNIX - Para volumes com estilo de segurança UNIX

- Identidade do Windows - Para volumes com estilo de segurança NTFS
9. (Opcional) Em Política de ponto de acesso, insira uma política do IAM que define quais diretores do IAM podem realizar quais operações em objetos acessados por meio desse ponto de acesso. Para obter mais informações, consulte [Gerenciando o acesso ao ponto de acesso](#).
 10. Escolha Criar.
 11. Após a criação, anote o alias do ponto de acesso para uso na configuração do Transfer Family.

Note

Quando AWS Transfer Family acessa os recursos do S3 em nome dos SFTP/FTPS usuários conectados, as solicitações se originam da AWS Transfer Family infraestrutura, não da sua VPC. Por esse motivo, os pontos de acesso S3 configurados com uma origem de rede VPC negarão essas solicitações. No entanto, mesmo se você usar um Access Point configurado com uma origem de rede na Internet, todo o tráfego entre o Transfer Family e o Access Point permanece privado e viaja pela rede de AWS backbone — ele não atravessa a Internet pública.

Configurando permissões do sistema de arquivos

O usuário do sistema de arquivos que você especifica determina quais operações os usuários do Transfer Family podem realizar. Você deve configurar as permissões apropriadas em seu volume FSx.

Exemplo de UNIX:

```
# Create a directory for Transfer Family users
mkdir -p /vol1/transfer-users

# Set ownership to match the access point user
chown 1001:1001 /vol1/transfer-users

# Set permissions
chmod 755 /vol1/transfer-users
```

Exemplo do Windows:

```
# Create a directory for Transfer Family users
```

```
New-Item -Path "D:\vol1\transfer-users" -ItemType Directory

# Set permissions for the file system user associated with the access point
# Replace DOMAIN\TransferUser with your Windows user identity
icacls "D:\vol1\transfer-users" /grant "DOMAIN\TransferUser:(OI)(CI)M" /T

# Verify permissions
icacls "D:\vol1\transfer-users"
```

Usando aliases de ponto de acesso S3 com FSx

Ao usar sistemas de arquivos FSx com Transfer Family, você deve usar aliases de ponto de acesso S3. O Transfer Family não suporta o uso de ARNs de pontos de acesso ou outros métodos de referência para armazenamento FSx.

Important

AWS Transfer Family só suporta aliases de ponto de acesso S3 ao usar sistemas de arquivos FSx. Você não pode usar ARNs de ponto de acesso ou URIs de estilo hospedado virtual.

Important

O ponto de acesso deve estar na mesma região do volume.

Sobre aliases de pontos de acesso

Quando você cria um ponto de acesso S3 conectado a um volume FSx, o Amazon S3 gera automaticamente um alias de ponto de acesso. Esse alias é um identificador exclusivo que você pode usar em qualquer lugar em que use um nome de bucket do S3.

Para pontos de acesso conectados a volumes FSx, o alias usa o seguinte formato:

```
access-point-name-metadata-ext-s3alias
```

Exemplo de alias:

```
my-fsx-ap-aqfqprinstn7aefdfbarligizwgyfouse1a-ext-s3alias
```

Note

O `-ext-s3alias` sufixo é reservado para aliases de pontos de acesso FSx. Você não pode usar esse sufixo em nomes de pontos de acesso.

Encontrando seu alias de ponto de acesso

Você pode encontrar o alias do ponto de acesso depois de criar o ponto de acesso.

Para encontrar o alias do ponto de acesso (console)

1. Abra o console do Amazon FSx em. <https://console.aws.amazon.com/fsx/>
2. No painel de navegação, escolha Sistemas de arquivos.
3. Escolha o sistema de arquivos.
4. Escolha a guia Volumes e selecione o volume para o qual você criou o ponto de acesso.
5. Vá para a coluna de detalhes do ponto de acesso S3.
6. O alias é exibido na coluna Alias.

Para encontrar o alias do ponto de acesso (CLI)

Use o comando `describe-s3-access-point-attachments`.

```
aws fsx describe-s3-access-point-attachments \
  --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

A resposta inclui o alias:

```
{
  "S3AccessPointAttachments": [
    {
      "S3AccessPoint": {
        "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-fsx-
ap",
        "Alias": "my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias"
      }
    }
  ]
}
```

```
}
```

Ao configurar usuários do Transfer Family, use o alias do ponto de acesso nos mapeamentos do diretório inicial.

Formato do diretório inicial:

```
/access-point-alias/path/to/directory
```

Exemplo:

```
/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/jsmith
```

Configurando o Transfer Family para armazenamento FSx

Depois de criar o ponto de acesso S3, configure um servidor Transfer Family para usá-lo.

Criar um perfil do IAM

Você deve criar uma função do IAM que conceda à Transfer Family acesso ao ponto de acesso do S3.

Important

As políticas do IAM exigem o formato ARN do ponto de acesso, não o alias. Use o formato `arn:aws:s3:region:account-id:accesspoint/access-point-name` em suas declarações de recursos de política do IAM. O alias do ponto de acesso (terminado em `-ext-s3alias`) é usado somente para mapeamentos do diretório inicial.

Para criar perfil do IAM

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Funções e, em seguida, escolha Criar função.
3. Em Tipo de entidade confiável, escolha Serviços da AWS .
4. Em Caso de uso, escolha Transferir.
5. Escolha Próximo.
6. Escolha Criar política e insira sua política (veja o exemplo de política abaixo).

7. Anexe a política à função e escolha Criar função.

Exemplo de política do IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFileOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap/
object/*"
    },
    {
      "Sid": "AllowDirectoryOperations",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap"
    }
  ]
}
```

Gerenciando usuários para armazenamento FSx

Crie usuários do Transfer Family com mapeamentos de diretório inicial que usam o alias do ponto de acesso S3.

Criar um usuário

Ao criar um usuário para armazenamento FSx, use o alias do ponto de acesso nos mapeamentos do diretório inicial.

Para criar um usuário do Service Managed (console)

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores.
3. Escolha seu servidor.
4. Na seção Usuários, escolha Adicionar usuário.
5. Em Nome de usuário, insira um nome de usuário.
6. Em Role, escolha a função do IAM que você criou.
7. Em Diretório pessoal, escolha Restrito.
8. Para mapeamentos do diretório inicial, adicione um mapeamento usando o alias do ponto de acesso:

```
[{"Entry": "/", "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias/users/jsmith"}]
```

Para criar um usuário (CLI)

Use o comando `create-user`. Substitua o alias do ponto de acesso pelo seu alias.

```
aws transfer create-user \
  --server-id s-0123456789abcdef0 \
  --user-name jsmith \
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \
  --home-directory-type LOGICAL \
  --home-directory-mappings '[
    {
      "Entry": "/",
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias/users/
jsmith"
    }
  ]'
```

Configurando vários mapeamentos de diretórios

Você pode mapear vários diretórios virtuais para caminhos diferentes no volume FSx.

Exemplo: diretórios separados de upload e download

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings '[  
    {  
      "Entry": "/inbox",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/  
jsmith/inbox"  
    },  
    {  
      "Entry": "/outbox",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/  
jsmith/outbox"  
    }  
  ]'
```

Configurando clientes de transferência de arquivos

Ao usar sistemas de arquivos FSx com Transfer Family, você deve configurar seus clientes de transferência de arquivos para desativar recursos que não são suportados.

Configuração WinSCP

O WinSCP usa um recurso de renomeação temporária por padrão que não é suportado com pontos de acesso S3 para FSx.

Warning

Se você não desativar o recurso de renomeação temporária no WinSCP, os carregamentos de arquivos falharão.

Para desativar a renomeação temporária no WinSCP

1. Abra o WinSCP.
2. Na caixa de diálogo Login, escolha Editar para modificar as configurações da sessão.
3. Escolha Advanced (Avançado).
4. No painel de navegação à esquerda, em Transferir, escolha Resistência.

5. Em Habilitar transferência resume/transfer para nome de arquivo temporário, escolha Desabilitar.
6. Escolha OK para salvar as configurações.

Como alternativa, você pode desativar essa configuração para uma sessão existente:

1. Conecte-se ao seu servidor Transfer Family.
2. Escolha Opções e, em seguida, Preferências.
3. Escolha Transferência e, em seguida, Resistência.
4. Em Habilitar transferência resume/transfer para nome de arquivo temporário, escolha Desabilitar.
5. Escolha OK.

Outros clientes SFTP

Para outros clientes SFTP, desative os seguintes recursos, se disponíveis:

- Uploads de arquivos temporários (faça upload para arquivo temporário e renomeie)
- Retomar transferências usando arquivos temporários
- Uploads atômicos usando operações de renomeação
- Modo de anexação para uploads

Consulte a documentação do cliente para ver as etapas específicas de configuração.

Solução de problemas de armazenamento FSx

Esta seção descreve como identificar e resolver problemas comuns ao usar o Transfer Family com sistemas de arquivos FSx.

Problemas de operação de arquivos

Permissão negada

Se você receber erros de permissão negada:

1. Verifique se a função do IAM tem as permissões corretas para o alias do ponto de acesso. Você pode fazer isso testando diretamente com as APIs do S3.

2. Verifique se a política do ponto de acesso permite a função do IAM.
3. Verifique se o usuário do sistema de arquivos tem permissões no caminho de destino.
4. Confirme se o mapeamento do diretório inicial usa o alias de ponto de acesso correto.

O upload falha com o WinSCP

Se o upload do arquivo falhar com o WinSCP, desative a renomeação temporária:

1. No WinSCP, escolha Opções e, em seguida, Preferências.
2. Escolha Transferência e, em seguida, Resistência.
3. Em Habilitar transferência resume/transfer para nome de arquivo temporário, escolha Desabilitar.

Para obter mais informações, consulte [the section called “Configurando clientes de transferência de arquivos”](#).

Falha no upload do arquivo

Se o upload do arquivo falhar:

1. Verifique se o tamanho do arquivo está abaixo de 5 GB.
2. Verifique se o volume FSx tem armazenamento disponível suficiente.
3. Monitore CloudWatch as métricas de limitação.

Aplicativos web Transfer Family

Você pode criar aplicativos web para habilitar uma interface simples para transferir dados de e para o Amazon Simple Storage Service (S3) por meio de um navegador da web. Isso não exige que você crie ou provisione AWS Transfer Family servidores.

Antes da introdução dos aplicativos web Transfer Family, os usuários finais precisavam usar uma solução cliente, personalizada ou de terceiros para acessar seus dados no Amazon S3. Isso ocorreu devido aos rigorosos requisitos de segurança para clientes e parceiros e porque os aplicativos dos clientes são difíceis de operar para usuários não técnicos.

Com o lançamento de aplicativos web, agora você pode estender um portal de marca, seguro e altamente disponível para que seus usuários finais naveguem, façam upload e baixem dados no Amazon S3. Os aplicativos web são integrados de forma nativa com o Centro de Identidade do AWS IAM Amazon S3 Access Grants. Isso significa que somente seus usuários autenticados podem visualizar os dados que estão autorizados a acessar. Os aplicativos web são criados usando o [Storage Browser para Amazon S3](#) e oferecem as mesmas funcionalidades do usuário final em uma oferta totalmente gerenciada, sem precisar escrever código ou hospedar seu próprio aplicativo.

Para obter mais informações sobre o outro Serviços da AWS que você usa com os aplicativos web Transfer Family, consulte a documentação a seguir:

- [Gerenciando o acesso com o S3 Access Grants no Guia do usuário do Amazon Simple Storage Service](#)
- [Centro de Identidade do AWS IAM Guia do usuário](#)
- [Workshop sobre subsídios de acesso ao Amazon S3](#)
- [Anunciando aplicativos AWS Transfer Family web para transferências de arquivos totalmente gerenciadas do Amazon S3](#)

Os recursos a seguir estão disponíveis para ajudar você a começar a usar os aplicativos web Transfer Family.

- O guia do usuário oferece um passo a passo detalhado sobre a configuração de um aplicativo web Transfer Family aqui: [Tutorial: Configurando um aplicativo web básico do Transfer Family](#)
- O AWS Getting Started Resource Center oferece um tutorial aqui: [Introdução ao aplicativo AWS Transfer Family web](#).

- Veja [Introdução ao aplicativo AWS Transfer Family web](#).

Regiões da AWS para aplicativos web Transfer Family

AWS Transfer Family os aplicativos web estão disponíveis em todas as regiões suportadas pelo Transfer Family, conforme listado na [Tabela de AWS Regiões](#), exceto na Ásia-Pacífico (Nova Zelândia) AWS European Sovereign Cloud e.

Os endpoints VPC para aplicativos web são compatíveis em todos os Regiões da AWS lugares onde os aplicativos web estão disponíveis.

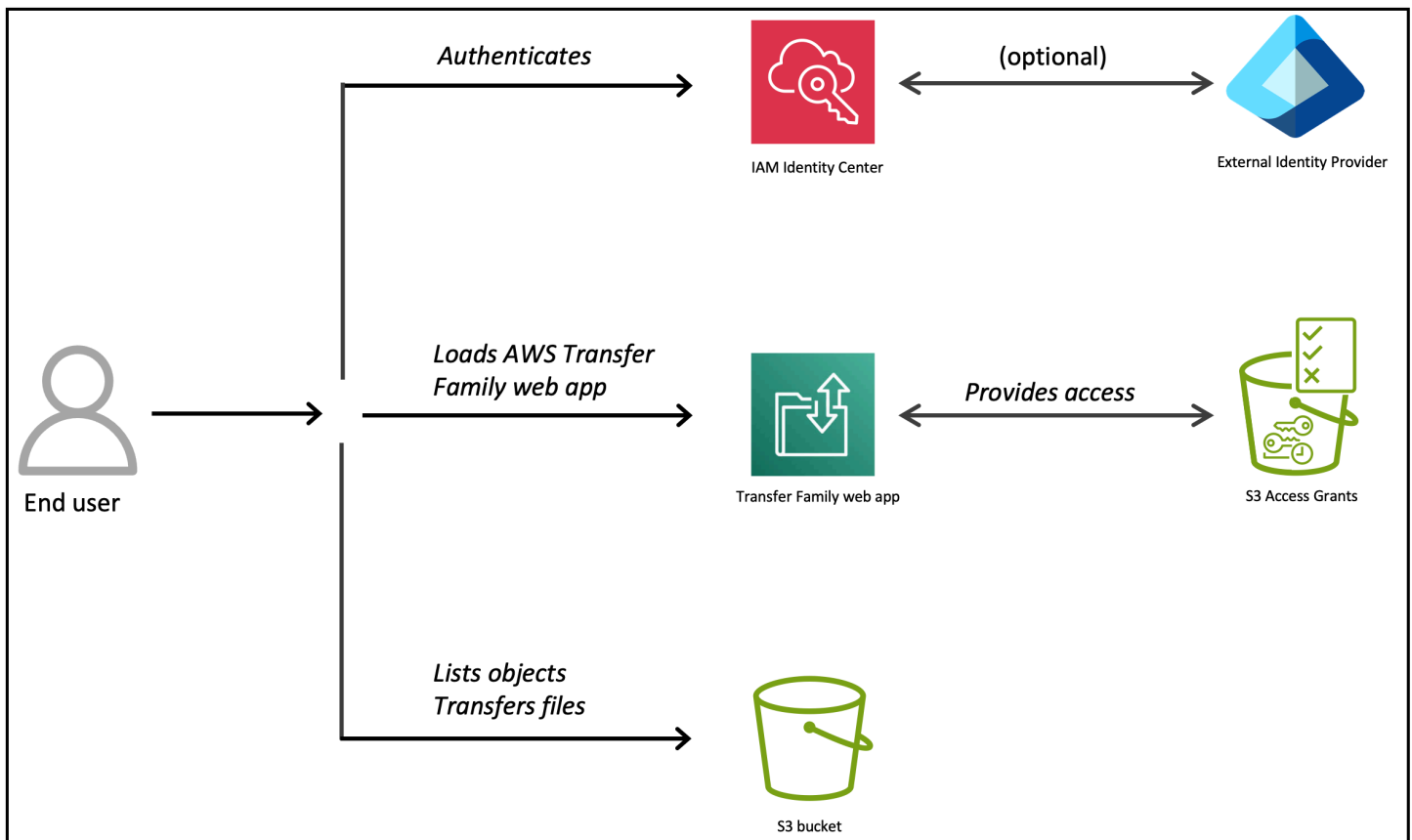
Compatibilidade do navegador para aplicativos AWS Transfer Family da web

Os aplicativos web Transfer Family são compatíveis com os seguintes navegadores.

Navegador	Versão	Compatibilidade
Microsoft Edge	Últimas 3 versões	Compatível
Mozilla Firefox	Últimas 3 versões	Compatível
Google Chrome	Últimas 3 versões	Compatível
Apple Safari	Últimas 3 versões	Compatível

Como criar um aplicativo web Transfer Family

O diagrama a seguir ilustra a arquitetura do aplicativo web Transfer Family.



Com base no diagrama, você pode ver que os aplicativos web Transfer Family interagem com o seguinte Serviços da AWS:

- Amazon S3 para armazenamento e Amazon S3 Access Grants para adquirir credenciais de sessão.
- Centro de Identidade do AWS IAM como provedor de identidade federado.
- Amazon CloudFront se você configurar uma URL personalizada para seu aplicativo web.

Observe as seguintes limitações ao usar aplicativos da web.

- Número máximo de resultados de pesquisa por consulta: 10.000
- Os buckets do Amazon S3 usados pelo aplicativo web Transfer Family devem estar na mesma conta do próprio aplicativo web. Cross-account No momento, não há suporte para buckets.
- Amplitude máxima de pesquisa por consulta: 10.000 arquivos pesquisados
- Tamanho máximo de upload por arquivo: 160 GB (149 GiB)
- Tamanho máximo do arquivo para cópia: 5,36 GB (5 GiB)

- Não há suporte para nomes de pastas que comecem ou terminem com pontos (.)

Pré-requisitos

Em AWS Identity and Access Management, configure as funções necessárias. Cole os blocos de código que fornecemos nas instruções. Para obter informações sobre como configurar as funções necessárias, consulte [Configurar funções do IAM para aplicativos web Transfer Family](#).

- Crie uma função de portador de identidade.
- Crie uma função do IAM para ser usada pelo S3 Access Grants. O S3 Access Grants assume essa função do IAM para fornecer credenciais temporárias ao beneficiário da localização registrada do Amazon S3.

Processo para criar um aplicativo web Transfer Family

Para criar seu aplicativo web e colocar seus usuários finais em funcionamento, você executa as seguintes tarefas:

1. Configure o IAM Identity Center para atuar como seu provedor de identidade federado. Execute as seguintes tarefas no IAM Identity Center. Para obter mais detalhes sobre a configuração do IAM Identity Center, consulte [Configure seu provedor de identidade para os aplicativos web Transfer Family](#).
 - a. Crie uma instância do IAM Identity Center, se você ainda não tiver uma.
 - b. Determine sua fonte de identidade. Ele pode ser o diretório padrão do IAM Identity Center ou um provedor terceirizado (por exemplo, Okta).
 - c. Crie ou identifique os usuários ou grupos que usarão seu aplicativo web.
 - d. Se você estiver usando o diretório do IAM Identity Center para sua fonte de identidade, anote os IDs de usuário ou grupo que você criou. Você precisará deles posteriormente ao criar uma concessão de acesso usando o S3 Access Grants.
2. No Amazon S3, configure as concessões de acesso ao Amazon S3. Para obter mais informações sobre a funcionalidade Concessões de Acesso do S3, consulte [Configurar Amazon S3 Access Grants para aplicativos web Transfer Family](#).
 - Crie uma instância do S3 Access Grants se você ainda não tiver uma. Região da AWS
 - Registre sua localização usando a função do IAM.
 - Crie a concessão de acesso.

3. Em Transfer Family, execute as seguintes tarefas.

- a. Crie o aplicativo web Transfer Family. Para obter mais informações sobre como criar o aplicativo web Transfer Family, consulte [Configurar um aplicativo web Transfer Family](#).

 Important

Configure o compartilhamento de Cross-origin recursos (CORS) para todos os buckets do Amazon S3 usados pelo seu aplicativo web. Para obter informações sobre como configurar o CORS, consulte [Configure o compartilhamento de Cross-origin recursos \(CORS\) para seu bucket](#).

- b. Atribua usuários ou grupos ao aplicativo web. Para obter mais informações sobre como atribuir usuários e grupos, consulte [Atribuir ou adicionar usuários ou grupos a um aplicativo web Transfer Family](#).
- c. (Opcional) Atualize o endpoint de acesso do seu aplicativo web com um URL personalizado. Para obter informações sobre como criar um URL personalizado, consulte [Atualize seu endpoint de acesso com um URL personalizado](#).
- d. Forneça aos usuários finais a URL do endpoint de acesso para que eles possam fazer login e interagir com seu aplicativo web.

Configure seu provedor de identidade para os aplicativos web Transfer Family

A seção a seguir descreve como configurar seu provedor de identidade.

Para começar, você deve ter uma fonte de identidade. Você pode usar um diretório do IAM Identity Center ou um provedor de identidade externo. AWS Directory Service for Microsoft Active Directory. O Transfer Family usa o IAM Identity Center como um provedor de identidade federado, que é um sistema que armazena as credenciais do usuário e autentica os usuários em várias organizações.

Se você não estiver usando um diretório do IAM Identity Center como fonte de identidade, consulte os tópicos a seguir:

- [Gerenciar um provedor de identidade externo](#)
- [Conecte-se a um diretório do Microsoft AD](#)
- [Instâncias de organização e conta do IAM Identity Center](#)

- [Tutoriais de origem de identidade do IAM Identity Center](#)

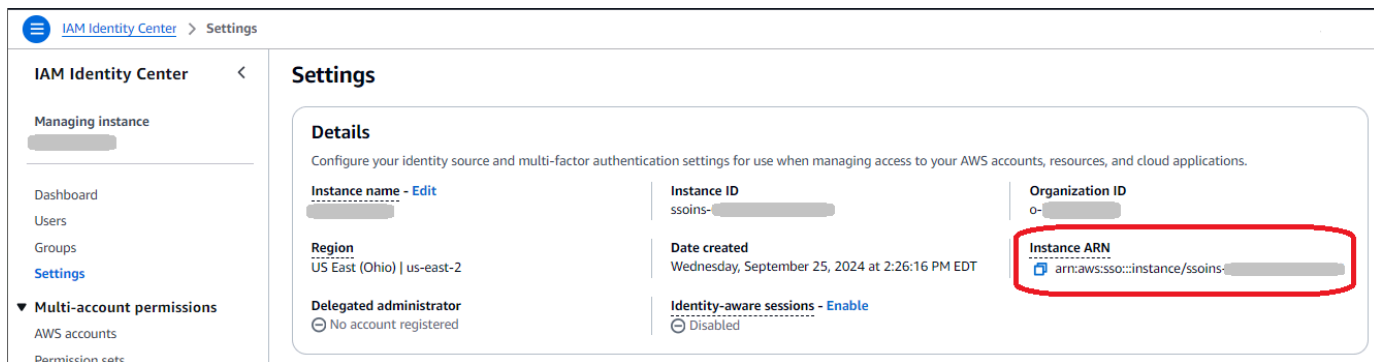
 Note

Você só pode ter uma fonte de identidade no IAM Identity Center, por instância, por Região da AWS. Para obter detalhes, consulte os [pré-requisitos e considerações do IAM Identity Center](#).

Se você planeja usar o diretório do IAM Identity Center como sua fonte de identidade e quer uma configuração rápida, pode pular este tópico e acessar [Crie um aplicativo web Transfer Family](#) para criar uma instância do IAM Identity Center a partir do assistente.

Para configurar Centro de Identidade do AWS IAM para uso com os aplicativos web Transfer Family

1. Faça login no Console de gerenciamento da AWS e abra o Centro de Identidade do AWS IAM console em <https://console.aws.amazon.com/singlesignon/>.
2. Você pode criar e usar uma instância de conta ou uma instância de organização do Centro de Identidade do AWS IAM.
 - Para obter detalhes sobre instâncias de conta, consulte [Criar uma instância de conta de Centro de Identidade do AWS IAM](#). Com uma instância de conta do IAM Identity Center, você pode implantar aplicativos AWS gerenciados compatíveis e aplicativos gerenciados pelo cliente baseados no OpenID Connect (OIDC). As instâncias de conta oferecem suporte a implantações isoladas de aplicativos em um único aplicativo Conta da AWS, aproveitando os recursos do portal de acesso e identidade da força de trabalho do IAM Identity Center.
 - Para obter detalhes sobre as instâncias da organização, consulte [Instâncias da organização do IAM Identity Center](#). Você pode gerenciar centralmente o acesso de usuários e grupos com uma única instância da organização.
3. Na página de configurações do IAM Identity Center, anote o ARN da instância. Você precisará desse valor ao criar uma instância do Amazon S3 Access Grant.



4. Crie um ou mais usuários e, opcionalmente, grupos para usar com seu aplicativo web Transfer Family. Se você estiver usando um diretório do IAM Identity Center como seu provedor de identidade, você também pode adicionar usuários diretamente do próprio aplicativo web. Para obter mais informações, consulte [Atribuir ou adicionar usuários ou grupos a um aplicativo web Transfer Family](#).

Configurar funções do IAM para aplicativos web Transfer Family

Você precisará de duas funções: uma para usar como portador de identidade para seu aplicativo web e uma segunda para configurar uma concessão de acesso. Uma função de portador de identidade é uma função que inclui a identidade de um usuário autenticado em suas sessões. Ele é usado para fazer solicitações ao S3 Access Grants para acesso aos dados em nome do usuário.

Note

Você pode pular o procedimento para criar uma função de portador de identidade. Para obter informações sobre como fazer com que o serviço Transfer Family crie a função de portador de identidade, consulte [Crie um aplicativo web Transfer Family](#).

Você pode pular o procedimento para criar uma função de concessão de acesso. No procedimento para criar uma concessão de acesso, na etapa em que você registra um local do S3, escolha Criar nova função.

Crie uma função de portador de identidade

1. Faça login no Console de gerenciamento da AWS e abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. Escolha Funções e, em seguida, Criar função.

3. Escolha Política de confiança personalizada e cole o código a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

4. Escolha Avançar e, em seguida, pule Adicionar permissões e selecione Avançar novamente.
5. Insira um nome, por exemplo web-app-identity-bearer.
6. Escolha Criar função para criar a função de portador de identidade.
7. Escolha a função que você acabou de criar na lista e, no painel Políticas de permissões, escolha Adicionar permissões > Criar política embutida.
8. No editor de políticas, selecione JSON e cole o bloco de código a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "s3:ListAccessGrantsInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

9. Para o nome da política AllowS3AccessGrants, insira e selecione Criar política.

Em seguida, você cria a função que o S3 Access Grants assume para fornecer credenciais temporárias ao beneficiário.

 Note

Se você permitir que o serviço crie a função de portador de identidade para você, essa função configurará uma proteção adjunta confusa. Portanto, seu código é diferente do que é exibido aqui.

Crie uma função de concessão de acesso

1. Faça login no Console de gerenciamento da AWS e abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. Escolha Funções e, em seguida, Criar função. Essa função deve ter permissão para acessar seus dados do S3 na Região da AWS.
3. Escolha Política de confiança personalizada e cole o código a seguir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

4. Escolha Avançar para adicionar uma política mínima conforme descrito em [Registrar um local](#). Embora não seja recomendado, você pode adicionar a política AmazonS3FullAccessgerenciada, que pode ser muito permissiva para suas necessidades.
5. Escolha Avançar e insira um nome (por exemplo access-grants-location).
6. Escolha Criar função para criar a função.

Note

Se você permitir que o serviço crie a função de concessão de acesso para você, essa função configurará uma proteção adjunta confusa. Portanto, seu código é diferente do que é exibido aqui.

Configurar um aplicativo web Transfer Family

Esta seção descreve os procedimentos para criar um aplicativo web Transfer Family. Para atribuir usuários e grupos que possam usá-lo, consulte [Atribuir ou adicionar usuários ou grupos a um aplicativo web Transfer Family](#).

Note

Repita esses procedimentos para adicionar outros aplicativos da web. Você pode reutilizar as funções do IAM que você criou anteriormente. Certifique-se de adicionar os endpoints de acesso para os novos aplicativos web à política de compartilhamento de Cross-origin recursos (CORS) de cada bucket.

Crie um aplicativo web Transfer Family

Note

Se você não estiver usando o diretório do IAM Identity Center para seu provedor de identidade, não tente criar um aplicativo web até que você já tenha configurado o IAM Identity Center e configurado um provedor de identidade terceirizado, conforme descrito em [Configure seu provedor de identidade para os aplicativos web Transfer Family](#).

Conclua as etapas a seguir para criar um aplicativo web Transfer Family.

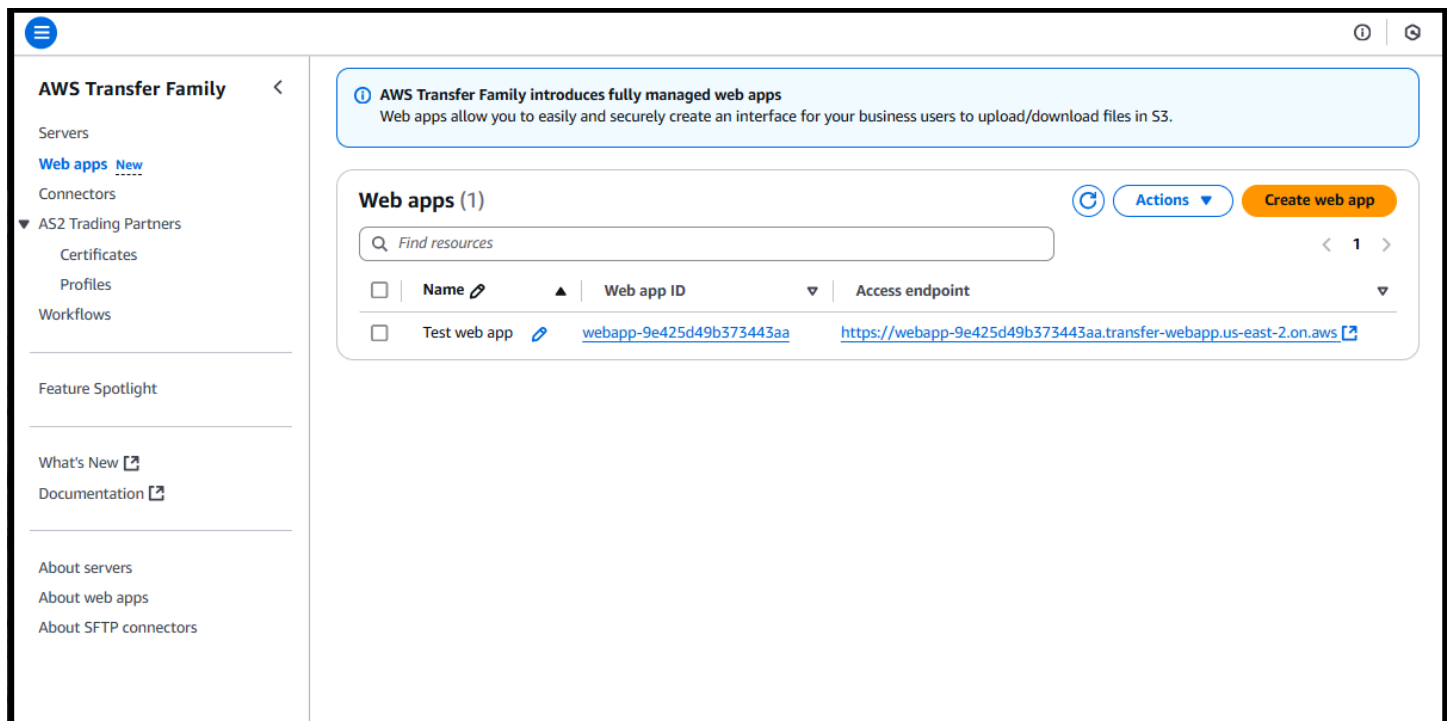
Para criar um aplicativo web Transfer Family

1. Faça login no Console de gerenciamento da AWS e abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.

2. No painel de navegação esquerdo, escolha Aplicativos Web.
3. Escolha Criar aplicativo web.

Para acesso à autenticação, o painel é preenchido da seguinte forma.

- Se você já criou uma instância de organização ou conta no Centro de Identidade do AWS IAM, verá esta mensagem: Seu AWS Transfer Family aplicativo está conectado a uma instância de conta do IAM Identity Center.
 - Se você já tem uma instância de conta e é membro de uma instância da organização, você tem a opção de escolher qual instância conectar.
 - Se você ainda não tem uma instância de conta ou é membro de uma instância da organização, você tem as opções para criar uma instância de conta.
4. Em Tipo de endpoint, escolha o tipo de endpoint Acessível publicamente. Para um endpoint hospedado no VPC, consulte [Crie um aplicativo web Transfer Family em uma VPC](#).
 5. No painel Tipo de permissão, você pode usar uma função criada anteriormente ou fazer com que o serviço crie uma para você.
 - Se você já criou uma função de portador de identidade, escolha Usar uma função existente e escolha sua função no menu Selecionar uma função existente.
 - Para que o serviço crie uma função para você, escolha Criar e use uma nova função de serviço.
 6. No painel Unidades do aplicativo Web, escolha um valor. Uma unidade de aplicativo da web permite a atividade do aplicativo da web em até 250 sessões exclusivas. Ao criar um aplicativo web, você provisiona quantas unidades você precisa com base nos volumes de pico de carga de trabalho esperados. Alterar suas unidades de aplicativos web afeta seu faturamento. Para obter mais informações sobre preços consulte [AWS Transfer Family Pricing](#).
 7. Se você estiver usando Transfer Family em um AWS GovCloud (US) Region, você pode marcar a caixa de seleção do endpoint FIPS Enabled no painel FIPS Enabled. Para todos os outros Regiões da AWS, essa opção não está disponível.
 8. (Opcional) Adicione uma tag para ajudar você a organizar seus aplicativos da web. Sugerimos que você adicione uma tag com Nome como chave e um nome descritivo como valor.
 9. Escolha Próximo. Nessa tela, você pode, opcionalmente, fornecer um título para seu aplicativo web. Se você não fornecer um título, o título padrão de Transfer Web App será fornecido. Você também pode fazer upload de arquivos de imagem para seu logotipo e favicon.
 10. Escolha Avançar e, em seguida, escolha Criar aplicativo web.



Note

Certifique-se de configurar uma política de compartilhamento de Cross-origin recursos (CORS) para todos os buckets que são acessados do endpoint do aplicativo web.

Endereçamento IP

Os aplicativos web da Transfer Family usam endpoints de pilha dupla, oferecendo suporte à conectividade IPv4 e IPv6. Para autenticação, os aplicativos da web usam Centro de Identidade do AWS IAM, que também oferecem suporte a IPv6 por meio de endpoints de pilha dupla.

Se sua conta tinha aplicativos web em uma região quando o suporte de endpoint do IAM Identity Center de pilha dupla foi lançado, todos os aplicativos web dessa conta e região continuarão usando o endpoint do IPv4-only IAM Identity Center para compatibilidade com versões anteriores. Isso se aplica tanto aos aplicativos da web existentes quanto aos recém-criados. As contas que não tinham aplicativos web no momento do lançamento usam o endpoint de pilha dupla do IAM Identity Center. Se você precisar alterar qual endpoint do IAM Identity Center seu aplicativo web usa, entre em contato com o AWS Support.

 Note

Para determinar qual endpoint seu aplicativo web usa, inspecione a URL ao ser redirecionado para a página de login do IAM Identity Center:

- IPv4-only: [Region].signin.aws.amazon.com
- Dual-stack: [Region].sso.signin.aws

Se sua organização usa firewalls ou gateways de rede, liste o IPv4 existente e os novos endpoints do IAM Identity Center de pilha dupla para garantir acesso ininterrupto, independentemente do endpoint usado por seus aplicativos web. Para ver a lista completa de domínios e endpoints de URL a serem permitidos, consulte [Atualizar firewalls e gateways para permitir o acesso ao portal de acesso no Guia do usuário do AWS IAM Identity Center](#).

Crie um aplicativo web Transfer Family em uma VPC

Esta seção descreve os procedimentos para criar um aplicativo web Transfer Family em uma VPC. Você pode hospedar o endpoint do seu aplicativo web em uma nuvem privada virtual (VPC) para usar na transferência de dados de e para um bucket do Amazon S3 sem usar a Internet pública. Para atribuir usuários e grupos que podem usar seu aplicativo web, consulte [Atribuir ou adicionar usuários ou grupos a um aplicativo web Transfer Family](#).

 Note

Para garantir um fluxo de dados privado de ponta a ponta ao usar um endpoint VPC do aplicativo web Transfer Family, você deve implementar três componentes adicionais. Primeiro, configure um PrivateLink endpoint para as operações da API Amazon S3 Control, o que é necessário para as chamadas de API do Amazon S3 Access Grants. Segundo, configure um endpoint para acesso aos dados do Amazon S3 usando um endpoint do Amazon PrivateLink S3 Gateway (para tráfego de dentro da sua VPC) ou um endpoint de interface do Amazon S3 (para tráfego de redes locais via VPN ou Direct Connect). Em terceiro lugar, bloqueie o acesso ao bucket do Amazon S3 atualizando as políticas do bucket para permitir apenas o tráfego desses endpoints de VPC. Essa combinação garante que todas as transferências de dados permaneçam em sua infraestrutura de rede privada e nunca atravessem a Internet pública.

Crie um aplicativo web Transfer Family

Pré-requisitos

- Centro de Identidade do AWS IAM configurado com o provedor de identidade configurado. Consulte [Configure seu provedor de identidade para os aplicativos web Transfer Family](#).
- Configuração de componentes de rede e VPC. Consulte [Criar uma VPC](#).
- Endpoint de API configurado para operações de controle do Amazon S3. Consulte [Acesso aos endpoints da interface Amazon S3](#).
- Configuração de endpoints VPC para Amazon S3 (gateway ou interface). Consulte [Tipos de VPC endpoints para o Amazon S3](#). Se você estiver usando um endpoint de interface, deverá habilitar o DNS privado. Por exemplo, consulte [Introdução ao suporte de DNS privado para o Amazon AWS PrivateLink S3](#) com.

Note

Centro de Identidade do AWS IAM não oferece suporte a endpoints VPC; todas as solicitações de autenticação transitam pela Internet pública. Além disso, os aplicativos web da Transfer Family exigem acesso à Internet para carregar conteúdo estático (como JavaScript arquivos CSS e HTML). Os requisitos para acesso público à Internet são separados do acesso aos dados. Seu VPC endpoint garante que as conexões sejam roteadas por meio de sua infraestrutura de VPC.

Para criar um aplicativo web Transfer Family

1. Faça login no Console de gerenciamento da AWS e abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, escolha Aplicativos Web.
3. Escolha Criar aplicativo web. Para acesso à autenticação, o painel é preenchido da seguinte forma.
 - Se você já criou uma instância de organização ou conta no Centro de Identidade do AWS IAM, verá esta mensagem: Seu AWS Transfer Family aplicativo está conectado a uma instância de conta do IAM Identity Center.

- Se você já tem uma instância de conta e é membro de uma instância da organização, você tem a opção de escolher qual instância conectar.
 - Se você ainda não tem uma instância de conta ou é membro de uma instância da organização, você tem as opções para criar uma instância de conta.
4. Na seção Configuração do Endpoint, escolha como seus usuários acessarão seu aplicativo web:
- **Acessível publicamente:** o endpoint do seu aplicativo web pode ser acessado pelo público via HTTPS. Essa opção não exige nenhuma configuração de VPC, o que a torna simples de configurar e adequada para aplicativos destinados ao amplo uso público.
 - **Hospedado em VPC:** seu endpoint de aplicativo web está hospedado em sua Nuvem Privada Virtual (VPC), fornecendo acesso à rede privada por meio de sua rede VPC ou conexões VPN. AWS Direct Connect Essa opção oferece segurança aprimorada por meio do isolamento da rede e é recomendada para aplicativos internos.

Ao configurar um endpoint hospedado em VPC, você precisará especificar:

- **VPC:** selecione uma VPC existente ou crie uma nova. O botão Criar uma VPC está disponível.
- **Zonas de disponibilidade:** escolha as zonas de disponibilidade em que seu endpoint será implantado.
- **Sub-redes:** selecione sub-redes em cada zona de disponibilidade escolhida.
- **Grupos de segurança:** selecione ou crie grupos de segurança para controlar o acesso com base nos endereços IP de origem. Se não for especificado, o grupo de segurança padrão da VPC será usado. Gerencie grupos de segurança por meio do console VPC. Configure seus grupos de segurança da VPC para permitir o tráfego de entrada da sua rede via HTTPS na porta TCP 443. Isso é necessário para a autenticação do IAM Identity Center e para o carregamento de conteúdo estático do aplicativo web.

 Note

O endpoint de acesso não pode ser personalizado para endpoints VPC. Para adicionar um URL personalizado, use o endpoint público.

Post-creation etapas

- Certifique-se de configurar uma política de compartilhamento de Cross-origin recursos (CORS) para todos os buckets que são acessados do endpoint do aplicativo web. Consulte [Cross-origin política de compartilhamento de recursos \(CORS\)](#).
- Atualize sua política de bucket para permitir tráfego proveniente somente de sua VPC por meio de seu VPC endpoint. Consulte [Restringir o acesso a um VPC endpoint específico](#).
- Atribua ou adicione usuários ou grupos ao aplicativo web Transfer Family. Consulte [Atribuir ou adicionar usuários ou grupos a um aplicativo web Transfer Family](#).

Cross-origin política de compartilhamento de recursos (CORS)

Você deve configurar o compartilhamento de recursos de origem cruzada (CORS) para todos os buckets usados pelo seu aplicativo web. Para obter mais informações sobre CORS, consulte [Configure o compartilhamento de Cross-origin recursos \(CORS\) para seu bucket](#).

Important

Antes de usar o exemplo de política a seguir, substitua a Origem permitida pelo seu endpoint de acesso. Caso contrário, seus usuários finais receberão uma mensagem de erro ao tentarem acessar um local no seu aplicativo web.

Exemplo de política:

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://vpce-1234567-example.vpce-mq.transfer-webapp.us-east-1.on.aws"
    ]
  }
]
```

```
],
  "ExposeHeaders": [
    "last-modified",
    "content-length",
    "etag",
    "x-amz-version-id",
    "content-type",
    "x-amz-request-id",
    "x-amz-id-2",
    "date",
    "x-amz-cf-id",
    "x-amz-storage-class",
    "access-control-expose-headers"
  ],
  "MaxAgeSeconds": 3000
}
```

Restringir o acesso a um VPC endpoint específico

O seguinte é um exemplo de uma política de bucket do Amazon S3 que restringe o acesso a um bucket específico, `amzn-s3-demo-bucket`, somente no VPC endpoint com o ID `vpce-1a2b3c4d`. Se o endpoint especificado não for usado, essa política negará todo acesso ao bucket. A condição `aws:SourceVpce` especifica o endpoint. A condição `aws:SourceVpce` não requer um ARN para o recurso do VPC endpoint, somente o ID do VPC endpoint. Para obter mais informações sobre como atualizar sua política de bucket para permitir somente o tráfego proveniente da sua VPC, [consulte Como controlar o acesso de VPC endpoints com políticas de bucket](#). Para obter mais informações sobre o uso de condições em uma política, consulte [Exemplos de políticas de bucket usando chaves de condição](#). Como pré-requisito para aplicar essa política, você deve criar um endpoint Amazon [S3 VPC](#).

Important

Antes de usar a política de exemplo a seguir, substitua o ID do VPC endpoint por um valor apropriado para o caso de uso. Caso contrário, não será possível acessar o bucket.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
```

```
"Statement": [  
  {  
    "Sid": "Access-to-specific-VPCE-only",  
    "Principal": "*",  
    "Action": "s3:*",  
    "Effect": "Deny",  
    "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket",  
                 "arn:aws:s3:::amzn-s3-demo-bucket/*"],  
    "Condition": {  
      "StringNotEquals": {  
        "aws:SourceVpce": "vpce-1a2b3c4d"  
      }  
    }  
  }  
]
```

Atribuir ou adicionar usuários ou grupos a um aplicativo web Transfer Family

Depois de criar um aplicativo web Transfer Family, você pode atribuir usuários e grupos que podem então acessar o aplicativo web. Você pode recuperar usuários que já foram criados e armazenados no IAM Identity Center ou [adicionar novos usuários diretamente](#) (se estiver usando um diretório do IAM Identity Center como seu provedor de identidade). Se você adicionar novos usuários, eles também serão adicionados à sua instância do IAM Identity Center.

Observe o seguinte:

- Você só pode adicionar novos usuários se estiver usando o diretório do IAM Identity Center como sua fonte de identidade e tiver as permissões adequadas. Se você for membro de uma instância da organização, talvez não tenha as permissões necessárias para adicionar usuários.

Note

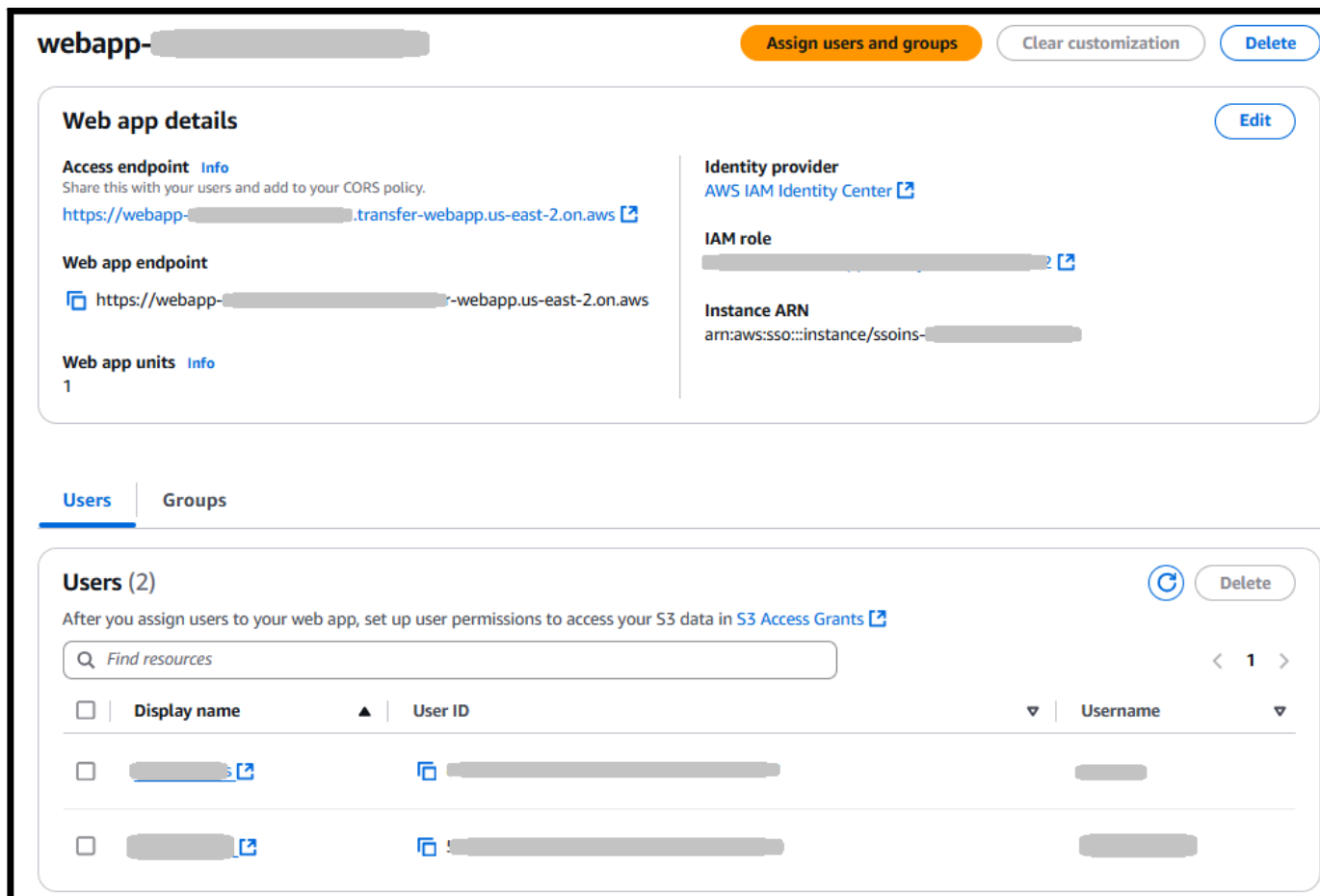
Se você não atribuir usuários ou grupos ao seu aplicativo, seus usuários receberão um erro ao tentarem fazer login no seu aplicativo web.

- Se você criar um novo usuário, também deverá criar uma concessão de acesso do S3 para esse usuário para que ele possa acessar os dados em seu aplicativo web.

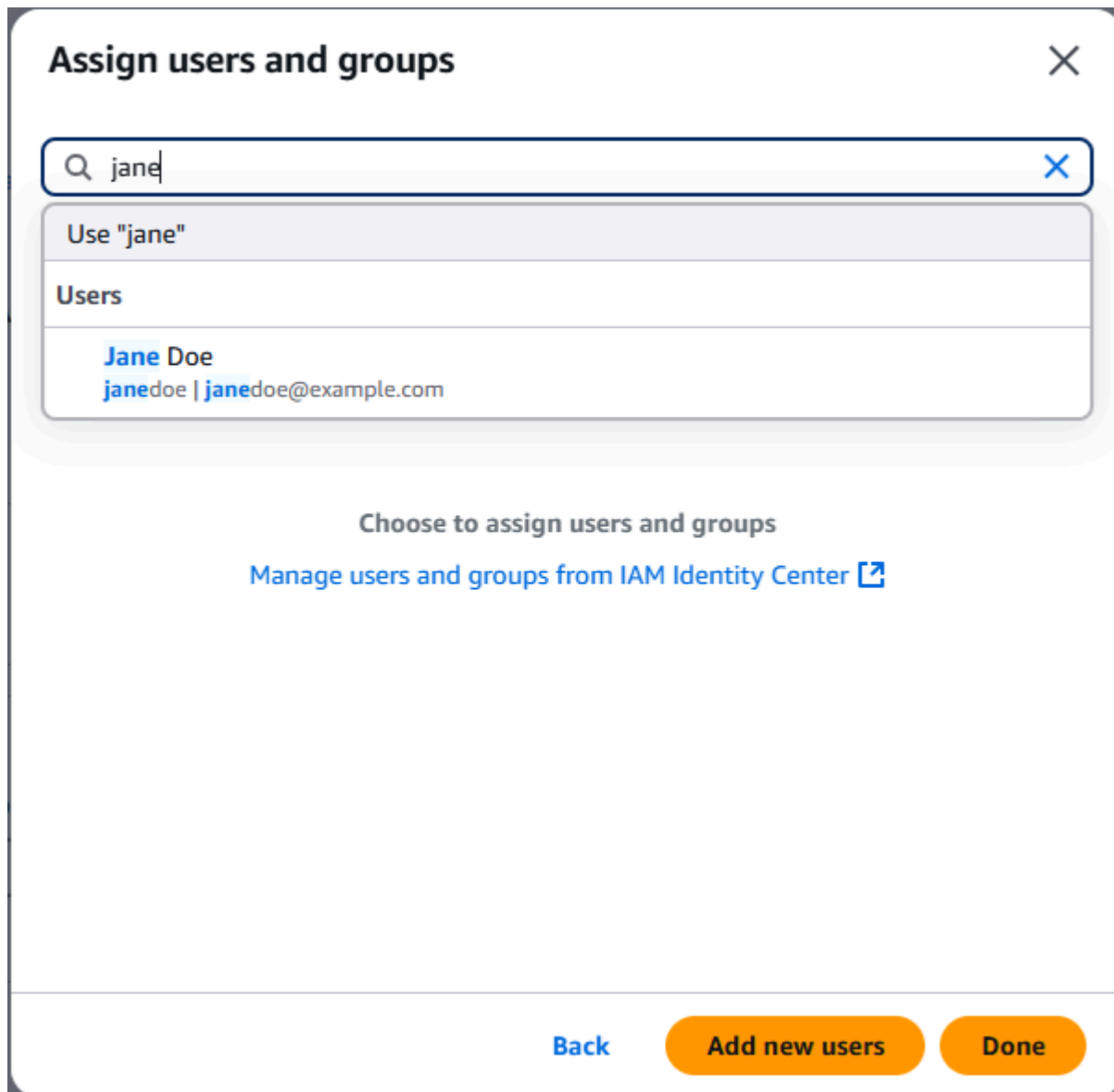
- Depois de criar um novo usuário, esse usuário recebe um e-mail de integração do IAM Identity Center com instruções sobre como proceder.

Para atribuir usuários a um aplicativo web Transfer Family

1. Navegue até sua lista de aplicativos da web e escolha aquela que você deseja editar.
2. Escolha Atribuir usuários e grupos.



3. Para atribuir usuários que você criou anteriormente no IAM Identity Center, selecione Atribuir usuários e grupos existentes. Para criar novos usuários, vá para a etapa 4.
 - a. Uma tela de informações é exibida. Escolha Começar para continuar.
 - b. Pesquise o usuário. Observe que nenhum usuário aparece até você começar a inserir seus critérios de pesquisa. Você deve pesquisar pelo nome de exibição, não pelo nome de usuário, se for diferente. Somente as correspondências exatas são retornadas. Se você não conseguir encontrar seu usuário, navegue até o console de gerenciamento do IAM Identity Center, encontre o usuário e copie e cole seu nome de exibição aqui.



- c. Escolha os usuários e grupos a serem adicionados e, em seguida, escolha Atribuir.
4. Para criar um novo usuário, selecione Adicionar e atribuir novos usuários.
 - a. Uma tela de informações é exibida. Escolha Começar para continuar.
 - b. Escolha Add new users (Adicionar novos usuários).
 - c. Insira os seguintes detalhes do usuário na caixa de diálogo: nome de usuário, nome e sobrenome e endereço de e-mail.

Add new users [X]

Info Newly-created users are enabled by default. To grant them access to Add User Widget, you must set their password in the IAM Identity Center console. [Manage user passwords in the IAM Identity Center console](#) [X]

Username
A username is required for this person to sign in to the AWS access portal. You can't change the username later.

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +, -, @, _

First name **Last name**

Email address **Confirm email address**

Display name
This is typically the full name of the user (first and last name) and appears in the users list.

[Cancel](#) [Next](#)

- d. Escolha Avançar e escolha Adicionar para adicionar o usuário e fechar a caixa de diálogo ou Adicionar novo usuário para criar outro usuário.

Configure o compartilhamento de Cross-origin recursos (CORS) para seu bucket

Você deve configurar o compartilhamento de recursos de origem cruzada (CORS) para todos os buckets usados pelo seu aplicativo web. Uma configuração CORS é um documento que define regras que identificam as origens que você permitirá acessar seu bucket. Para obter mais informações sobre o CORS, consulte [Configurando o compartilhamento de recursos de origem cruzada \(CORS\)](#).

 Important

Se você não configurar o CORS, seus usuários finais receberão um erro ao tentarem acessar um local no seu aplicativo web.

Para configurar o compartilhamento Cross-origin de recursos (CORS) para seu bucket Amazon S3

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em. <https://console.aws.amazon.com/s3/>
2. Escolha Buckets no painel de navegação esquerdo, pesquise seu bucket na caixa de diálogo de pesquisa e, em seguida, escolha a guia Permissões.
3. Em compartilhamento Cross-origin de recursos (CORS), escolha Editar e cole o código a seguir.
WebAppEndpoint Substitua pelo endpoint de acesso real do seu aplicativo web. Isso pode ser o endpoint de acesso público ou hospedado em VPC que é criado quando o aplicativo web é criado ou um endpoint de acesso personalizado, se você criar um. Certifique-se de não inserir barras finais, pois isso causa erros quando os usuários tentam fazer login no seu aplicativo web.
 - Exemplo incorreto: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Exemplos corretos:
 - `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`
 - `https://vpce-05668789767a-fh45z079.vpce-mq.transfer-webapp.us-east-1.on.aws`

Se você estiver reutilizando um bucket para vários aplicativos da web, anexe seus endpoints à lista. `AllowedOrigins`

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
```

```
    "HEAD"
  ],
  "AllowedOrigins": [
    "https://WebAppEndpoint"
  ],
  "ExposeHeaders": [
    "last-modified",
    "content-length",
    "etag",
    "x-amz-version-id",
    "content-type",
    "x-amz-request-id",
    "x-amz-id-2",
    "date",
    "x-amz-cf-id",
    "x-amz-storage-class",
    "access-control-expose-headers"
  ],
  "MaxAgeSeconds": 3000
}
]
```

4. Escolha Salvar alterações para atualizar o CORS.

Para testar sua configuração do CORS, consulte [Testando o CORS](#).

Configurar Amazon S3 Access Grants para aplicativos web Transfer Family

Este tópico descreve como adicionar uma concessão de acesso usando o Amazon S3 Access Grants. Essa concessão de acesso define o acesso aos seus dados diretamente para seus usuários e grupos em seu diretório corporativo e vende credenciais temporárias just-in-time, com privilégios mínimos, com base em concessões. Uma concessão individual em uma instância do S3 Access Grants permite que um usuário ou grupo específico em um diretório corporativo tenha acesso em um local registrado em sua instância do S3 Access Grants. Para obter mais detalhes, consulte os [conceitos do S3 Access Grants](#) no Guia do usuário do Amazon S3.

 Note

Você não pode usar o diretório do IAM Identity Center com o S3 Access Grants, exceto com os aplicativos web Transfer Family.

Você deve especificar uma concessão de acesso ao Amazon S3 para propagação de identidade. Uma concessão de acesso ao Amazon S3 armazena os dados que seus usuários finais devem acessar. Quando seus usuários finais acessam seu aplicativo web Transfer Family, o S3 Access Grants passa a identidade do usuário para o aplicativo confiável. Esta seção descreve como adicionar e configurar uma instância de concessão de acesso do Amazon S3 e, em seguida, uma concessão de acesso para um bucket do Amazon S3.

 Note

Prepare o [ARN e o ID de usuário ou grupo da instância do IAM Identity Center](#), pois você precisa que eles concluem a configuração da concessão de acesso.

Para criar uma concessão usando o Amazon S3 Access Grants

1. Faça login no Console de gerenciamento da AWS e abra o console do Amazon S3 em. <https://console.aws.amazon.com/s3/>
2. Crie um bucket ou anote um bucket existente para usar com seu aplicativo web. Para obter informações sobre a criação de buckets, consulte o Guia do [usuário do Amazon S3](#).
3. No painel de navegação esquerdo, escolha Access Grants.
4. Escolha Criar instância do S3 Access Grants e forneça as seguintes informações.
 - Selecione Adicionar instância do IAM Identity Center em **your-Region** onde **your-Region** está sua Região da AWS. Mantenha essa caixa desmarcada se você não estiver usando o IAM Identity Center como seu provedor de identidade.
 - Cole o ARN da instância do IAM Identity Center.

[Amazon S3](#) > [Access Grants](#) > Set up Access Grants Instance

- Step 1
☒ **Create S3 Access Grants instance**
- Step 2
☐ Register S3 Buckets or prefixes as locations
- Step 3
☐ Create grant
- Step 4
☐ Review and finish

Create S3 Access Grants instance [Info](#)

When you create your S3 Access Grants instance, you can use identities from your corporate directory or you can use IAM users and roles. This Access Grants instance serves as the container for your individual grants.

S3 Access Grants instance [Info](#)

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

☒ Add IAM Identity Center instance in US East (Ohio) us-east-2 - *optional*

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

IAM Identity Center instance ARN

You can find the IAM Identity Center instance ARN in the [IAM Identity Center console](#).

arn:aws:sso::instance/ssoins-

Format: arn:aws:sso::instance/<instanceIdentifier>

Escolha Próximo para continuar.

- Registre buckets ou prefixos do S3 como locais. Recomendamos que você registre o local padrão e `s3://` o mapeie para uma função do IAM. A localização nesse caminho padrão abrange o acesso a todos os seus buckets do Amazon S3 na Região da AWS sua conta. Ao criar uma concessão de acesso, você pode restringir o escopo a um bucket, um prefixo ou um objeto dentro do local padrão.

Forneça as informações a seguir.

- Para o Escopo, procure um bucket ou insira o nome do seu bucket e, opcionalmente, um prefixo.
- Para a função do IAM, escolha Criar nova função para que o serviço crie uma função.

Como alternativa, você mesmo pode criar a função, conforme descrito em [Configurar funções do IAM para aplicativos web Transfer Family](#), e inserir seu ARN aqui.

Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Register location

Register location [Info](#)

Registering a location for S3 your S3 Access Grants instance assigns an IAM role the permission to get temporary credentials to access resources within the specified scope.

Location [Info](#)

Location scope [Info](#)

You can't edit the location scope after registering the location.

Scope

s3://

View [\[link\]](#) Browse S3

Format for all buckets: s3://
Format for bucket: s3://<bucket>
Format for prefix: s3://<bucket>/<prefix-with-path>

Permissions

This IAM role allows S3 Access Grants to access your specified location scope.

[To ensure the role has proper permissions to access the location scope, consult the list of permissions \[link\].](#)

IAM role [Info](#)

This IAM role allows S3 Access Grants to access your specified location scope.

☒ Create new role
☐ Choose from existing IAM roles
☐ Enter IAM role ARN

Cancel Register location

Escolha Próximo para continuar.

6. Na tela Criar concessão, forneça os seguintes detalhes.

- Em Permissões, selecione Ler e gravar. As permissões de concessão de acesso podem ser somente leitura ou leitura e gravação, mas não há suporte para somente gravação.
- Para o tipo de beneficiário, escolha Identidade do diretório no IAM Identity Center.
- Em Tipo de identidade de diretório, selecione Usuário ou Grupo, dependendo do tipo que você deseja registrar agora.
- No user/group ID do IAM Identity Center, cole o ID do seu usuário ou grupo. Esse ID está disponível no console do IAM Identity Center e no seu aplicativo web Transfer Family na tabela de usuários e grupos.

Create Grant [Info](#)

Grant [Info](#)

Grant a user or role a specific level of access to your S3 data.

Grant scope

The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location

s3://test

Location ID [Info](#)

IAM role [Info](#)

[web-app-access-grants](#)

[Browse locations](#)

[Register location](#)

Subprefix - optional [Info](#)

Further scope the grant to a bucket, prefix, or an individual object.

*

Don't include any part of the grant already specified in the location.

Format for bucket: <bucket>/*

Format for prefix: <bucket>/<prefix-with-path>*

Format for object: <bucket>/<prefix-with-path>/<object>

Grant scope [Info](#)

s3://test/*

☐ The grant scope is an object

Permissions and access

Grant a user or role a specific level of access to your S3 data.

 The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions

☒ Read

☒ Write

Grantee type [Info](#)

☒ Directory identity from IAM Identity Center

☐ IAM principal

Directory identity type [Info](#)

☒ User

☐ Group

IAM Identity Center user ID [Info](#)

The user that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#)

Format: a1b2c3d4-5678-90ab-cdef-EXAMPLE1111

► **Application - optional**

Escolha Próximo.

7. Revise as configurações na tela. Se tudo estiver correto, escolha Concluir para criar a concessão de acesso. Como alternativa, você pode escolher Cancelar ou Anterior para fazer alterações.

- Step 1
Create S3 Access Grants instance
- Step 2
Register S3 Buckets or prefixes as locations
- Step 3
Create grant
- Step 4
Review and finish

Review and finish

Step 1 - Create S3 Access Grants instance

S3 Access Grants instance

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.
US East (Ohio) us-east-2

Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.
arn:aws:sso:::application/ssoinstance:/apl

Successfully created S3 Access Grants instance

Instance ARN: arn:aws:s3:us-east-2:::access-grants/default

You can grant other accounts access to this S3 Access Grants instance in the Resource Access Management console

Step 2 - Register S3 buckets or prefixes as locations

Location

Location scope

s3://

IAM role

web-app-beta-access-grants

Successfully registered location

Location ID:

Step 3 - Create grants

Grant

Grant a user or role a specific level of access to your S3 data.

Grant scope

s3:///*

IAM role

web-app-beta-access-grants

Location ID

Permissions and access

Access Type

READWRITE

Grantee type

Directory identity user

Grantee ID

Application - optional

-

Successfully created grant

Grant ARN: arn:aws:s3:us-east-2:::access-grants/default/grant/

Create another grant

Cancel Previous Finish

Amazon S3 > Access Grants > US East (Ohio) us-east-2: default

US East (Ohio) us-east-2: default

Share InstanceDelete Instance

S3 Access Grants provides scalable access control to data sets in your S3 buckets. To share an S3 Access Grants instance with external accounts by using the AWS Resource Access Manager console, choose Share instance. With S3 Access Grants, you can use identities from your corporate directory or from AWS Identity and Access Management (IAM) to control access. You can create one S3 Access Grants instance per AWS Region per account.

S3 Access Grants instance overview

Amazon Resource Name (ARN)
arn:aws:s3:us-east-2:access-grants/default

Creation date
October 25, 2024, 11:50:11 (UTC-04:00)

Account ID

IAM Identity Center

IAM Identity Center instance ARN
arn:aws:sso:application/ssoins/apl

DeregisterAdd

GrantsLocations

Grants (1)

DeleteCreate Grant

Find by grant scope or grantee

Grant scopeGrant IDPermissionGrantee typeGrantee IDCreation dateLocation IDApplication ARN

s3://Read, WriteDirectory identity userOctober 25, 2024, 11:57:30 (UTC-04:00)ALL

Isso conclui a configuração do seu aplicativo web. Os usuários e grupos que você configurou podem visitar o aplicativo web no ponto de acesso, fazer login e carregar e baixar arquivos.

Atualize seu endpoint de acesso com um URL personalizado

O endpoint de acesso padrão criado com seu aplicativo web contém identificadores gerados pelo serviço. Para oferecer uma experiência de marca, talvez você queira fornecer uma URL personalizada para que seus usuários acessem seu aplicativo web Transfer Family. Este tópico descreve como atualizar seu endpoint de acesso com uma URL personalizada.

Note

O endpoint de acesso não pode ser personalizado para endpoints VPC. Para adicionar um URL personalizado, use o endpoint público.

Note

O procedimento a seguir depende do uso do modelo de [CloudFormation pilha](#) recomendado. Você não precisa usar o modelo: você pode criar a distribuição usando o [CloudFront console](#) diretamente.

Use um URL personalizado

318

No entanto, o modelo fornecido simplifica o processo e facilita a prevenção de configurações incorretas. Se você não usar o CloudFormation modelo, siga estas diretrizes:

- A [política de solicitação do Origin](#) deve encaminhar cadeias de caracteres de consulta e cookies para a origem e não deve encaminhar o Host cabeçalho para a origem.
- A [política de cache](#) não deve incluir o Host cabeçalho na chave de cache.

Para personalizar o URL do seu aplicativo web

1. Crie uma CloudFront distribuição usando o AWS CloudFormation modelo fornecido pela Transfer Family, modelo de [CloudFormation pilha](#).
 - a. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
 - b. Escolha Criar pilha e especifique o seguinte.
 - Na seção Pré-requisito - Preparar modelo, escolha Escolher um modelo existente.
 - Na seção Especificar modelo escolha Fazer carregar um arquivo de modelo.
 - Salve o arquivo de [modelo da CloudFormation pilha](#) e, em seguida, carregue-o aqui.
 - c. Escolha Avançar e forneça as seguintes informações.
 - WebAppEndpoint: copie o valor do seu aplicativo web
 - AccessEndpoint: forneça o nome de domínio personalizado que você deseja usar
 - AcmCertificateArn: forneça o ARN para um SSL/TLS certificado público ou privado armazenado em AWS Certificate Manager
 - d. Complete o CloudFormation assistente até que sua nova pilha seja criada.
2. Em seu aplicativo web, edite o endpoint do Access, atualizando o URL personalizado para o URL que você deseja usar.

Transfer Family > Web apps > webapp- > Edit web app details

Edit web app details

Authentication access [Info](#)

Connect or create an Identity Center instance

Instance ARN

Select your instance ARN

Permission type [Info](#)

Create and use a new service role

Create and use an IAM role to allow the service to access the AWS resource it needs to create your application

Use an existing role

Use an existing IAM role to allow the service to access the AWS resources it needs to create your application

By selecting use existing role, you need to manually create an IAM Role in order for the Transfer Family web application to access your AWS services data. Please select an existing IAM role below or [create a new role in IAM console](#)

Select an existing role

If your newly created role is not showing up in the dropdown list, please try the refresh button on the right

Find your IAM role

Make sure you have attached the trust policy and permission policy to the role you selected.

[learn more about required policies](#)

Access endpoint [Info](#)

Map your own fully qualified domain name to this web app so your end users can use your custom URL, not the service-provided URL to access your web app. Note- you can only complete this step in CloudFront after you have created the web app.

Custom URL

`https://my-custom-url`

[Create a new distribution](#)

3. Crie registros DNS para direcionar o tráfego do seu nome de domínio personalizado para a CloudFront distribuição. Se você estiver usando o Route 53 para a zona, poderá criar um registro Alias ou CNAME para o nome da CloudFront distribuição (por exemplo, xxxx.cloudfront.net). Para obter informações sobre como usar o Amazon Route 53 com CloudFront, consulte [Configuração do Amazon Route 53 para rotear o tráfego para uma CloudFront distribuição](#).
4. Atualize sua política de compartilhamento de recursos entre origens substituindo o endpoint de acesso padrão pela seguinte linha no bloco de AllowedOrigins código:

```
"https://custom-url"
```

Você precisa fazer essa alteração para cada bucket usado pelo seu aplicativo web.

Depois de fazer a atualização, a AllowedOrigins seção da sua política de CORS deve ter a seguinte aparência:

```
"AllowedOrigins": [
  "https://custom-url",
```

Você precisa apenas de uma única AllowedOrigins entrada para cada aplicativo web Transfer Family.

Consulte o procedimento [Configurar compartilhamento de Cross-origin recursos \(CORS\) para seu bucket do Amazon S3](#) para obter mais detalhes.

Agora você pode visitar seu endpoint de acesso personalizado e compartilhar esse link com seus usuários finais.

CloudTrail registro para aplicativos web Transfer Family

CloudTrail é um AWS service (Serviço da AWS) que cria um registro das ações realizadas dentro do seu Conta da AWS. Ele monitora e registra continuamente as operações da API para atividades como logins, AWS Command Line Interface comandos e SDK/API operações do console. Isso permite que você mantenha um registro de quem realizou qual ação, quando e de onde. CloudTrail ajuda na auditoria, no gerenciamento de acesso e na conformidade regulatória, fornecendo um histórico de todas as atividades em seu AWS ambiente.

Para aplicativos web Transfer Family, você pode rastrear eventos de autenticação e operações de acesso a dados realizadas por seus usuários. Para habilitar o registro abrangente, você precisa:

1. Configure CloudTrail para registrar eventos de gerenciamento para rastrear atividades de autenticação.
2. Habilite eventos de dados do Amazon S3 para rastrear operações de arquivos realizadas por meio de seu aplicativo web.

Consulte também

- [CloudTrail casos de uso do IAM Identity Center](#)
- [Entendendo os eventos de login do IAM Identity Center](#)
- [CloudTrail Elemento UserIdentity](#)
- [Habilitando o registro de CloudTrail eventos para buckets e objetos do S3](#)
- [Eventos do Amazon S3 CloudTrail](#)

Habilitando eventos de dados do Amazon S3

Para rastrear operações de arquivos realizadas por meio dos aplicativos web da Transfer Family em seus buckets do Amazon S3, você precisa habilitar eventos de dados para esses buckets. Os eventos de dados fornecem atividade de API em nível de objeto e são particularmente úteis para rastrear uploads, downloads e outras operações de arquivos realizadas por usuários de aplicativos web.

Para habilitar eventos de dados do Amazon S3 para seu aplicativo web Transfer Family:

1. Abra o CloudTrail console em <https://console.aws.amazon.com/cloudtrail/>.
2. No painel de navegação, escolha Trilhas e, em seguida, selecione uma trilha existente ou crie uma nova.
3. Em Seletores de eventos avançados, escolha Editar.
4. Escolha Adicionar seletor de eventos avançado.
5. Para o primeiro seletor de campo:
 - Definir campo como `eventCategory`
 - Definir operador como igual
 - Defina o valor como `Data`
6. Escolha Adicionar campo e para o segundo seletor de campo:
 - Definir campo como `resources.type`
 - Definir operador como igual
 - Defina o valor como `AWS::S3::Object`
7. (Opcional) Para registrar eventos somente para buckets específicos, escolha Adicionar campo e adicione:
 - Definir campo como `resources.ARN`
 - Defina o operador para começar com
 - Defina o valor como `arn:aws:s3:::your-bucket-name/`
8. Escolha Salvar alterações.

Como alternativa, você pode usar a configuração de eventos de dados legados:

1. Em Eventos de dados, escolha Editar.
2. Em Tipo de evento de dados, selecione Eventos de bucket e objeto do S3.

3. Escolha os buckets do Amazon S3 para registrar eventos de dados. Você pode selecionar Todos os buckets atuais e futuros do S3 ou especificar buckets individuais.
4. Escolha se deseja registrar eventos de leitura, eventos de gravação ou ambos.
5. Escolha Salvar alterações.

Depois de habilitar os eventos de dados, você pode acessar esses logs no bucket do Amazon S3 configurado para CloudTrail. Os registros incluem detalhes como o usuário que realizou a ação, o registro de data e hora da ação, o objeto específico afetado e o `onBehalfOf` campo que ajuda a rastrear as ações realizadas `userId` por meio dos aplicativos web Transfer Family.

Encontrando e visualizando seus registros

Há várias maneiras de encontrar e visualizar CloudTrail registros do seu aplicativo web Transfer Family:

Usando o CloudTrail console

A maneira mais rápida de ver eventos recentes:

1. Abra o CloudTrail console em <https://console.aws.amazon.com/cloudtrail/>.
2. Escolha Histórico de eventos.
3. Filtrar eventos por:
 - Fonte do evento: `signin.amazonaws.com` para eventos de aplicativos da web
 - Fonte do evento: `s3.amazonaws.com` para operações de arquivo
4. Clique em qualquer evento para ver informações detalhadas.

Acessando registros no Amazon S3

Para acessar os arquivos de log completos armazenados no Amazon S3:

1. Identifique o CloudTrail bucket Amazon S3 da sua trilha:

```
aws cloudtrail describe-trails --query 'trailList[*].[Name,S3BucketName]' --output table
```

2. Navegue até os arquivos de log no Amazon S3:

```
aws s3 ls s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/
```

3. Baixe e pesquise arquivos de log para o ID do seu aplicativo web:

```
aws s3 cp s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/ . --recursive
gunzip *.json.gz
grep -l "webapp-1a2b3c4d5e6f7g8h9" *.json
```

Usando AWS CLI para pesquisar eventos

Pesquise eventos específicos de aplicativos da web usando AWS CLI:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "webapp-1a2b3c4d5e6f7g8h9" \
  --start-time $(date -d "1 day ago" +%s)000
```

Ou pesquise eventos de autenticação:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "UserAuthentication" \
  --start-time $(date -d "1 day ago" +%s)000
```

Exemplos de registros de autenticação

CloudTrail registra eventos de autenticação para aplicativos web Transfer Family, que podem ajudar você a monitorar tentativas de login bem-sucedidas e malsucedidas. Esses registros são particularmente úteis para fins de monitoramento de segurança e conformidade.

Tópicos

- [Exemplo de entrada de registro para verificação de credenciais](#)
- [Exemplo de entrada de registro para autenticação de login](#)
- [Exemplo de entrada de registro para ListCallerAccessGrants](#)
- [Exemplo de entrada de registro para GetDataAccess evento](#)

Exemplo de entrada de registro para verificação de credenciais

O exemplo a seguir mostra uma entrada de CloudTrail registro para um evento de verificação de credencial que ocorre durante o processo de autenticação.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "58138a11-87e5-401d-8f0b-7161c9389112"
  },
  "eventTime": "2025-08-08T15:29:30Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.224",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "f304a48b-7b6d-41c8-b136-4f49c91c1f31",
    "CredentialType": "PASSWORD"
  },
  "requestID": "ff936828-4a81-453c-802d-81368b6bca1a",
  "eventID": "70cb7008-493d-42c2-a9eb-38bf168af6a8",
  "readOnly": false,
  "eventType": "AWS ServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
    "CredentialVerification": "Success"
  },
}
```

```

    "eventCategory": "Management"
  }

```

Esse evento fornece detalhes adicionais sobre a etapa de verificação de credenciais no processo de autenticação, mostrando a ID específica da credencial e a ID do fluxo de trabalho de autenticação usadas.

Exemplo de entrada de registro para autenticação de login

O exemplo a seguir mostra uma entrada de CloudTrail registro de um evento de autenticação de usuário bem-sucedido durante o login do aplicativo web usando o IAM Identity Center.

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "b41f0a02-1635-4d07-a414-aecf9e14b906"
  },
  "eventTime": "2025-08-07T14:09:07Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.14",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "7a4ef12c-7c4b-4bc3-b5bd-c2469afcc795",
    "LoginTo": "https://example.awsapps.com/start/",
    "CredentialType": "PASSWORD"
  },
  "requestID": "fc91bcf0-ac53-4454-a1a0-fb911eacc095",

```

```
"eventID": "18522007-1e60-4a71-b2b5-150baf504ab3",
"readOnly": false,
"eventType": "AWS ServiceEvent",
"managementEvent": true,
"recipientAccountId": "123456789012",
"serviceEventDetails": {
  "UserAuthentication": "Success"
},
"eventCategory": "Management"
}
```

Neste exemplo, observe os seguintes campos importantes:

- `eventSource`: mostra “signin.amazonaws.com”, indicando que esse é um evento de autenticação do IAM Identity Center.
- `userIdentity.onBehalfOf`: contém o ID do usuário e o ARN do repositório de identidades do usuário do aplicativo web.
- `additionalEventData.LoginTo`: mostra o URL do aplicativo IAM Identity Center que está sendo acessado.
- `additionalEventData.CredentialType`: indica o método de autenticação usado (SENHA).
- `serviceEventDetails`: Mostra o resultado da autenticação (Sucesso).

Exemplo de entrada de registro para ListCallerAccessGrants

O exemplo a seguir mostra uma entrada de CloudTrail registro para um ListCallerAccessGrants evento, que ocorre quando o aplicativo web Transfer Family consulta as concessões de acesso disponíveis para um usuário.

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:aws-transfer",
    "arn": "arn:aws:sts::123456789012:assumed-role/AWS
TransferWebAppIdentityBearer-us-east-2/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
```

```

        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/service-role/AWS
TransferWebAppIdentityBearer-us-east-2",
        "accountId": "123456789012",
        "userName": "AWS TransferWebAppIdentityBearer-us-east-2"
    },
    "attributes": {
        "creationDate": "2025-08-08T15:29:34Z",
        "mfaAuthenticated": "false"
    }
},
"invokedBy": "transfer.amazonaws.com",
"onBehalfOf": {
    "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
    "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9a670c546e"
},
},
"eventTime": "2025-08-08T15:29:35Z",
"eventSource": "s3.amazonaws.com",
"eventName": "ListCallerAccessGrants",
"awsRegion": "us-east-2",
"sourceIPAddress": "transfer.amazonaws.com",
"userAgent": "transfer.amazonaws.com",
"requestParameters": {
    "Host": "123456789012.s3-control.dualstack.us-east-2.amazonaws.com",
    "allowedByApplication": "true",
    "maxResults": "100"
},
"responseElements": null,
"additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "bytesTransferredIn": 0,
    "AuthenticationMethod": "AuthHeader",
    "x-amz-id-2": "1g34AaAELn/
fntxwriFVsr41VDl8dp5ygWFasHJFNVq5FDCWYfX0ye7s4tWHEJC8ppI5lLePYLIcw3iTXAgn5Q==",
    "bytesTransferredOut": 462
},
"requestID": "48485MTZEDWT0ANT",
"eventID": "3de5dd60-b7cf-474c-a1ab-631467c1a5c3",
"readOnly": true,
"resources": [
    {

```

```

        "accountId": "123456789012",
        "type": "AWS:S3::AccessGrantsInstance",
        "ARN": "arn:aws:s3:us-east-2:123456789012:access-grants/default"
    }
],
"eventType": "AWS ApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}

```

Neste exemplo, observe os seguintes campos importantes:

- `eventName`: Mostra que se trata de um `ListCallerAccessGrants` evento que consulta as concessões de acesso disponíveis do S3.
- `requestParameters.allowedByApplication`: indica que a consulta está filtrada de acordo com as concessões permitidas pelo aplicativo.
- `requestParameters.maxResults`: mostra o número máximo de subsídios a serem devolvidos na resposta.
- `userIdentity.onBehalfOf`: vincula a solicitação ao usuário específico do aplicativo web.

Esse evento ajuda a monitorar quando o aplicativo web Transfer Family consulta a quais recursos do S3 um usuário tem acesso, fornecendo visibilidade das operações de descoberta de concessões de acesso.

Exemplo de entrada de registro para GetDataAccess evento

O exemplo a seguir mostra uma entrada de CloudTrail registro para um `GetDataAccess` evento, que ocorre quando o aplicativo web Transfer Family solicita permissões de acesso aos recursos do S3 em nome de um usuário.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROASEQRAEABP7ADWEZA5:aws-transfer",
    "arn": "arn:aws:sts::123456789012:assumed-role/AWSTransferWebAppIdentityBearer-
ap-southeast-1/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",

```

```

    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROASEQRAEABP7ADWEZA5",
        "arn": "arn:aws:iam::123456789012:role/service-role/
AWSTransferWebAppIdentityBearer-ap-southeast-1",
        "accountId": "123456789012",
        "userName": "AWSTransferWebAppIdentityBearer-ap-southeast-1"
      },
      "attributes": {
        "creationDate": "2025-05-08T16:09:05Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "transfer.amazonaws.com",
    "onBehalfOf": {
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9667b0da7a",
      "userId": "191a35ec-10a1-70c1-e4ab-e2802411e13e"
    }
  },
  "eventTime": "2025-05-08T16:10:25Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetDataAccess",
  "awsRegion": "ap-southeast-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "Host": "123456789012.s3-control.dualstack.ap-southeast-1.amazonaws.com",
    "durationSeconds": 900,
    "permission": "READWRITE",
    "target": "s3://amzn-s3-demo-bucket/users/john.doe/documents/*"
  },
  "responseElements": null,
  "additionalEventData": {
    "AuthenticationMethod": "AuthHeader",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "SignatureVersion": "SigV4",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2244,
    "x-amz-id-2": "8ce8sZ0gNwsaj9w1mzagyA
+cs0NjYl8FgEw4FGpE8DARi90aNc0RFwLTYNE7ChqE9RCJrTzMvS+ru7Vz2xXHrkQt/1uQ9exZTZdlhX+/fm="
  },
  "requestID": "BXGSKKQXCWS5RAHB",

```

```
{
  "eventID": "c11db1d1-dfb8-431e-8625-48eba2ebadfe",
  "readOnly": true,
  "resources": [
    {
      "type": "AWS:S3::AccessGrantsInstance",
      "ARN": "arn:aws:s3:ap-southeast-1:123456789012:access-grants/default",
      "accountId": "123456789012"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
}
```

Neste exemplo, observe os seguintes campos importantes:

- `eventName`: mostra que esse é um `GetDataAccess` evento que ocorre quando o Transfer Family solicita permissões de acesso aos recursos do S3.
- `userIdentity.onBehalfOf`: contém o ARN e o ID do usuário do repositório de identidades, vinculando a solicitação de acesso ao usuário específico do aplicativo web.
- `requestParameters.target`: mostra o padrão de caminho do S3 para o qual o acesso foi solicitado.
- `requestParameters.permission`: indica o tipo de acesso solicitado (READWRITE, READ ou WRITE).
- `requestParameters.durationSeconds`: mostra por quanto tempo a concessão de acesso é válida (normalmente 900 seconds/15 minutos).
- `sourceIPAdresseuserAgent`: Ambos mostram “transfer.amazonaws.com”, indicando que se trata de uma solicitação de serviço interna.

`GetDataAccess` os eventos são particularmente úteis para rastrear quando os usuários do aplicativo web Transfer Family recebem acesso a recursos específicos do S3, ajudando você a monitorar os padrões de acesso e garantir a autorização adequada.

Visualizando entradas CloudTrail de registro

Há várias maneiras de visualizar e analisar as entradas de CloudTrail registro do seu aplicativo web Transfer Family:

Usando o CloudTrail console

O CloudTrail console fornece uma interface fácil de usar para visualizar e filtrar entradas de registro:

1. Abra o CloudTrail console em <https://console.aws.amazon.com/cloudtrail/>.
2. No painel de navegação, escolha Event history (Histórico de eventos).
3. Use as opções de filtro para restringir os eventos:
 - Defina Origem do evento como `transfer.amazonaws.com` para ver somente os eventos do Transfer Family.
 - Filtre por nome do evento para ver operações específicas, como `UserAuthentication`.
 - Use o intervalo de tempo para se concentrar em eventos dentro de um período específico.
4. Clique em qualquer evento para ver suas informações detalhadas.

Acessando registros no Amazon S3

Se você configurou uma CloudTrail trilha para entregar registros para um bucket do Amazon S3, você pode acessar os arquivos de log brutos diretamente:

1. Abra o console do Amazon S3 em <https://console.aws.amazon.com/s3/>.
2. Navegue até o bucket e o prefixo em que seus CloudTrail registros estão armazenados.
3. Os registros são organizados por ano, mês, dia e região. Navegue até o diretório apropriado.
4. Baixe e abra os arquivos de log, que estão no formato JSON.

Solução de problemas em seus aplicativos da web

Note

Essas dicas de solução de problemas são destinadas ao administrador do aplicativo web e não ao usuário final. Para usuários finais, se você encontrar algum problema, entre em contato com o administrador do aplicativo web. Todas as instâncias de você nos parágrafos a seguir se referem ao administrador do aplicativo web.

Solucionar erros de rede

Descrição

Seu usuário final vê um banner de rede Network Error ao carregar o endpoint do aplicativo web.

Causa

Os problemas mais comuns são os seguintes:

- O administrador não atribuiu o usuário que está tentando fazer login no novo aplicativo.
- O administrador não adicionou as ações necessárias às suas funções do IAM.
- Você vê uma lista de concessões de acesso do S3 atribuídas ao seu usuário, mas o CORS não está configurado corretamente para seu bucket ou buckets do Amazon S3.

Solução

- No IAM Identity Center, certifique-se de atribuir o usuário ao aplicativo correto. Ou, se você tiver um grupo atribuído, verifique se o usuário que está tentando fazer login pertence ao grupo correto. Isso está descrito em [Atribuir ou adicionar usuários ou grupos a um aplicativo web Transfer Family](#).
- Verifique se suas funções contêm as ações necessárias na política de confiança personalizada para ambas `sts:AssumeRole` e `sts:SetContext` ações. Isso está descrito em [Configurar funções do IAM para aplicativos web Transfer Family](#).
- Verifique a política do CORS para todos os buckets usados pelo seu aplicativo web. Isso está descrito em [Configurar o compartilhamento Cross-origin de recursos \(CORS\) para seu bucket do Amazon S3](#).

Solucione o problema de que o bucket configurado não aparece

Descrição

Tudo parece estar configurado corretamente, mas o bucket do Amazon S3 não aparece no aplicativo web.

Causa

Uma possível causa é que o bucket do Amazon S3 não está na mesma conta do aplicativo web.

Solução

Certifique-se de que o bucket do Amazon S3 esteja na mesma conta do aplicativo web. Cross-accountNo momento, não há suporte para buckets.

Solucionar erros de URL personalizados

Descrição

Quando seu usuário final faz login no aplicativo web, ele recebe a mensagem de erro Falha na autorização: código de autorização ausente.

Causa

Se você usou CloudFront diretamente, em vez do CloudFormation modelo fornecido, provavelmente configurou incorretamente a política de solicitação de origem para não encaminhar cadeias de caracteres de consulta.

Solução

Atualize sua política de solicitação de origem para encaminhar sequências de caracteres de consulta e cookies para a origem.

Descrição

Quando seu usuário final tenta acessar um aplicativo web Transfer Family, ele recebe uma resposta 404.

Causa

Se você usou CloudFront diretamente, em vez do CloudFormation modelo fornecido, provavelmente configurou incorretamente a política de cache para incluir o Host cabeçalho na chave de cache ou configurou incorretamente a política de solicitação de origem para encaminhar o Host cabeçalho.

Solução

- Certifique-se de que sua política de cache não inclua o Host cabeçalho na chave de cache
- Certifique-se de que sua política de solicitação de origem não encaminhe o Host cabeçalho.

Solucionar erros diversos

Descrição

Seu usuário final não consegue fazer login, não consegue visualizar nenhum bucket ou arquivo, ou você recebe outro erro.

Causa

Uma causa possível é que o ARN da instância do IAM Identity Center não corresponda ao valor do ARN de suas concessões ou do ARN da instância do IAM Identity Center do seu aplicativo web.

Solução

Verifique os itens a seguir para ver se eles coincidem.

- No IAM Identity Center, navegue até Configurações e visualize o ARN da instância.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

- No Amazon S3, navegue até Access Grants e visualize o ARN da instância do IAM Identity Center.

```
arn:aws:sso:::account-id:application/ssoins-instance-identifier/ap1-1234567890abcdef0
```

- Em Transfer Family, navegue até a página de detalhes do seu aplicativo web e veja o ARN da instância.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

O *instance-identifier* valor deve ser o mesmo em todos esses três lugares.

Buckets S3 duplicados que aparecem no aplicativo web

Descrição

Os usuários veem o mesmo bucket do S3 listado várias vezes na interface do aplicativo web Transfer Family.

Causa

Isso ocorre quando um usuário faz parte de vários grupos do Active Directory que têm concessões duplicadas para o mesmo bucket do S3. O aplicativo web lista todas as concessões de nível superior associadas ao usuário (UID ou GID), independentemente de o usuário ter várias concessões atribuídas ao mesmo local do bucket.

Solução

Para resolver esse problema, os administradores devem eliminar a duplicação das concessões para que cada usuário tenha apenas uma concessão para cada local do S3. Revise sua configuração do S3 Access Grants e consolide concessões duplicadas para o mesmo bucket em diferentes grupos do Active Directory.

Instruções para o usuário final dos aplicativos web Transfer Family

Note

Neste tópico, as informações são destinadas aos usuários finais que estão interagindo com o aplicativo web. Todas as suas instâncias neste tópico se referem a usuários finais.

Este tópico descreve como acessar um aplicativo AWS Transfer Family web que você está autorizado a usar e descreve como você pode interagir com ele.

Cotas de aplicativos web

Observe as seguintes limitações ao usar aplicativos da web.

- Número máximo de resultados de pesquisa por consulta: 10.000
- Os buckets do Amazon S3 usados pelo aplicativo web Transfer Family devem estar na mesma conta do próprio aplicativo web. Cross-account No momento, não há suporte para buckets.
- Amplitude máxima de pesquisa por consulta: 10.000 arquivos pesquisados
- Tamanho máximo de upload por arquivo: 160 GB (149 GiB)
- Tamanho máximo do arquivo para cópia: 5,36 GB (5 GiB)
- Não há suporte para nomes de pastas que comecem ou terminem com pontos (.)

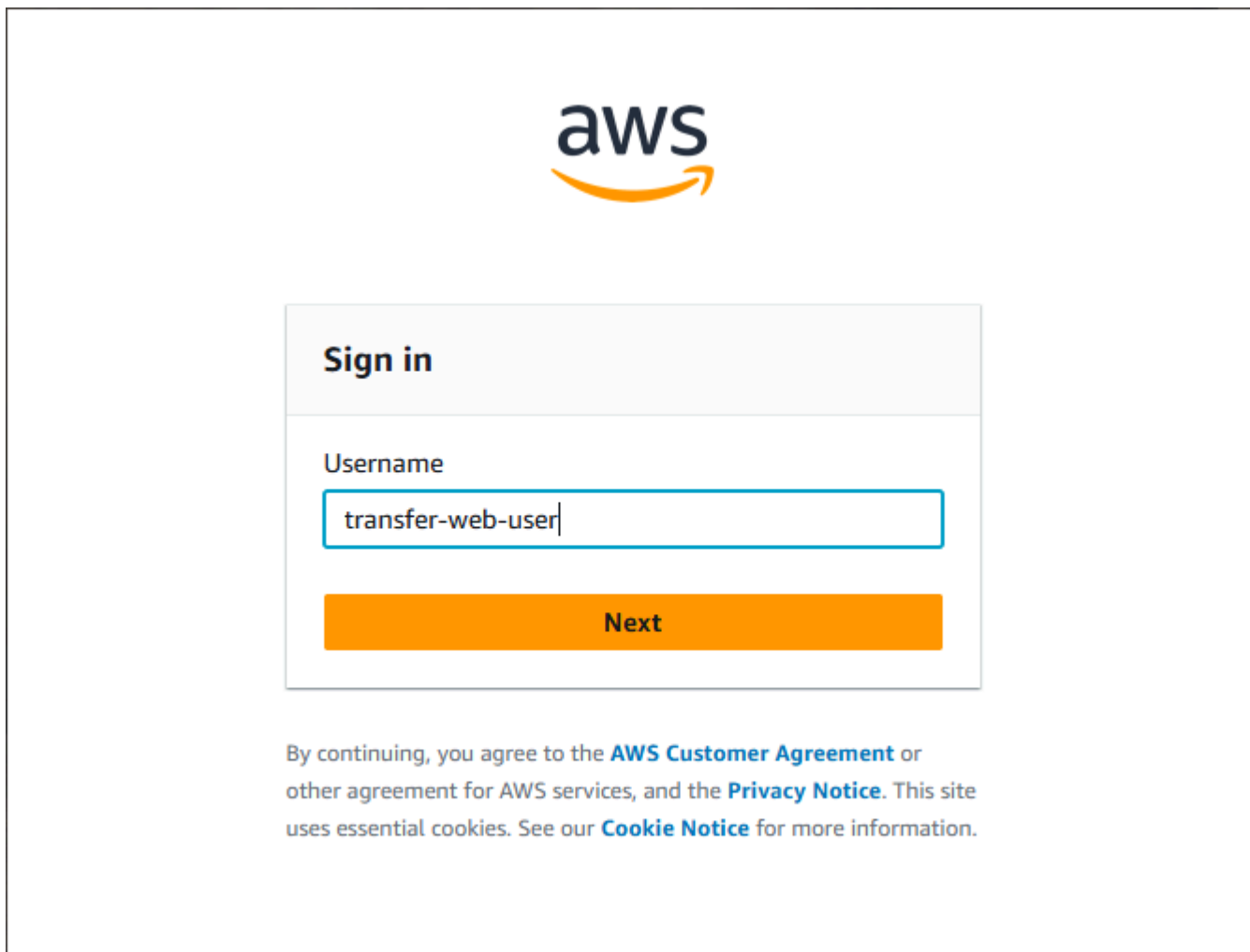
Experiência do usuário para usuários do IAM Identity Center

Esta seção descreve a experiência do usuário se sua organização usou o IAM Identity Center para configurar seus usuários.

Para acessar um aplicativo web Transfer Family

1. Você deve receber um e-mail de `no-reply@login.awsapps.com` com o título “Convite para participar” Centro de Identidade do AWS IAM. Aceite o convite para ativar sua conta de usuário.
2. Na mensagem, escolha a URL abaixo da URL do seu portal de AWS acesso.

Isso leva você para a tela de AWS login.



aws

Sign in

Username

transfer-web-user

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

3. Insira suas credenciais e escolha Entrar.

Isso leva você ao Portal de acesso da AWS, que mostra uma lista dos aplicativos disponíveis.

4. Escolha o aplicativo para seu aplicativo web Transfer Family.

Experiência do usuário para usuários de provedores de identidade terceirizados

Se sua organização não usou Centro de Identidade do AWS IAM para configurar seus usuários, sua experiência de integração dependerá do aplicativo do provedor de identidade que eles usaram para configurar seus usuários finais. Depois de se autenticar e fazer login, a interface do seu aplicativo web é a mesma descrita na próxima seção.

Note

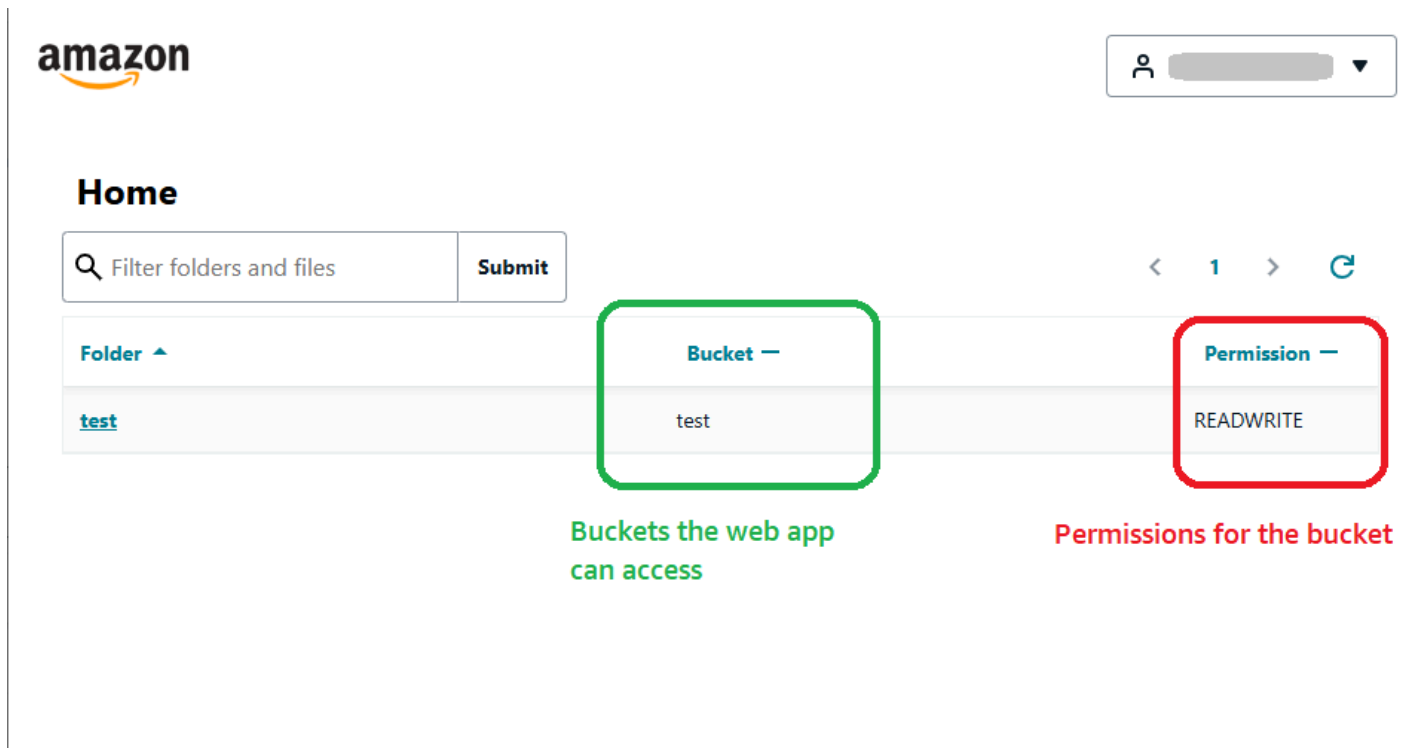
Se um usuário pertencer a vários grupos do Active Directory que têm concessões para o mesmo bucket do Amazon S3, o bucket aparece várias vezes na interface do aplicativo web. Isso ocorre porque o aplicativo web lista todas as concessões de nível superior associadas ao UID ou GID do usuário, incluindo concessões duplicadas para o mesmo bucket. Para evitar listagens duplicadas, os administradores podem consolidar várias concessões para que cada usuário tenha apenas uma concessão por local do Amazon S3.

Interface de usuário final do Transfer Family

Depois de se autenticar e fazer login, você pode interagir com o aplicativo web.

Há quatro vistas principais.

- **Página inicial:** sua página inicial lista os locais do S3, que você pode acessar, bem como as permissões para cada um. Um local do S3 é um bucket ou prefixo do S3, que você pode definir ao usar as concessões de acesso do S3. Essa é a visualização inicial para usuários que mostra os recursos do S3 de nível raiz aos quais seus usuários finais têm acesso e as permissões para cada local do S3.



- Detalhes do local: essa exibição permite que os usuários naveguem por arquivos e pastas no S3 e carreguem ou baixem arquivos.
- Ação de localização: depois de escolher uma ação (como Carregar), ela abre outra visualização da localização do arquivo.
- Elipse vertical: O ícone de reticências verticais abre o menu Ações.

Ações disponíveis

A maioria das ações está disponível no menu Ações. Para a outra ação principal, baixar arquivos, você usa o ícone de download depois de selecionar um arquivo (atualmente, você só pode baixar um arquivo por vez).

Transfer Web App

Scott

Home / test2 / Testing-01

Testing-01/

☐ Include subfolders

< 1 > ↺ ⋮

☐	Name ▲	Type —	Last Modified —	Size —	
☐	 scott-small.png	png	10/30/2024, 2:28:31 PM	375.4 kB	
☐	 Scott-02.jpg	jpg	10/30/2024, 2:28:30 PM	196.6 kB	
☐	 Scott-badge.jpg	jpg	10/30/2024, 2:28:31 PM	1.3 MB	

Download icon

Em uma pasta, use o menu Ações para realizar qualquer uma das seguintes tarefas:

- Copie um ou mais arquivos para outro local.
- Crie uma pasta.
- Exclua um ou mais arquivos.
- Faça upload de um ou mais arquivos.
- Faça upload de uma pasta inteira (incluindo subpastas, se houver).
- Selecione uma pasta e navegue até ela. Em seguida, você pode executar qualquer uma das ações listadas anteriormente.
- Classifique por página.
- Filtre por nome de arquivo ou pasta por pasta e subpastas.

amazon

Home / test

test

Q

Search current folder

Submit

☐ Include subfolders

<

1

>

Name ▲	Type —	Last Modified —
My First Folder/	Folder	
My Second Folder/	Folder	
Testing-01/	Folder	
Testing-02/	Folder	

Copy files

Create folder

Delete files

Upload files

Upload folder

AWS Transfer Family Conectores SFTP

Um conector AWS Transfer Family SFTP estabelece uma conexão com um servidor SFTP remoto para transferir arquivos entre o armazenamento da Amazon e um servidor remoto, usando o protocolo SFTP. Você pode enviar arquivos do Amazon S3 para um servidor SFTP externo de propriedade do parceiro, recuperar arquivos do servidor SFTP de um parceiro para o Amazon S3 ou listar, excluir, renomear ou mover arquivos no servidor remoto. Os conectores SFTP oferecem suporte a dois tipos de saída: serviço gerenciado (usando infraestrutura AWS gerenciada) e VPC (roteamento pela sua VPC usando o Amazon VPC Lattice). Usando conectores SFTP, você pode criar fluxos de trabalho de transferência de arquivos automatizados e orientados por eventos no AWS.

Veja os [conectores SFTP do AWS Transfer Family](#) para uma breve introdução aos conectores SFTP do Transfer Family.

Tópicos

- [Criação de conectores SFTP](#)
- [Conectividade VPC para conectores SFTP](#)
- [Usando conectores SFTP](#)
- [Monitorando conectores SFTP](#)
- [Gerenciando conectores SFTP](#)
- [Dimensionamento e cotas para conectores SFTP](#)
- [Arquiteturas de referência usando conectores SFTP](#)

Criação de conectores SFTP

Este tópico descreve como criar conectores SFTP. Cada conector oferece a capacidade de se conectar a um servidor SFTP remoto. Você executa as seguintes tarefas de alto nível para configurar um conector SFTP.

Note

Para VPC-based conectores que roteiam o tráfego por meio de sua nuvem privada virtual, consulte [Crie um conector SFTP com saída VPC-based](#).

1. Armazene as credenciais de autenticação do conector em AWS Secrets Manager.
2. Crie o conector especificando o ARN secreto, a URL do servidor remoto ou o ARN de configuração de recursos, a política de segurança contendo os algoritmos que serão suportados pelo conector e outras definições de configuração.
3. Depois de criar o conector, você pode testá-lo para garantir que ele possa estabelecer conexões com o servidor SFTP remoto.

Escolhendo o tipo de saída do conector SFTP

Ao criar um conector SFTP, você escolhe o tipo de saída entre “Serviço gerenciado” e “VPC Lattice”.

- Serviço gerenciado (padrão): o conector usa gateways NAT e endereços IP de propriedade da AWS Transfer Family para rotear conexões pela Internet pública. O serviço fornece três endereços IP estáticos para seus conectores que precisam estar na lista de permissões nos servidores remotos para estabelecer conexões.
- VPC Lattice: o conector roteia o tráfego pelo seu ambiente VPC usando o Amazon VPC Lattice. Use a conectividade VPC para conectores SFTP nesses cenários:
 - Servidores SFTP privados: conecte-se a servidores SFTP que só podem ser acessados pela sua VPC
 - On-premises conectividade: conecte-se a servidores SFTP locais por meio AWS Direct Connect de conexões AWS Virtual Private Network
 - Endereços IP personalizados: apresente seus próprios gateways NAT e endereços IP elásticos ao servidor remoto
 - Controles de segurança centralizados: direcione as transferências de arquivos pelos controles centrais ingress/egress da sua organização

A matriz a seguir ajuda você a escolher o tipo de conector certo para seus casos de uso.

Matriz do tipo de saída do conector SFTP

Recurso	Tipo de saída = Serviço gerenciado	Tipo de saída = VPC Lattice
Conectividade com servidores SFTP hospedados publicamente (acessíveis pela Internet)	Compatível	Suportado ¹

Recurso	Tipo de saída = Serviço gerenciado	Tipo de saída = VPC Lattice
Conectividade com servidores SFTP hospedados de forma privada (no local)	Não compatível	Suportado ²
Conectividade com servidores SFTP hospedados de forma privada (em VPC)	Não compatível	Compatível
Endereços IP estáticos apresentados ao servidor SFTP remoto	Compatível por meio de endereços IP estáticos fornecidos pelo serviço	Compatível por meio de endereços IP estáticos de propriedade do cliente
Largura de banda disponível	50 MBPS por conta	Maior largura de banda, conforme disponível no Resource Gateway e no NAT Gateway de propriedade do cliente
Roteamento de tráfego para a Internet por meio de gateways NAT e firewalls de rede de propriedade do cliente	Sem compatibilidade. Os gateways NAT são de propriedade e gerenciados pelo serviço Transfer Family.	Compatível

¹ Com Tipo de saída = VPC Lattice, a conectividade com servidores hospedados publicamente é suportada usando a configuração da infraestrutura de saída (NAT Gateways) em suas VPCs de saída.

² Com o tipo de saída = VPC Lattice, a conectividade com servidores hospedados de forma privada é suportada usando redes existentes em sua VPC, como VPN. AWS Direct Connect

Escolhendo o modo de endereçamento IP

Ao criar um conector SFTP com saída gerenciada pelo serviço, você pode escolher entre dois modos de endereçamento IP:

- **Somente IPv4 (padrão):** o conector usa endereços IPv4 exclusivamente para se conectar ao servidor SFTP remoto. Esse é o modo padrão ao criar conectores por meio do console, da AWS CLI ou da API.
- **Dual-stack:** O conector suporta endereços IPv6 e IPv4. No modo de pilha dupla, o conector prefere IPv6 quando a resolução DNS retorna resultados IPv6 e usa IPv4 quando somente resultados de DNS IPv4 são retornados.

Note

O modo de endereçamento IP se aplica somente aos conectores com tipo de saída gerenciado pelo serviço. Os conectores que usam a saída VPC Lattice não oferecem suporte a essa configuração.

Tópicos

- [Armazene credenciais de autenticação para conectores SFTP no Secrets Manager](#)
- [Crie um conector SFTP com saída gerenciada por serviços](#)
- [Crie um conector SFTP com saída VPC-based](#)
- [Testar um conector SFTP](#)

Armazene credenciais de autenticação para conectores SFTP no Secrets Manager

É possível usar o Secrets Manager para armazenar as credenciais do usuário para seus conectores SFTP. Ao criar seu segredo, forneça um nome de usuário. Além disso, é possível fornecer uma senha, uma chave privada ou ambas. Para obter detalhes, consulte [Cotas da para conectores SFTP](#).

Note

Quando você armazena segredos no Secrets Manager, você Conta da AWS incorre em cobranças. Para obter mais informações sobre preços consulte [AWS Secrets Manager Pricing](#).

É possível usar o Secrets Manager para armazenar as credenciais do usuário para um conector SFTP.

1. Faça login no Console de gerenciamento da AWS e abra o AWS Secrets Manager console em <https://console.aws.amazon.com/secretsmanager/>.
2. No painel de navegação à esquerda, selecione Segredos.
3. Na página Segredos, escolha Armazenar um novo segredo.
4. Na página Escolher tipo de segredo, em Tipo de segredo, escolha Outro tipo de segredo.
5. Forneça as key/value informações do seu segredo: você precisa fornecer o nome de usuário e uma chave privada ou uma senha.
 - a. Na seção Key/value de pares, escolha a Key/valueguia.
 - Chave — Insira **Username**.
 - valor — insira o nome do usuário autorizado a se conectar ao servidor do parceiro.
 - b. Se você quiser fornecer um par de chaves, escolha Adicionar linha e, na seção de Key/value pares, escolha a Key/valueguia.
 - Chave — Insira **PrivateKey**.
 - valor — cole sua chave privada.

Dica: Os dados da chave privada inseridos devem corresponder à chave pública armazenada para esse usuário no servidor SFTP remoto.

 Note

Não é possível usar uma chave privada protegida por senha para autenticação com um conector SFTP. AWS Transfer Family

Para obter detalhes sobre como gerar um public/private key pair, consulte [Criação de chaves SSH no macOS, Linux ou Unix](#).

- c. Se você quiser fornecer uma senha, escolha Adicionar linha e, na seção de Key/value pares, escolha a Key/valueguia.
 - Chave — Insira **Password**.

- valor – Insira uma senha para o usuário.
6. Escolha Próximo.
 7. Na página Configurar segredo, insira um nome e uma descrição para seu segredo. Recomendamos utilizar o prefixo **aws/transfer/** para o nome. Por exemplo, é possível dar ao seu segredo o nome de **aws/transfer/connector-1**.
 8. Escolha Próximo e aceite os padrões na página Configurar alternância. Em seguida, escolha Próximo.
 9. Na página Revisão, escolha Armazenar para criar e armazenar o segredo.

Crie um conector SFTP com saída gerenciada por serviços

Este procedimento explica como criar conectores SFTP usando o AWS Transfer Family console ou AWS CLI

Console

Para criar um conector SFTP

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, escolha Conectores SFTP e, em seguida, escolha Criar conector SFTP.
3. Na seção Configuração do conector, em Tipo de saída, escolha Serviço gerenciado. Essa opção usa infraestrutura de saída AWS Transfer Family gerenciada. O serviço Transfer Family fornece e gerencia endereços IP estáticos para cada conector SFTP.
4. Na seção Configuração do conector, forneça as seguintes informações:

Connector configuration

Egress type [Info](#)
Choose your SFTP connector's egress type: either directly over public internet, or via your VPC environment

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

URL
Enter the URL of remote server to which you need to connect using the SFTP connector

`sftp://sftp.example.com`

URL of the remote (target) SFTP server

Access role [Info](#)
IAM Role for Amazon S3 access and AWS Secrets Manager access

Choose an IAM role

Logging role - optional [Info](#)
IAM role for the connector to push events to your CloudWatch logs

Choose a logging role

- Para URL, insira o URL de um servidor SFTP remoto. Esse URL deve ser formatado como `sftp://partner-SFTP-server-url`, por exemplo, `sftp://AnyCompany.com`.

Note

Como opção, é possível fornecer um número de porta no seu URL. O formato é `sftp://partner-SFTP-server-url:port-number`. O número da porta padrão (quando nenhuma porta é especificada) é a porta 22.

- Para a função Access, escolha o Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) a ser usada.
- Assegure que esta função forneça acesso de leitura e gravação ao diretório principal do local do arquivo usado na solicitação do `StartFileTransfer`.
- Essa função deve dar permissão para `secretsmanager:GetSecretValue` para acessar o segredo.

Note

Na política, você deve especificar o ARN para o segredo. O ARN contém o nome secreto, mas acrescenta ao nome seis caracteres alfanuméricos aleatórios. Um ARN para um segredo tem o seguinte formato.


```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Certifique-se de que essa função contenha uma relação de confiança que permite que o conector acesse os recursos quando estiver atendendo às solicitações de transferência dos seus usuários. Para obter informações sobre como estabelecer um relacionamento de confiança, consulte [Estabelecer um relacionamento de confiança](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
  }
]
}

```

 Note

Para a função de acesso, o exemplo concede acesso a um único segredo. Porém, é possível usar um caractere curinga, que pode poupar trabalho se você quiser reutilizar o mesmo perfil do IAM para vários usuários e segredos. Por exemplo, a declaração de recurso a seguir concede permissões para todos os segredos que têm nomes começando com `aws/transfer`.

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

Você também pode armazenar segredos contendo suas credenciais de SFTP em outra Conta da AWS. Para obter detalhes sobre como habilitar o acesso secreto entre contas, consulte [Permissões a AWS Secrets Manager segredos para usuários em uma conta diferente](#).

5. Conclua a configuração do conector:

- (Opcional) Para a função Logging, escolha a função do IAM que o conector usará para enviar eventos aos seus CloudWatch registros. O exemplo de política a seguir lista as permissões necessárias para registrar eventos para conectores SFTP.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ]
    }
  ]
}

```

```

    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
  }
]
}

```

6. No painel Configuração do SFTP, forneça as seguintes informações:

SFTP configuration [Info](#)

Connector credentials [Info](#)
Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server

aws/transfer/sftp-connector1 [Store a new secret](#)

Trusted host keys - optional [Info](#)
Enter the public portion of the host key(s) that is used to identify the remote server you need to connect to. You can enter the trusted host key(s) now, or add them after creating the connector by using the host key information returned by the TestConnection action.

Connections to the remote server are established only if it's SSH fingerprint matches one of the provided trusted host key(s).

ssh-rsa AAAA... [Remove](#)

[Add trusted host key](#)

Maximum concurrent connections [Info](#)
Select the maximum number of concurrent connections that your connector can create to the remote server

5

- Para credenciais do Connector, na lista suspensa, escolha o nome de um segredo AWS Secrets Manager que contenha a chave privada ou a senha do usuário do SFTP. Você precisa criar um segredo e armazená-lo de uma maneira específica. Para obter detalhes, consulte [Armazene credenciais de autenticação para conectores SFTP no Secrets Manager](#).
- (Opcional) Você tem a opção de criar seu conector deixando o TrustedHostKeys parâmetro vazio. No entanto, seu conector não poderá transferir arquivos com o servidor remoto até que você forneça esse parâmetro na configuração do conector. Você pode inserir as chaves de host confiáveis no momento da criação do conector ou atualizá-lo posteriormente usando as informações da chave do host retornadas pela ação do TestConnection console ou pelo comando da API. Ou seja, para a caixa de texto Chaves de host confiáveis, você pode fazer o seguinte:
 - Forneça a (s) chave (s) de host confiável (s) no momento da criação do conector. Cole a parte pública da chave do host usada para identificar o servidor externo. É possível adicionar mais de uma chave escolhendo Adicionar chave de host confiável

para adicionar uma chave adicional. Você pode usar o comando `ssh-keyscan` no servidor SFTP para recuperar a chave necessária. Para obter detalhes sobre o formato e o tipo de chaves de host confiáveis compatíveis com o Transfer Family, consulte [SFTPConnectorConfig](#).

- Deixe a caixa de texto Trusted Host Key (s) vazia ao criar seu conector e atualize-o posteriormente com essas informações. Se você não tiver as informações da chave do host no momento da criação do conector, deixe esse parâmetro vazio por enquanto e continue com a criação do conector. Depois que o conector for criado, use o ID do novo conector para executar o `TestConnection` comando, na página de detalhes do conector AWS CLI ou na página de detalhes do conector. Se for bem-sucedido, `TestConnection` retornará as informações necessárias da chave do host. Em seguida, você pode editar seu conector usando o console (ou executando o `UpdateConnector` AWS CLI comando) e adicionar as informações da chave do host que foram retornadas quando você executou `TestConnection`.

 Important

Se você recuperar a chave do host do servidor remoto executando `TestConnection`, certifique-se de realizar a validação fora de banda na chave retornada.

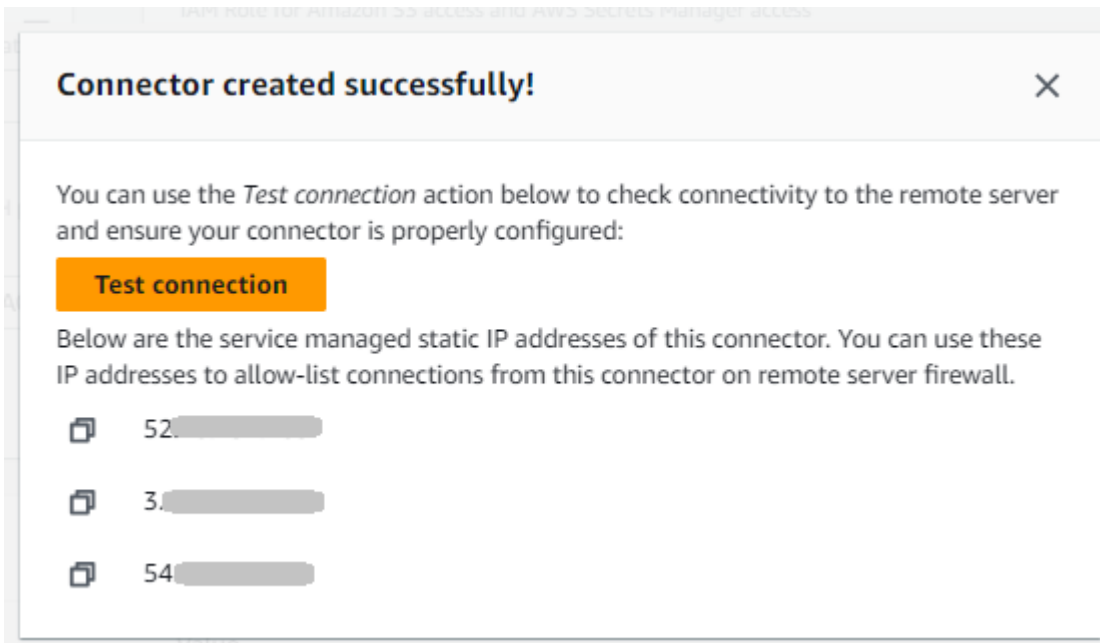
Você deve aceitar a nova chave como confiável ou verificar a impressão digital apresentada com uma impressão digital conhecida anteriormente que você recebeu do proprietário do servidor SFTP remoto ao qual está se conectando.

- (Opcional) Para Máximo de conexões simultâneas, na lista suspensa, escolha o número de conexões simultâneas que seu conector cria com o servidor remoto. A seleção padrão no console é 5.

Essa configuração especifica o número de conexões ativas que seu conector pode estabelecer com o servidor remoto ao mesmo tempo. A criação de conexões simultâneas pode melhorar o desempenho do conector ao permitir operações paralelas.

7. Na seção Opções de algoritmo criptográfico, escolha uma política de segurança na lista suspensa no campo Política de segurança. A política de segurança permite que você selecione os algoritmos criptográficos que seu conector suporta. Para obter detalhes sobre as políticas e algoritmos de segurança disponíveis, consulte [Políticas de segurança para AWS Transfer Family Conectores SFTP](#).

8. (Opcional) Na seção Tags para Chave e Valor, insira uma ou mais tags como pares de chave/valor.
9. Depois de confirmar todas as configurações, escolha Criar conector SFTP para criar o conector SFTP. Se o conector for criado com sucesso, uma tela será exibida com uma lista dos endereços IP estáticos atribuídos e um botão Testar conexão. Use o botão para testar a configuração do seu novo conector.



A página Conectores é exibida, com o ID do seu novo conector SFTP adicionado à lista. Para visualizar os detalhes de seus conectores, consulte [Exibir detalhes do conector SFTP](#).

CLI

Você usa o comando [create-connector](#) para criar um conector. Para usar esse comando para criar um conector SFTP, forneça as seguintes informações.

- O URL de um servidor SFTP remoto. Esse URL deve ser formatado como `sftp://partner-SFTP-server-url`, por exemplo, `sftp://AnyCompany.com`
- A função de acesso. O nome do recurso da Amazon (ARN) do perfil do (IAM) AWS Identity and Access Management a ser usado.
 - Assegure que esta função forneça acesso de leitura e gravação ao diretório principal do local do arquivo usado na solicitação do `StartFileTransfer`.
 - Essa função deve dar permissão para `secretsmanager:GetSecretValue` para acessar o segredo.

Note

Na política, você deve especificar o ARN para o segredo. O ARN contém o nome secreto, mas acrescenta ao nome seis caracteres alfanuméricos aleatórios. Um ARN para um segredo tem o seguinte formato.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Certifique-se de que essa função contenha uma relação de confiança que permite que o conector acesse os recursos quando estiver atendendo às solicitações de transferência dos seus usuários. Para obter informações sobre como estabelecer um relacionamento de confiança, consulte [Estabelecer um relacionamento de confiança](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ]
    }
  ]
}
```

```

    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
  },
  {
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
  }
]
}

```

Note

Para a função de acesso, o exemplo concede acesso a um único segredo. Porém, é possível usar um caractere curinga, que pode poupar trabalho se você quiser reutilizar o mesmo perfil do IAM para vários usuários e segredos. Por exemplo, a declaração de recurso a seguir concede permissões para todos os segredos que têm nomes começando com `aws/transfer`.

```

"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"

```

Você também pode armazenar segredos contendo suas credenciais de SFTP em outra Conta da AWS. Para obter detalhes sobre como habilitar o acesso secreto entre contas, consulte [Permissões a AWS Secrets Manager segredos para usuários em uma conta diferente](#).

- (Opcional) Escolha a função do IAM que o conector usará para enviar eventos aos seus CloudWatch registros. O exemplo de política a seguir lista as permissões necessárias para registrar eventos para conectores SFTP.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",

```

```

        "Action": [
            "logs:CreateLogStream",
            "logs:DescribeLogStreams",
            "logs:CreateLogGroup",
            "logs:PutLogEvents"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
}

```

- Forneça as seguintes informações de configuração do SFTP.
 - O ARN de um segredo AWS Secrets Manager que contém a chave privada ou a senha do usuário do SFTP.
 - A parte pública da chave do host que é usada para identificar o servidor externo. É possível fornecer várias chaves de host confiáveis, se quiser.

A maneira mais fácil de fornecer as informações do SFTP é salvá-las em um arquivo. Por exemplo, copie o texto de exemplo a seguir em um arquivo chamado `testSFTPConfig.json`.

```

// Listing for testSFTPConfig.json
{
    "UserSecretId": "arn:aws::secretsmanager:us-east-2:123456789012:secret:aws/transfer/example-username-key",
    "TrustedHostKeys": [
        "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
    ]
}

```

- Especifique uma política de segurança para seu conector, inserindo o nome da política de segurança.

Note

SecretId pode ser o ARN inteiro ou o nome do segredo (*example-username-key* na lista anterior).

Em seguida, execute o comando a seguir para criar o conector:


```
aws transfer create-connector --url "sftp://partner-SFTP-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/
AWSTransferLoggingAccess \
--sftp-config file:///path/to/testSFTPConfig.json \
--security-policy-name security-policy-name \
--maximum-concurrent-connections integer-from-1-to-5
```

Quando você descreve um conector do tipo de saída VPC, a resposta inclui os novos campos:

```
{
  "Connector": {
    "AccessRole": "arn:aws:iam::123456789012:role/connector-role",
    "Arn": "arn:aws:transfer:us-east-1:123456789012:connector/c-1234567890abcdef0",
    "ConnectorId": "c-1234567890abcdef0",
    "Status": "ACTIVE",
    "EgressConfig": {
      "VpcLattice": {
        "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-12345678",
        "PortNumber": 22
      }
    },
    "EgressType": "VPC",
    "ServiceManagedEgressIpAddresses": null,
    "SftpConfig": {
      "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
      "UserSecretId": "aws/transfer/connector-secret"
    },
    "Url": "sftp://my.sftp.server.com:22"
  }
}
```

Observe que isso `ServiceManagedEgressIpAddresses` é nulo para conectores do tipo de saída de VPC, pois o tráfego é roteado por sua VPC em vez da infraestrutura gerenciada. AWS

Crie um conector SFTP com saída VPC-based

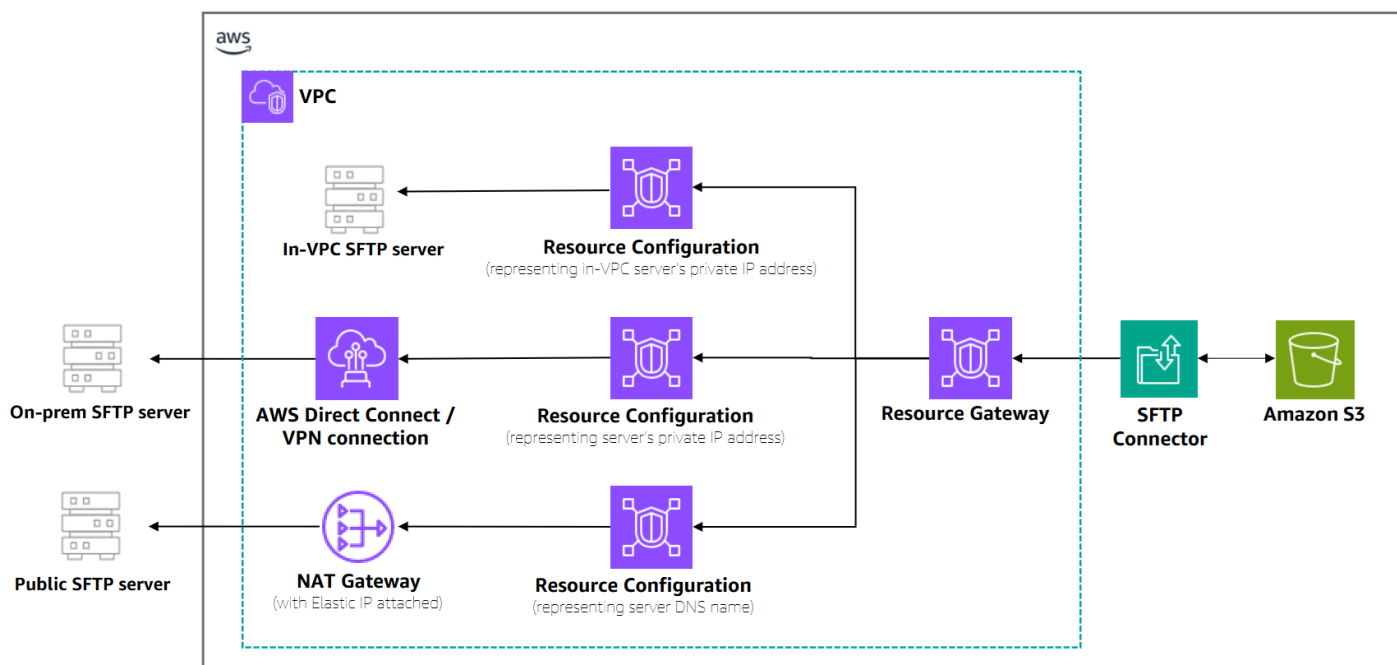
Este tópico fornece instruções passo a passo para criar conectores SFTP com conectividade VPC. Os LATTICE-enabled conectores VPC_ usam o Amazon VPC Lattice para rotear o tráfego por meio

de sua nuvem privada virtual, permitindo conexões seguras com endpoints privados ou usando seus próprios gateways NAT para acesso à Internet.

Quando usar a conectividade VPC

Use a conectividade VPC para conectores SFTP nesses cenários:

- Servidores SFTP privados: conecte-se a servidores SFTP que só podem ser acessados pela sua VPC.
- On-premises conectividade: conecte-se a servidores SFTP locais por meio de conexões AWS Direct Connect ou AWS Site-to-Site VPN.
- Endereços IP personalizados: use seus próprios gateways NAT e endereços IP elásticos, incluindo cenários de BYOIP.
- Controles de segurança centralizados: encaminhe as transferências de arquivos pelos ingress/egress controles centrais da sua organização.



Pré-requisitos para conectores VPC_ SFTP LATTICE-enabled

Antes de criar um conector VPC_ LATTICE-enabled SFTP, você deve preencher os seguintes pré-requisitos:

Como a VPC-based conectividade funciona

O VPC Lattice permite que você compartilhe com segurança os recursos do VPC com outros serviços. AWS Transfer Family usa uma rede de serviços para simplificar o processo de compartilhamento de recursos. Os principais componentes são:

- **Resource Gateway:** serve como ponto de acesso à sua VPC. Você cria isso em sua VPC com no mínimo duas zonas de disponibilidade.
- **Configuração de recursos:** contém o endereço IP privado ou o nome DNS público do servidor SFTP ao qual você deseja se conectar.

Quando você cria um LATTICE-enabled conector VPC_, AWS Transfer Family usa o Forward Access Session (FAS) para obter temporariamente suas credenciais e associar sua configuração de recursos à nossa rede de serviços.

Etapas de configuração necessárias

1. **Infraestrutura de VPC:** certifique-se de ter uma VPC configurada adequadamente com as sub-redes, tabelas de rotas e grupos de segurança necessários para os requisitos de conectividade do servidor SFTP.
2. **Resource Gateway:** crie um Resource Gateway em sua VPC usando o comando VPC Lattice. `create-resource-gateway` O Resource Gateway deve estar associado a sub-redes em pelo menos duas zonas de disponibilidade. Para obter mais informações, consulte [Resource gateways no Guia](#) do usuário do Amazon VPC Lattice.
3. **Configuração de recursos:** crie uma configuração de recursos que represente o servidor SFTP de destino usando o comando VPC `create-resource-configuration` Lattice. Você pode especificar:
 - Um endereço IP privado para endpoints privados
 - Um nome DNS público para endpoints públicos (endereços IP não são compatíveis com endpoints públicos)
4. **Credenciais de autenticação:** armazene as credenciais do usuário do SFTP AWS Secrets Manager conforme descrito em. [Armazene credenciais de autenticação para conectores SFTP no Secrets Manager](#)

 Important

O gateway de recursos e a configuração de recursos devem ser criados na mesma AWS conta. Ao criar uma configuração de recursos, você deve primeiro ter um gateway de recursos instalado.

Para obter mais informações sobre configurações de recursos de VPC, consulte [Configurações de recursos no Guia do usuário](#) do Amazon VPC Lattice.

 Note

A conectividade VPC para conectores SFTP está disponível onde os recursos do Regiões da AWS Amazon VPC Lattice estão disponíveis. Para obter mais informações, consulte Perguntas frequentes sobre o [VPC Lattice](#). O suporte à zona de disponibilidade varia de acordo com a região, e os gateways de recursos exigem no mínimo duas zonas de disponibilidade.

Crie um conector VPC_ LATTICE-enabled SFTP

Depois de concluir os pré-requisitos, você pode criar um conector SFTP com conectividade VPC usando o AWS CLI Management Console ou SDKs. AWS AWS

Console

Para criar um conector VPC_ LATTICE-enabled SFTP

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, escolha Conectores SFTP e, em seguida, escolha Criar conector SFTP.
3. Na seção Configuração do conector, em Tipo de saída, escolha VPC Lattice.

Essa opção roteia o tráfego pela sua VPC usando o Amazon VPC Lattice para acesso a recursos entre VPCs. Você pode usar essa opção para se conectar a endpoints de servidores hospedados de forma privada, rotear o tráfego por meio dos controles de segurança da sua VPC ou usar seus próprios gateways NAT e endereços IP elásticos. O endereço do servidor SFTP remoto é representado como uma configuração de recursos

em sua VPC. Para obter mais informações sobre configurações de recursos, consulte [Configurações de recursos para recursos de VPC no Guia do usuário do Amazon VPC Lattice](#).

4. Conclua a configuração do conector:

- Para a função Access, escolha o Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) a ser usada.
- Assegure que esta função forneça acesso de leitura e gravação ao diretório principal do local do arquivo usado na solicitação do `StartFileTransfer`.
- Essa função deve dar permissão para `secretsmanager:GetSecretValue` para acessar o segredo.

 Note

Na política, você deve especificar o ARN para o segredo. O ARN contém o nome secreto, mas acrescenta ao nome seis caracteres alfanuméricos aleatórios. Um ARN para um segredo tem o seguinte formato.

```
arn:aws:secretsmanager:region:account-id:secret:aws/transfer/SecretName-6RandomCharacters
```

- Certifique-se de que essa função contenha uma relação de confiança que permite que o conector acesse os recursos quando estiver atendendo às solicitações de transferência dos seus usuários. Para obter informações sobre como estabelecer um relacionamento de confiança, consulte [Estabelecer um relacionamento de confiança](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    }
  ]
}
```

```

    ],
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/SecretName-6RandomCharacters"
    }
  ]
}

```

Note

Para a função de acesso, o exemplo concede acesso a um único segredo. Porém, é possível usar um caractere curinga, que pode poupar trabalho se você quiser reutilizar o mesmo perfil do IAM para vários usuários e segredos. Por exemplo, a declaração de recurso a seguir concede permissões para todos os segredos que têm nomes começando com `aws/transfer`.

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

Você também pode armazenar segredos contendo suas credenciais de SFTP em outra Conta da AWS. Para obter detalhes sobre como ativar o acesso secreto

entre contas, consulte [Permissões para AWS Secrets Manager segredos para usuários em uma conta diferente](#).

- Em Resource Configuration ARN, insira o ARN da configuração de recursos VPC Lattice que aponta para seu servidor SFTP:

```
arn:aws:vpc-lattice:region:account-id:resourceconfiguration/rcfg-12345678
```

- (Opcional) Para a função Logging, escolha a função do IAM que o conector usará para enviar eventos aos seus CloudWatch registros.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

5. No painel Configuração do SFTP, forneça as seguintes informações:

- Para credenciais do Connector, escolha o nome de um segredo AWS Secrets Manager que contenha a chave privada ou a senha do usuário do SFTP.
- Para chaves de host confiáveis, cole a parte pública da chave de host usada para identificar o servidor externo ou deixe em branco para configurar posteriormente usando o `TestConnection` comando.

Como essa chave de host é para um conector VPC_LATTICE, remova o nome do host na chave

- (Opcional) Em Máximo de conexões simultâneas, escolha o número de conexões simultâneas que seu conector cria com o servidor remoto (o padrão é 5).

6. Na seção Opções de algoritmo criptográfico, escolha uma política de segurança na lista suspensa.
7. (Opcional) Na seção Tags, adicione tags como pares de valores-chave.
8. Escolha Criar conector SFTP para criar o conector VPC_ LATTICE-enabled SFTP.

O conector será criado com o status de PENDING enquanto a associação de recursos está sendo provisionada, o que normalmente leva alguns minutos. Quando o status mudar para ACTIVE, o conector estará pronto para uso.

CLI

Use o comando a seguir para criar um conector VPC_ LATTICE-enabled SFTP:

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
  --sftp-config UserSecretId=my-secret-id,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0} \
  --security-policy-name TransferSecurityPolicy-2024-01
```

O principal parâmetro para conectividade VPC é `--egress-config`, que especifica o ARN de configuração de recursos que define o destino do seu servidor SFTP.

Monitorando o status do conector VPC

Os LATTICE-enabled conectores VPC_ têm um processo de configuração assíncrono. Após a criação, monitore o status do conector:

- **PENDENTE:** O conector está sendo provisionado. O provisionamento da rede de serviços está em andamento, o que normalmente leva vários minutos.
- **ATIVO:** O conector está pronto para uso e pode transferir arquivos.
- **ERRO:** Falha no provisionamento do conector. Verifique os detalhes do erro para obter informações sobre solução de problemas.

Verifique o status do conector usando o `describe-connector` comando:


```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Durante o estado **PENDENTE**, a `test-connection` API retornará “Conector não disponível” até que o provisionamento seja concluído.

Limitações e considerações

- **Endpoints públicos:** ao se conectar a endpoints públicos por meio da VPC, você deve fornecer um nome DNS na Configuração de recursos. Endereços IP públicos não são suportados.
- **Disponibilidade regional:** a conectividade VPC está disponível em select. Regiões da AWS Cross-region o compartilhamento de recursos não é suportado.
- **Requisitos da zona de disponibilidade:** os gateways de recursos devem estar associados a sub-redes em pelo menos duas zonas de disponibilidade. Nem todas as zonas de disponibilidade oferecem suporte ao VPC Lattice em todas as regiões.
- **Limites de conexão:** máximo de 350 conexões por recurso com um tempo limite de inatividade de 350 segundos para conexões TCP.

Considerações sobre custos

Não há cobranças adicionais AWS Transfer Family além das taxas de serviço regulares. No entanto, os clientes podem estar sujeitos a cobranças adicionais da Amazon VPC Lattice associadas ao compartilhamento de seus recursos da Amazon Virtual Private Cloud e cobranças de gateway NAT se usarem seus próprios gateways NAT para acessar a Internet.

Para obter informações completas sobre AWS Transfer Family preços, consulte a [página AWS Transfer Family de preços](#).

Exemplos de conectividade VPC para conectores SFTP

Esta seção fornece exemplos de criação de conectores SFTP com conectividade VPC para vários cenários. Antes de usar esses exemplos, certifique-se de ter concluído a configuração da infraestrutura da VPC conforme descrito na documentação de conectividade da VPC.

Exemplo: conexão de endpoint privada

Este exemplo mostra como criar um conector SFTP que se conecta a um servidor SFTP privado acessível somente pela sua VPC.

Pré-requisitos

1. Crie um gateway de recursos em sua VPC:

```
aws vpc-lattice create-resource-gateway \  
  --name my-private-server-gateway \  
  --vpc-identifier vpc-1234567890abcdef0 \  
  --subnet-ids subnet-1234567890abcdef0 subnet-0987654321fedcba0
```

2. Crie uma configuração de recursos para seu servidor SFTP privado:

```
aws vpc-lattice create-resource-configuration \  
  --name my-private-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"} \  
  --port-ranges 22
```

Crie o conector VPC_ LATTICE-enabled

1. Crie o conector SFTP com conectividade VPC:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-private-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

2. Monitore o status do conector até que ele se torne ACTIVE:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

O servidor SFTP remoto verá as conexões provenientes do endereço IP do Resource Gateway dentro do intervalo CIDR da sua VPC.

Exemplo: endpoint público via VPC

Este exemplo mostra como rotear conexões para um servidor SFTP público por meio de sua VPC para aproveitar os controles de segurança centralizados e usar seus próprios endereços IP do NAT Gateway.

Pré-requisitos

1. Crie um Resource Gateway em sua VPC (o mesmo exemplo de endpoint privado).
2. Crie uma configuração de recursos para o servidor SFTP público usando seu nome DNS:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"} \  
  --port-ranges 22
```

Note

Para endpoints públicos, você deve usar um nome DNS, não um endereço IP.

Criar o conector

- Crie o conector SFTP:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-public-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-0987654321fedcba0,PortNumber=22}
```

O tráfego fluirá do conector para o Resource Gateway e, em seguida, pelo NAT Gateway para chegar ao servidor SFTP público. O servidor remoto verá o endereço IP elástico do seu NAT Gateway como origem.

Exemplo: endpoint Cross-account privado

Este exemplo mostra como se conectar a um servidor SFTP privado em uma AWS conta diferente usando o compartilhamento de recursos.

 Note

Se você já tem o compartilhamento de recursos entre VPCs habilitado por meio de outros mecanismos, como AWS Transit Gateway, por exemplo, não é necessário configurar o compartilhamento de recursos descrito aqui. Os mecanismos de roteamento existentes, como as tabelas de rotas do Transit Gateway, são usados automaticamente pelos conectores SFTP. Você só precisa criar uma configuração de recursos na mesma conta em que está criando o conector SFTP.

Conta A (provedor de recursos) - Compartilhe a configuração do recurso

1. Crie o gateway de recursos e a configuração de recursos na Conta A (igual aos exemplos anteriores).
2. Compartilhe a configuração do recurso com a conta B usando o AWS Resource Access Manager:

```
aws ram create-resource-share \  
    --name cross-account-sftp-share \  
    --resource-arns arn:aws:vpc-lattice:us-  
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0 \  
    --principals 222222222222
```

Conta B (consumidor de recursos) - Aceite e use o compartilhamento

1. Aceite o convite de compartilhamento de recursos:

```
aws ram accept-resource-share-invitation \  
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-  
share-invitation/invitation-id
```

2. Crie o conector SFTP na Conta B:

```
aws transfer create-connector \  
    --access-role arn:aws:iam::222222222222:role/TransferConnectorRole \  
    --sftp-config UserSecretId=cross-account-server-  
credentials,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \  

```

```
--egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

O conector na Conta B agora pode acessar o servidor SFTP privado na Conta A por meio da Configuração de Recursos compartilhada.

Cenários comuns de solução de problemas

Aqui estão as soluções para problemas comuns ao criar conectores VPC_LATTICE-enabled :

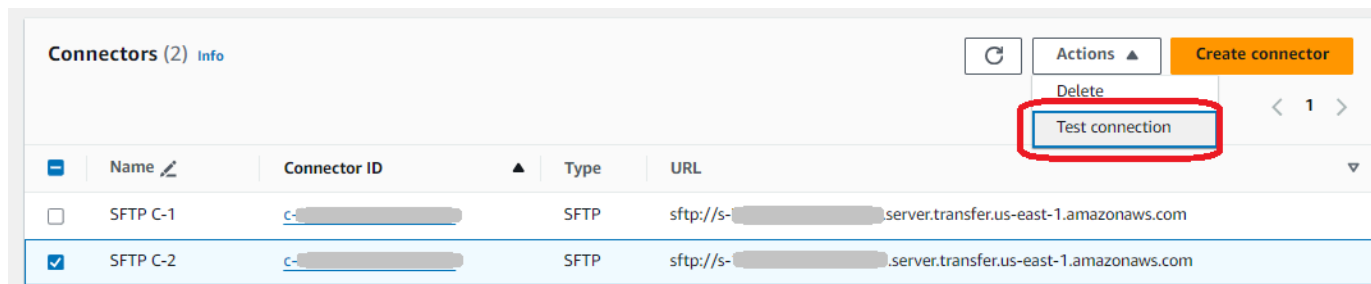
- Conector preso no status PENDENTE: verifique se o Resource Gateway está ATIVO e tem sub-redes em zonas de disponibilidade suportadas. Se o conector ainda estiver preso com o status PENDENTE, chame UpdateConnector usando os mesmos parâmetros de configuração que você usou inicialmente. Isso aciona um novo evento de status que pode resolver o problema.
- Tempos limite de conexão: verifique se as regras do grupo de segurança permitem tráfego na porta 22 e se o roteamento da VPC está correto.
- Problemas de resolução de DNS: para endpoints públicos, certifique-se de que sua VPC tenha conectividade com a Internet por meio de um NAT Gateway ou Internet Gateway.
- Cross-account acesso negado: verifique se o compartilhamento de recursos foi aceito e se o ARN de configuração de recursos está correto. Se a política de permissão adequada estiver anexada à configuração do recurso quando a conta de origem criar o compartilhamento de recursos, essas permissões serão necessárias: vpc-lattice:AssociateViaAWSService, vpc-lattice:AssociateViaAWSService-EventsAndStates, vpc-lattice:CreateServiceNetworkResourceAssociation, vpc-lattice:GetResourceConfiguration.

Testar um conector SFTP

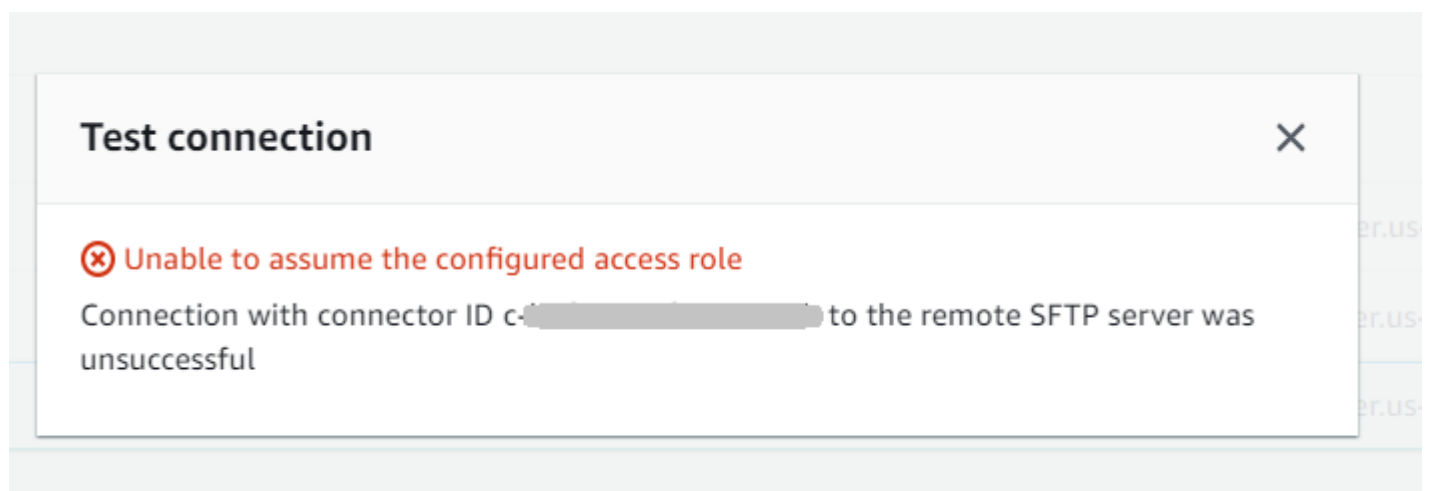
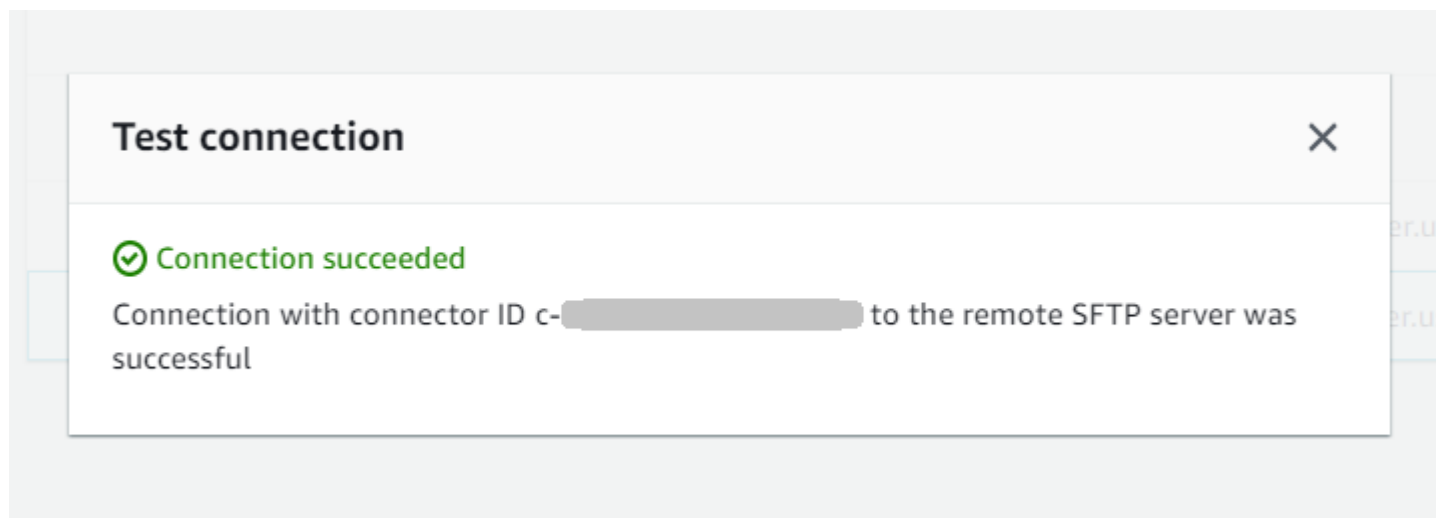
Depois de criar um conector SFTP, recomendamos que você o teste antes de tentar transferir qualquer arquivo usando o novo conector.

Para testar um conector SFTP

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, escolha Conectores SFTP e selecione um conector.
3. No menu Ações, selecione Testar conexões.



O sistema retorna uma mensagem indicando se o teste foi aprovado ou reprovado. Se o teste falhar, o sistema enviará uma mensagem de erro com base no motivo pelo qual o teste falhou.



Note

Para usar a API para testar seu conector, consulte a documentação da API [TestConnection](#).

Conectividade VPC para conectores SFTP

AWS Transfer Family Os conectores SFTP oferecem suporte à conectividade com servidores SFTP remotos por meio de seus ambientes VPC usando o Amazon VPC Lattice. Isso permite que você se conecte a servidores SFTP hospedados de forma privada ou roteie o tráfego da Internet por meio dos controles de segurança da sua VPC e use seus próprios gateways NAT e endereços IP elásticos.

Tipos de saída

Os conectores SFTP podem usar um dos dois tipos de saída:

- Serviço gerenciado (padrão): o conector usa gateways NAT e endereços IP de propriedade da AWS Transfer Family para rotear conexões pela Internet pública.
- VPC_LATTICE: o conector roteia o tráfego pelo seu ambiente VPC usando o Resource Access. Cross-VPC

Quando usar a conectividade VPC

Use a conectividade VPC para conectores SFTP nesses cenários:

- Servidores SFTP privados: conecte-se a servidores SFTP que só podem ser acessados pela sua VPC.
- On-premises conectividade: conecte-se a servidores SFTP locais por meio de conexões AWS Direct Connect ou AWS Site-to-Site VPN.
- Endereços IP personalizados: use seus próprios gateways NAT e endereços IP elásticos, incluindo cenários de BYOIP.
- Controles de segurança centralizados: encaminhe as transferências de arquivos pelos ingress/egress controles centrais da sua organização.

Requisitos

Antes de criar um conector VPC_ LATTICE-enabled SFTP, você precisa:

- VPC e infraestrutura relacionada (sub-redes, tabelas de rotas, grupos de segurança)
- Resource Gateway em sua VPC (mínimo de duas zonas de disponibilidade)
- Configuração de recursos especificando o servidor SFTP de destino

Para obter instruções detalhadas de configuração, consulte [Crie um conector VPC_LATTICE-enabled SFTP](#). E, para exemplos, consulte [Exemplos de conectividade VPC para conectores SFTP](#).

Usando conectores SFTP

Este tópico descreve como realizar as operações de arquivo suportadas usando seu conector SFTP. Você também pode encontrar exemplos de comandos para realizar essas operações selecionando os detalhes do seu conector no AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.

Depois de criar um conector SFTP, você pode usá-lo para realizar as seguintes operações de arquivo no servidor SFTP remoto ao qual ele está associado.

- Envie arquivos do Amazon S3 para o servidor SFTP remoto.
- Recupere arquivos do servidor SFTP remoto para o Amazon S3.
- Listar arquivos e subpastas de um diretório no servidor SFTP remoto.
- Exclua, renomeie ou mova arquivos e diretórios no servidor SFTP remoto.

Consulte [Criação de conectores SFTP](#) para obter detalhes sobre a criação de conectores.

Tópicos

- [Transferir arquivos](#)
- [Listar o conteúdo de um diretório remoto](#)
- [Mover, renomear ou excluir arquivos ou diretórios no servidor remoto](#)

Transferir arquivos

Tópicos

- [Enviar e recuperar arquivos usando um conector SFTP](#)

Enviar e recuperar arquivos usando um conector SFTP

Para enviar e recuperar arquivos usando um conector SFTP, você usa a operação de [StartFileTransfer](#) API e especifica os parâmetros a seguir, dependendo se você está enviando arquivos (transferências de saída) ou recebendo arquivos (transferências de entrada). Observe que cada `StartFileTransfer` solicitação pode conter 10 caminhos distintos.

Note

Por padrão, os conectores SFTP processam um arquivo por vez, transferindo arquivos sequencialmente. Você tem a opção de acelerar o desempenho da transferência fazendo com que seus conectores criem sessões simultâneas com servidores remotos que suportem sessões simultâneas do mesmo usuário e processem até 5 arquivos em paralelo. Para habilitar conexões simultâneas para qualquer conector, você pode editar a configuração Máximo de conexões simultâneas ao criar ou atualizar um conector. Para obter detalhes, consulte [Crie um conector SFTP com saída gerenciada por serviços](#).

- Transferências de saída
 - `send-file-paths` contém de um a dez caminhos de arquivo de origem, para que os arquivos sejam transferidos para o servidor SFTP do parceiro.
 - `remote-directory-path` é o caminho remoto para o qual enviar um arquivo no servidor SFTP do cliente.
- Transferências de saída
 - `retrieve-file-paths` contém de um a dez caminhos remotos. Cada caminho especifica um local para transferir arquivos do servidor SFTP do parceiro para o servidor Transfer Family.
 - `local-directory-path` é o local do Amazon S3 (bucket e prefixo opcional) onde seus arquivos são armazenados.

Para enviar arquivos, você especifica os parâmetros `send-file-paths` e `remote-directory-path`. É possível especificar até 10 arquivos para o parâmetro `send-file-paths`. O comando de exemplo a seguir envia os arquivos nomeados `/amzn-s3-demo-source-bucket/file1.txt` e `/amzn-s3-demo-source-bucket/file2.txt`, localizados no armazenamento do Amazon S3, para o diretório `/tmp` no servidor SFTP do seu parceiro. Para usar este comando de exemplo, substitua *amzn-s3-demo-source-bucket* pelo seu próprio bucket.

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt /amzn-s3-demo-source-bucket/file2.txt \
  --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

Para recuperar arquivos, você especifica os `local-directory-path` parâmetros `retrieve-file-paths` e. O exemplo a seguir recupera os arquivos `/my/remote/file1.txt` e o servidor SFTP do parceiro e os coloca `/my/remote/file2.txt` no local `/amzn-s3-demo-`

bucket/ do Amazon S3. *prefix* Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws transfer start-file-transfer --retrieve-file-paths /my/remote/file1.txt /my/remote/file2.txt \
  --local-directory-path /amzn-s3-demo-bucket/prefix --connector-id
c-2222BBBB3333CCCC4 --region us-east-2
```

Os exemplos anteriores especificam caminhos absolutos no servidor SFTP. É possível também usar caminhos relativos: ou seja, caminhos relativos ao diretório inicial do usuário do SFTP. Por exemplo, se o usuário do SFTP estiver marymajor e seu diretório inicial no servidor SFTP for /users/marymajor/, o comando a seguir envia /amzn-s3-demo-source-bucket/file1.txt para /users/marymajor/test-connectors/file1.txt

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt \
  --remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --
region us-east-2
```

Listar o conteúdo de um diretório remoto

Antes de recuperar arquivos de um servidor SFTP remoto, você pode recuperar o conteúdo de um diretório no servidor SFTP remoto. Para fazer isso, você usa a operação [StartDirectoryListing](#) da API.

O exemplo a seguir lista o conteúdo da home pasta no servidor SFTP remoto, que é especificado na configuração do conector. Os resultados são colocados no local /amzn-s3-demo-bucket/connector-files do Amazon S3 e em um arquivo chamado. c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json

```
aws transfer start-directory-listing \
  --connector-id c-AAAA1111BBBB2222C \
  --output-directory-path /amzn-s3-demo-bucket/example/connector-files \
  --remote-directory-path /home
```

Esse AWS CLI comando retorna uma ID de listagem e o nome do arquivo que contém os resultados.

```
{
  "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",
  "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"
```

```
}
```

Note

A convenção de nomenclatura para o arquivo de saída é *connector-ID-listing-ID.json*.

O arquivo JSON contém as seguintes informações:

- **filePath**: o caminho completo de um arquivo remoto, relativo ao diretório da solicitação de listagem do seu conector SFTP no servidor remoto.
- **modifiedTimestamp**: a última vez em que o arquivo foi modificado, em segundos, no formato UTC (Tempo Universal Coordenado). Esse campo é opcional. Se os atributos do arquivo remoto não contiverem um carimbo de data/hora, ele será omitido da lista de arquivos.
- **size**: o tamanho do arquivo, em bytes. Esse campo é opcional. Se os atributos do arquivo remoto não contiverem um tamanho de arquivo, ele será omitido da lista de arquivos.
- **path**: o caminho completo de um diretório remoto, relativo ao diretório da solicitação de listagem do seu conector SFTP no servidor remoto.
- **truncated**: um sinalizador indicando se a saída da lista contém todos os itens contidos no diretório remoto ou não. Se o valor **truncated** de saída for verdadeiro, você poderá aumentar o valor fornecido no atributo **max-items** de entrada opcional para poder listar mais itens (até o tamanho máximo permitido da lista de 200.000 itens).

Veja a seguir um exemplo do conteúdo do arquivo de saída (*c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json*), em que o diretório remoto contém dois arquivos e dois subdiretórios (caminhos).

```
{
  "files": [
    {
      "filePath": "/home/what.txt",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
      "size" : 2323
    },
    {
      "filePath": "/home/how.pgp",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
```

```
        "size" : 4691
      }
    ],
    "paths": [
      {
        "path": "/home/magic"
      },
      {
        "path": "/home/aws"
      },
    ],
    "truncated": "false"
  }
}
```

Mover, renomear ou excluir arquivos ou diretórios no servidor remoto

Tópicos

- [Mover ou renomear arquivos ou diretórios no servidor SFTP remoto](#)
- [Excluir arquivos ou diretórios no servidor SFTP remoto](#)

Mover ou renomear arquivos ou diretórios no servidor SFTP remoto

Você pode usar um conector SFTP para mover ou renomear arquivos e diretórios em um servidor SFTP remoto. Observe que o servidor remoto precisa oferecer suporte a essas operações para que o processamento seja bem-sucedido usando conectores.

Alguns casos de uso comuns são os seguintes.

- Um servidor remoto gera ou recebe um novo arquivo a cada hora, com o mesmo nome de arquivo, mas com um registro de data e hora diferente. Para manter a pasta principal atualizada (para que ela contenha somente o arquivo mais recente), você pode usar um conector para mover arquivos antigos para uma pasta arquivada.
- Você usa um conector para listar todos os arquivos em um diretório remoto e, em seguida, transfere todos os arquivos para o armazenamento local. Em seguida, você pode usar um conector para mover os arquivos para uma pasta arquivada no servidor remoto.

Você deve usar uma `StartRemoteMove` chamada para cada arquivo ou diretório que deseja processar, pois o comando usa um único arquivo ou diretório de origem e destino como argumentos.

No entanto, você pode acelerar o desempenho fazendo com que seus conectores criem sessões simultâneas com servidores remotos que suportam sessões simultâneas do mesmo usuário e move/rename até 5 arquivos em paralelo.

O exemplo a seguir move um arquivo no servidor SFTP remoto de `/source/folder/sourceFile` para `/destination/targetFile` e retorna um identificador exclusivo para a operação.

```
aws transfer --connector-id c-AAAA1111BBBB2222C start-remote-move \  
--source-path /source/folder/sourceFile --target-path /destination/targetFile
```

Note

Para as move/rename operações, o Transfer Family usa o SFTP `SSH_FXP_RENAME` comando padrão para fazer a move/rename operação.

Excluir arquivos ou diretórios no servidor SFTP remoto

Você pode usar um conector SFTP para excluir arquivos ou diretórios em um servidor SFTP remoto. Observe que o servidor remoto precisa oferecer suporte a essas operações para que o processamento seja bem-sucedido usando conectores.

Note

As operações de exclusão para diretórios remotos são suportadas somente para diretórios vazios.

Alguns casos de uso comuns são os seguintes.

- Você usa um conector para recuperar um arquivo de um servidor SFTP remoto, armazená-lo em seu bucket do Amazon S3 e criptografá-lo. Finalmente, você pode usar um conector para excluir o arquivo não criptografado no servidor remoto.
- Você usa um conector para listar todos os arquivos em um diretório remoto e, em seguida, transfere todos os arquivos para o armazenamento local. Em seguida, você pode usar um conector para excluir todos os arquivos que você transferiu. Você também pode excluir o diretório remoto, se preferir.

Você deve usar uma `StartRemoteDelete` chamada para cada arquivo ou diretório que deseja excluir, pois o comando usa um único arquivo ou diretório como argumento. No entanto, você pode acelerar o desempenho fazendo com que seus conectores criem sessões simultâneas com servidores remotos que suportem sessões simultâneas do mesmo usuário e excluam até 5 em `files/directories` paralelo.

O exemplo a seguir exclui um arquivo no servidor SFTP remoto no caminho `/delete/folder/deleteFile` e retorna um identificador exclusivo para a operação.

```
aws transfer start-remote-delete --connector-id c-AAAA1111BBBB2222C \
  --delete-path /delete/folder/deleteFile
```

Note

Para a operação de exclusão, o Transfer Family usa o `SSH_FXP_REMOVE` comando padrão para excluir um arquivo e `SSH_FXP_RMDIR` excluir um diretório.

Monitorando conectores SFTP

Você pode monitorar o status das operações do conector usando qualquer uma das seguintes formas. Escolha a abordagem que atenda às suas necessidades.

Use a API do conector para consultar o status das solicitações de transferência de arquivos

Para acompanhar o progresso de uma operação de transferência de arquivos, você usa a operação de [ListFileTransferResults](#) API, que retorna atualizações em tempo real e informações detalhadas sobre o status de cada arquivo individual que está sendo transferido em uma operação específica de transferência de arquivos. Você especifica a transferência do arquivo fornecendo sua ID de conector e sua ID de transferência. O exemplo a seguir retorna uma lista de arquivos para ID do conector `a-11112222333344444` e ID de transferência `aaa1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.

```
aws transfer list-file-transfer-results --connector-id a-11112222333344444 --transfer-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Note

Os resultados da transferência de arquivos estão disponíveis até 7 dias após você chamar a operação `ListFileTransferResults` da API.

Você também pode visualizar registros e eventos de suas solicitações de transferência de arquivos que usam conectores SFTP. Os eventos da Amazon para Transfer Family estão descritos em [Eventos do conector SFTP](#). Para saber como visualizar as entradas do CloudWatch registro do Transfer Family, consulte [Visualizando fluxos de registros do Transfer Family](#).

Veja eventos do conector SFTP na Amazon EventBridge

Para cada operação realizada por conectores SFTP, o Transfer Family gera e envia eventos automaticamente para o barramento de eventos padrão em sua conta da Amazon EventBridge. Os eventos contêm metadados detalhados sobre a operação, incluindo o status da operação. Você pode se inscrever nesses eventos em EventBridge, aplicar filtros em critérios específicos de eventos, como status da operação, e acionar automaticamente ações posteriores com base no status. Para obter detalhes sobre os eventos gerados pelas operações do conector SFTP, consulte [Eventos do conector SFTP](#).

Veja os registros do conector SFTP na Amazon CloudWatch

Todas as operações do conector SFTP geram registros CloudWatch detalhados. Por exemplo, entradas de registro geradas por conectores SFTP, consulte. [Exemplo de entradas de registro para conectores SFTP](#)

Monitorando conectores do tipo de saída VPC

Os conectores do tipo de saída VPC fornecem recursos e considerações adicionais de monitoramento além dos conectores gerenciados por serviços padrão:

monitoramento do status do conector

Os conectores VPC_LATTICE incluem informações adicionais para ajudá-lo a monitorar o provisionamento e o estado operacional:

- `EgressType` campo: Mostra os conectores do VPC tipo de saída VPC_LATTICE
- `EgressConfig` campo: contém o ARN de configuração do recurso e as informações da porta

Monitore o status do conector usando a `describe-connector` API:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Monitoramento de custos do VPC Lattice

Os conectores do tipo de saída VPC geram cobranças adicionais do VPC Lattice que você deve monitorar:

- Cobranças do provedor de recursos: você recebe uma cobrança de \$0.006/GB para processamento de dados como provedor de recursos (cobrado diretamente pela VPC Lattice)
- Cobranças do consumidor de recursos: a AWS Transfer Family absorve os \$0.01/GB custos do consumidor de recursos (primeiro 1 PB)
- Cobranças do NAT Gateway: para endpoints públicos acessados via VPC, taxas adicionais de NAT Gateway e transferência de dados podem ser aplicadas
- Taxas do Transfer Family: padrão \$0.40/GB taxas de processamento de dados ainda se aplicam

Monitore o uso e os custos do VPC Lattice por meio do console AWS Cost and Billing, filtrando pelo serviço VPC Lattice.

Monitoramento de rede para conectores VPC

Monitore a atividade e o desempenho da rede para conectores do tipo de saída VPC:

- Registros de fluxo de VPC: habilite os registros de fluxo de VPC para monitorar padrões de tráfego de rede entre gateways de recursos e servidores SFTP
- Registros de acesso ao VPC Lattice: o VPC Lattice fornece registros de acesso que mostram endereços source/destination IP, tempo de conexão e volumes de transferência de dados
- Monitoramento de grupos de segurança: monitore as regras do grupo de segurança e os padrões de tráfego para garantir controles adequados de acesso à rede
- Monitoramento da resolução de DNS: monitore os tempos e falhas de resolução de DNS para endpoints de rede de serviços

Exemplo de entrada de registro de acesso ao VPC Lattice:

```
{
```



```
{
  "eventTimestamp": "2025-01-16T20:59:08.531Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-1:123456789012:servicenetwork/sn-1234567890abcdef0",
  "sourceVpcArn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-12345678",
  "resourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-12345678",
  "protocol": "tcp",
  "sourceIpPort": "10.0.1.100:33760",
  "destinationIpPort": "10.0.2.200:22",
  "gatewayIpPort": "10.0.1.150:1769",
  "resourceIpPort": "10.0.2.200:22"
}
```

Solução de problemas por meio do monitoramento

Use dados de monitoramento para solucionar problemas comuns do conector VPC:

- Status PENDENTE: monitore o progresso da resolução de DNS e aguarde o status ATIVO antes de tentar transferências
- Tempos limite de conexão: verifique os registros de fluxo da VPC e as regras do grupo de segurança para ver se há tráfego bloqueado na porta 22
- Falhas de transferência: revise CloudWatch os registros para obter mensagens de erro detalhadas e os registros de acesso ao VPC Lattice para problemas no nível da rede
- Problemas de desempenho: monitore os registros de acesso ao VPC Lattice para verificar o tempo de conexão e as métricas de taxa de transferência

Gerenciando conectores SFTP

Este tópico descreve como exibir e atualizar conectores SFTP.

Note

Cada conector recebe automaticamente endereços IP estáticos que permanecem inalterados durante a vida útil do conector. Isso permite que você se conecte a servidores SFTP remotos que só aceitam conexões de entrada de endereços IP conhecidos. Seus conectores recebem um conjunto de endereços IP estáticos que são compartilhados por todos os conectores usando o mesmo protocolo (SFTP ou AS2) no seu. Conta da AWS Esses endereços não são dedicados exclusivamente à sua conta.

Se você precisar de endereços IP dedicados e previsíveis, configure seus conectores com VPC-based saída. Para obter mais informações, consulte [the section called “Crie um conector SFTP com saída VPC-based”](#).

Atualizar conectores SFTP

Para alterar os valores dos parâmetros existentes para seus conectores, é possível executar o comando `update-connector`. O comando a seguir atualiza o segredo do conector *connector-id*, na região *region-id* para *secret-ARN*. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws transfer update-connector --sftp-config '{"UserSecretId":"secret-ARN"}' \
  --connector-id connector-id --region region-id
```

Atualização das configurações de conectividade da VPC

Você pode atualizar as configurações de conectividade da VPC para conectores existentes, incluindo alternar entre os tipos de saída de VPC e gerenciados por serviços ou alterar o ARN da configuração de recursos.

Para mudar um conector de gerenciamento de serviço para saída de VPC:

```
aws transfer update-connector \
  --connector-id connector-id \
  --egress-type VPC \
  --egress-config ResourceConfigurationArn=resource-configuration-arn
```

Para atualizar o ARN de configuração de recursos para um conector VPC_: LATTICE-enabled

```
aws transfer update-connector \
  --connector-id connector-id \
  --egress-config ResourceConfigurationArn=new-resource-configuration-arn
```

Note

Ao atualizar as configurações de conectividade da VPC, o status do conector mudará para PENDING durante o processo de reconfiguração. Monitore o status do conector usando o `describe-connector` comando.

Exibir detalhes do conector SFTP

É possível encontrar uma lista de detalhes e propriedades de um conector SFTP no console AWS Transfer Family .

Como visualizar detalhes do conector

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerda, escolha Conectores.
3. Escolha o identificador na coluna ID do conector para ver a página de detalhes do conector selecionado.

É possível alterar as propriedades do conector SFTP escolhendo Editar na página de detalhes do conector.

Monitorando o status do conector VPC

LATTICE-enabled Os conectores VPC_ incluem informações adicionais de status para ajudá-lo a monitorar o processo de provisionamento:

- Status: PENDING Mostra ACTIVE, ou ERRORED
- EgressType: Shows VPC ou SERVICE_MANAGED
- EgressConfig: contém o ARN de configuração de recursos para conectores VPC
- Erro: fornece informações detalhadas sobre o erro se o conector estiver no ERRORED estado

Para conectores VPC, o ServiceManagedEgressIpAddresses campo será nulo, pois o tráfego usa seus endereços IP de VPC em vez disso.

Note

Você pode obter muitas dessas informações, embora em um formato diferente, executando o comando a seguir AWS Command Line Interface (AWS CLI). Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws transfer describe-connector --connector-id your-connector-id
```

Para obter mais informações, consulte [DescribeConnector](#) na referência da API.

Dimensionamento e cotas para conectores SFTP

Tópicos

- [Cotas da para conectores SFTP](#)
- [Dimensionando seus conectores SFTP](#)

Cotas da para conectores SFTP

As cotas a seguir estão em vigor para conectores SFTP.

Note

Mais cotas de serviço para conectores SFTP estão listadas em [AWS Transfer Family endpoints e](#) cotas no. Referência geral da Amazon Web Services

Cotas do conector SFTP

Nome	Padrão	Ajustável
Máximo de transações de conexão de teste por segundo (TPS)	1 solicitação por segundo, por conta	Não
Tamanho máximo da fila para Transferência de Arquivos pendentes	1000	Não
Tamanho máximo do arquivo	150 gibibytes (GiB)	Não
Tempo máximo de transferência por arquivo	12 horas	Não
Tempo máximo de espera da solicitação por arquivo	12 horas	Não
Largura de banda máxima para conectores por conta	50 MBps	Não

Nome	Padrão	Ajustável
(os conectores SFTP e AS2 contribuem para esse valor)		
Número máximo de itens para operações de listagem de diretórios	200.000	Não

Note

Por padrão, os conectores SFTP processam um arquivo por vez, transferindo arquivos sequencialmente. Você tem a opção de acelerar o desempenho da transferência fazendo com que seus conectores criem sessões simultâneas com servidores remotos que suportem sessões simultâneas do mesmo usuário e processem até 5 arquivos em paralelo. Para habilitar conexões simultâneas para qualquer conector, você pode editar a configuração Máximo de conexões simultâneas ao criar ou atualizar um conector. Para obter detalhes, consulte [Crie um conector SFTP com saída gerenciada por serviços](#).

Para armazenar as credenciais dos conectores SFTP, há cotas associadas a cada segredo do Secrets Manager. Se você usar o mesmo segredo para armazenar vários tipos de chaves, para várias finalidades, poderá encontrar essas cotas.

- Tamanho total de um único segredo: 12.000 caracteres
- Tamanho máximo da **Password** string: 1024 caracteres
- Comprimento máximo da **PrivateKey** string: 8192 caracteres
- Comprimento máximo da **Username** string: 100 caracteres

Dimensionando seus conectores SFTP

Esta seção descreve considerações sobre como escalar suas cargas de trabalho do conector AWS Transfer Family SFTP. Você precisa levar em consideração as três cotas a seguir que se aplicam quando você deseja escalar suas cargas de trabalho com conectores SFTP.

- O tamanho máximo da fila. Isso se refere ao número máximo de operações pendentes na fila de um conector que foram solicitadas. Uma operação pendente se refere a qualquer solicitação de transferência enviada anteriormente que ainda não foi concluída, com ou sem sucesso.

Atualmente, a profundidade máxima da fila para solicitações pendentes está definida em 1.000 por conector (conforme definido nas [cotas AWS Transfer Family de serviço](#)). Suas cargas de trabalho podem exceder esse limite de serviço quando você solicita milhares de operações de transferência em um curto período, e você receberá uma mensagem `ThrottlingException` com a mensagem Excedeu o máximo de solicitações pendentes. Se suas cargas de trabalho estiverem sujeitas a essa cota, entre em contato com a equipe de atendimento da Transfer Family AWS Support ou com sua equipe de contas para discutir seus requisitos de escalabilidade.

Você também pode realizar uma ou ambas as ações a seguir.

- Distribua seus volumes de arquivos em vários conectores.
- Faça com que seus conectores criem sessões simultâneas com o servidor remoto para processar várias solicitações da fila em paralelo.
- O número de sessões simultâneas. Por padrão, um conector SFTP transfere um arquivo por vez, transferindo arquivos sequencialmente de sua fila.

Você tem a opção de acelerar o desempenho da transferência fazendo com que seus conectores transfiram vários arquivos em paralelo. Você pode criar sessões simultâneas com servidores remotos que suportam sessões simultâneas do mesmo usuário e processar até 5 arquivos em paralelo. Ao criar um conector SFTP, escolha um valor de até 5 para a configuração Máximo de conexões simultâneas ao criar ou atualizar o conector. Para obter detalhes, consulte [Crie um conector SFTP com saída gerenciada por serviços](#).

- A taxa de **StartFileTransfer** solicitações. Você pode solicitar até 100 caminhos de arquivo por segundo para transferência com cada conector SFTP. Os caminhos de arquivo solicitados são adicionados à fila de seus conectores para processamento. Você pode usar o `StartFileTransfer` comando recursivamente para solicitar até 100 caminhos de arquivo por segundo por conector, independentemente do número de arquivos fornecidos em um comando `individualStartFileTransfer`.

Arquiteturas de referência usando conectores SFTP

Esta seção lista os materiais de referência que estão disponíveis para configurar fluxos de trabalho automatizados de transferência de arquivos usando conectores SFTP. Você pode criar suas próprias

arquiteturas orientadas a eventos usando os eventos do conector SFTP na Amazon EventBridge, para orquestrar entre sua ação de transferência de arquivos e as ações de pré e pós-processamento na Amazon. AWS

Publicações no blog

A postagem de blog a seguir fornece uma arquitetura de referência para criar um fluxo de trabalho de MFT usando conectores SFTP, incluindo criptografia de arquivos usando PGP antes de enviá-los para um servidor SFTP remoto usando conectores SFTP: [Arquitetando transferências de arquivos gerenciadas seguras e compatíveis com conectores SFTP e criptografia PGP](#). AWS Transfer Family

Workshops

- O workshop a seguir fornece laboratórios práticos para configurar conectores SFTP e usar seus conectores para enviar ou recuperar arquivos de servidores SFTP remotos: [workshop Transfer Family - SFTP](#).
- [O workshop a seguir fornece laboratórios práticos para criar fluxos de trabalho totalmente automatizados e orientados por eventos envolvendo transferência de arquivos de ou para servidores SFTP externos para o Amazon S3 e pré-processamento e pós-processamento comuns desses arquivos: workshop MFT. Event-driven](#)

Este vídeo fornece um resumo desse workshop.

Soluções

AWS Transfer Family fornece as seguintes soluções:

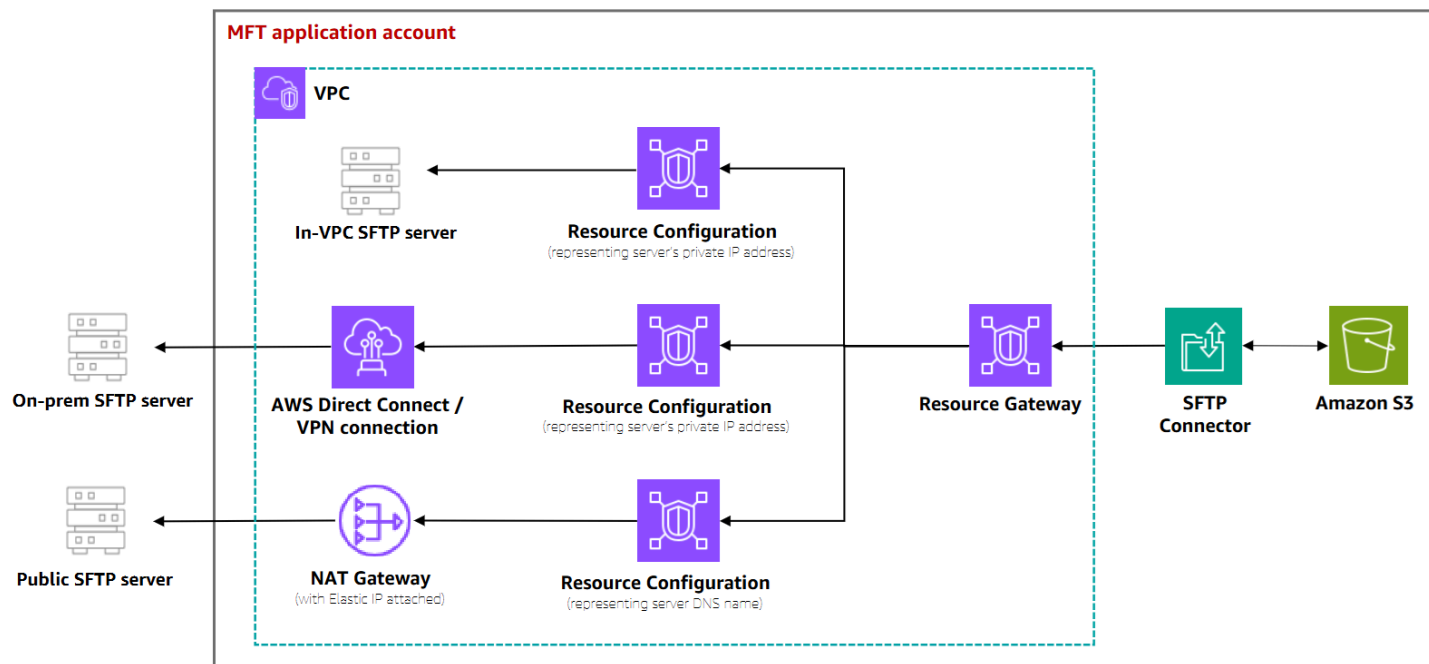
- A [solução de sincronização de transferência de arquivos](#) fornece uma arquitetura de referência para automatizar o processo de sincronização de diretórios SFTP remotos, incluindo estruturas de pastas inteiras, com seus buckets locais do Amazon S3 usando um conector SFTP. Ele orquestra o processo de listar diretórios remotos, detectar alterações e transferir arquivos novos ou modificados.
- [Serverlessland - A transferência seletiva de arquivos entre o servidor SFTP remoto e o S3; o uso AWS Transfer Family](#) fornece um padrão de amostra para listar arquivos armazenados em locais remotos de SFTP e transferir arquivos seletivos para o Amazon S3.

Arquiteturas de referência de VPC

As arquiteturas de referência a seguir mostram padrões comuns para a implantação de conectores LATTICE-enabled VPC_SFTP. Esses exemplos ajudam você a entender onde os recursos do VPC Lattice precisam ser criados em sua arquitetura geral. AWS

Conta única com infraestrutura de saída compartilhada

Nessa arquitetura, a infraestrutura de saída (NAT Gateway, túnel VPN ou Direct Connect) é configurada em uma VPC dentro da mesma conta que seus conectores SFTP. Todos os conectores podem compartilhar o mesmo Resource Gateway e o NAT Gateway.



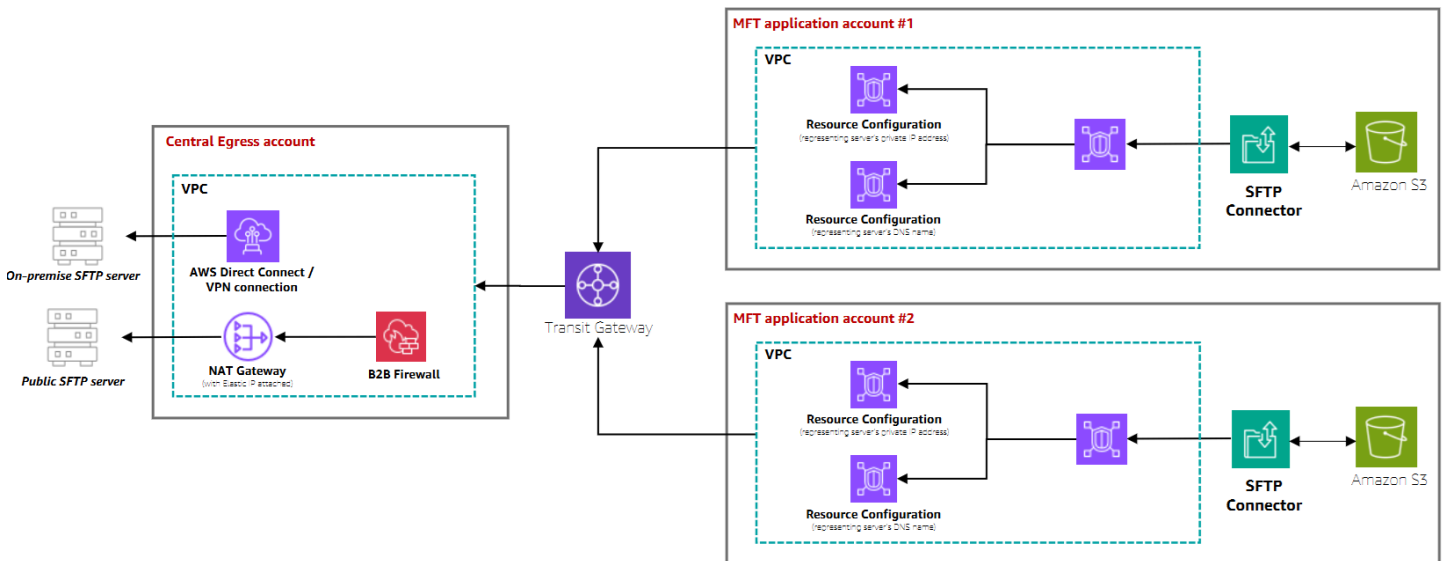
Esse padrão é ideal quando:

- Todos os conectores SFTP são gerenciados em um único Conta da AWS
- A infraestrutura de saída é configurada em uma VPC dentro da mesma conta que seus conectores SFTP

Cross-account com infraestrutura de saída centralizada

Nessa arquitetura, a infraestrutura de saída (NAT Gateway, túnel VPN, Direct Connect ou Firewalls B2B) é configurada em uma conta de saída central gerenciada pela equipe de rede. Os conectores SFTP são criados na conta do aplicativo MFT gerenciada pela equipe de administração do MFT.

Cross-account a rede é estabelecida usando o Transit Gateway para honrar as regras de rede existentes.



Esse padrão é ideal quando:

- A infraestrutura de rede é gerenciada por uma equipe separada em uma conta dedicada
- Você tem rotas existentes (como AWS Transit Gateway) entre a conta em que os conectores SFTP são criados e a conta em que a infraestrutura de saída está configurada. Os conectores SFTP poderão aproveitar suas rotas existentes conectando as duas contas.
- Controles de segurança centralizados e firewalls B2B são necessários
- Você precisa manter a separação de tarefas entre as equipes de rede e de aplicativos

AWS Transfer Family para AS2

A Declaração de Aplicabilidade 2 (AS2) é uma especificação de RFC-defined transmissão de arquivos que inclui mecanismos robustos de proteção e verificação de mensagens. A proteção de uma carga AS2 em trânsito usa a Sintaxe de Mensagens Criptográficas (CMS) com criptografia e assinaturas digitais para fornecer proteção de dados e autenticação entre pares. Uma carga de resposta assinada do Aviso de Disposição de Mensagens (MDN) fornece verificação (sem repúdio) de que uma mensagem foi recebida e descriptografada com sucesso.

O protocolo AS2 é essencial para fluxos de trabalho com requisitos de conformidade que dependem de recursos de proteção e segurança de dados incorporados ao protocolo. AWS Transfer Family Os endpoints AS2 são [certificados pela Drummond](#), permitindo que clientes em setores como varejo, ciências biológicas, manufatura, serviços financeiros e serviços públicos realizem transações com segurança com seus parceiros de negócios.

Quando você usa o AS2 com Transfer Family, os dados transacionados são acessíveis de forma nativa em para: AWS

- Processamento, análise e aprendizado de máquina
- Integração com sistemas de planejamento de recursos corporativos (ERP)
- Integração com sistemas de gerenciamento de relacionamento com o cliente (CRM)

Para trocar arquivos com um parceiro que tenha um AS2-enabled servidor, você deve:

- Gere um par de chaves pública-privada para criptografia
- Gere um par de chaves pública-privada para assinatura
- Troque as chaves públicas com seu parceiro

Important

Atualmente, os endpoints do servidor HTTPS AS2 não são suportados. Você é responsável pela rescisão do TLS.

O Transfer Family oferece um workshop do qual você pode participar, no qual você pode configurar um endpoint Transfer Family com AS2 habilitado e um conector Transfer Family AS2. É possível ver os detalhes desse workshop [aqui](#).

Para obter instruções passo a passo para configurar o AS2 no Transfer Family, consulte o seguinte:

1. [Importar certificados AS2](#)
2. [Crie perfis AS2](#)
3. [Crie um servidor AS2](#)
4. [Crie um contrato AS2](#)
5. [Configurar conectores AS2](#)

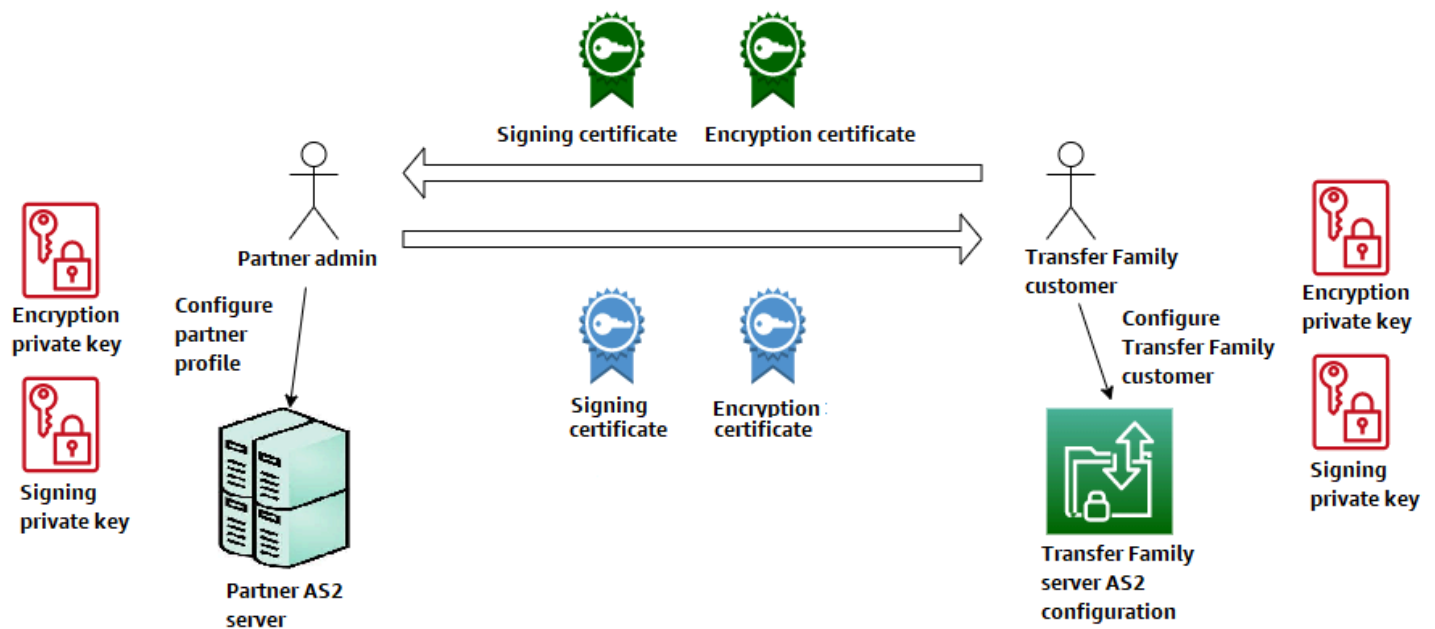
Para obter um exemplo completo, consulte [Configurando uma configuração AS2](#).

 Note

Para mostrar suporte aos modelos AS2 Terraform, adicione uma reação positiva (#) à solicitação de recurso de modelos do [Transfer Family Terraform](#). Você também pode adicionar um comentário descrevendo seu caso de uso.

Casos de uso do AS2

Se você é um AWS Transfer Family cliente que deseja trocar arquivos com um parceiro que tem um AS2-enabled servidor, a parte mais complexa da configuração envolve gerar um par de chaves público-privadas para criptografia e outro para assinar e trocar as chaves públicas com o parceiro.



Considere as seguintes variações para uso AWS Transfer Family com o AS2.

Note

O parceiro comercial é o parceiro associado a esse perfil de parceiro.
Todas as menções de MDN na tabela a seguir pressupõem mDNS assinado.

Casos de uso do AS2

Inbound-only casos de uso

- Transfira mensagens AS2 criptografadas de um parceiro comercial para um servidor Transfer Family.

Nesse caso, você faz o seguinte:

- Crie perfis para você e seu parceiro comercial.
- Crie um servidor Transfer Family que use o protocolo AS2.
- Crie um contrato e adicione-o ao seu servidor.
- Importe um certificado com uma chave privada e adicione-o ao seu perfil e, em seguida, importe a chave pública para seu perfil de parceiro para criptografia.
- Depois de ter esses itens, envie a chave pública do seu certificado ao seu parceiro comercial.

Agora, seu parceiro pode enviar mensagens criptografadas e é possível descriptografá-las e armazená-las em seu bucket do Amazon S3.

- Transfira mensagens AS2 criptografadas de um parceiro comercial para um servidor Transfer Family e adicione assinatura.

Nesse cenário, você ainda está fazendo apenas transferências de entrada, mas agora deseja que seu parceiro assine as mensagens enviadas. Nesse caso, importe a chave pública de assinatura do parceiro comercial (como um certificado de assinatura adicionado ao perfil do seu parceiro).

- Transfira mensagens AS2 criptografadas de um parceiro comercial para um servidor Transfer Family e adicione assinatura e envio de uma resposta MDN.

Nesse cenário, você ainda está fazendo apenas transferências de entrada, mas agora, além de receber cargas assinadas, seu parceiro comercial deseja receber uma resposta MDN assinada.

1. Importe suas chaves de assinatura públicas e privadas (como um certificado de assinatura para seu perfil).
2. Envie a chave pública de assinatura para seu parceiro comercial.

Outbound-only casos de uso

- Transfira mensagens AS2 criptografadas de um servidor Transfer Family para um parceiro comercial.

Esse caso é semelhante ao caso de uso de transferência somente de entrada, exceto que, em vez de adicionar um contrato ao seu servidor AS2, você cria um conector. Nesse caso, você importa a chave pública do seu parceiro comercial para o perfil dele.

- Transfira mensagens AS2 criptografadas de um servidor Transfer Family para um parceiro comercial e adicione assinatura.

Você ainda está fazendo apenas transferências externas, mas agora seu parceiro comercial quer que você assine a mensagem que você envia para ele.

1. Importe sua chave privada de assinatura (como um certificado de assinatura adicionado ao seu perfil).
 2. Envie sua chave pública ao seu parceiro comercial.
- Transfira mensagens AS2 criptografadas de um servidor Transfer Family para um parceiro comercial, adicione assinaturas e envie uma resposta MDN.

Você ainda está fazendo apenas transferências externas, mas agora, além de enviar cargas assinadas, deseja receber uma resposta MDN assinada do seu parceiro comercial.

1. Seu parceiro comercial envia a você a chave pública de assinatura.
2. Importe a chave pública do seu parceiro comercial (como um certificado de assinatura adicionado ao seu perfil de parceiro).

Casos de uso de entrada e saída

- Transfira mensagens AS2 criptografadas em ambas as direções entre um servidor Transfer Family e um parceiro comercial.

Nesse caso, você faz o seguinte:

1. Crie perfis para você e seu parceiro comercial.
2. Crie um servidor Transfer Family que use o protocolo AS2.
3. Crie um contrato e adicione-o ao seu servidor.
4. Crie um conector.
5. Importe um certificado com uma chave privada e adicione-o ao seu perfil e, em seguida, importe a chave pública para seu perfil de parceiro para criptografia.
6. Receba uma chave pública do seu parceiro comercial e adicione-a ao perfil dele para criptografia.
7. Depois de ter esses itens, envie a chave pública do seu certificado ao seu parceiro comercial.

Agora você e seu parceiro comercial podem trocar mensagens criptografadas e ambos podem decifrá-las. É possível armazenar as mensagens que você recebe em seu bucket do Amazon S3, e seu parceiro pode descriptografar e armazenar as mensagens que você envia para ele.

- Transfira mensagens AS2 criptografadas em ambas as direções entre um servidor Transfer Family e um parceiro comercial e adicione a assinatura.

Agora você e seu parceiro querem mensagens assinadas.

1. Importe sua chave privada de assinatura (como um certificado de assinatura adicionado ao seu perfil).
 2. Envie sua chave pública ao seu parceiro comercial.
 3. Importe a chave pública de assinatura do seu parceiro comercial e adicione-a ao perfil dele.
- Transfira mensagens AS2 criptografadas em ambas as direções entre um servidor Transfer Family e um parceiro comercial, adicione assinaturas e envie uma resposta MDN.

Agora, você quer trocar cargas assinadas, e você e seu parceiro comercial querem respostas da MDN.

1. Seu parceiro comercial envia a você a chave pública de assinatura.
2. Importe a chave pública do seu parceiro comercial (como um certificado de assinatura para seu perfil de parceiro).

3. Envie sua chave pública para seu parceiro comercial.

Modelos AS2 CloudFormation

Este tópico fornece informações sobre AWS CloudFormation modelos que você pode usar para implantar rapidamente servidores e configurações AS2. AWS Transfer Family Esses modelos automatizam o processo de configuração e ajudam você a implementar as melhores práticas para transferências de arquivos AS2.

- O modelo AS2 básico é descrito em [Use um modelo para criar uma pilha de demonstração do Transfer Family AS2](#)
- O modelo AS2 para personalizar cabeçalhos HTTP é descrito em. [Personalize cabeçalhos HTTP para mensagens AS2](#)

Personalizando modelos AS2

Você pode personalizar os modelos fornecidos para atender às suas necessidades específicas:

1. Faça o download do modelo a partir do URL do S3.
2. Modifique o código YAML para ajustar configurações como:
 - Configurações de segurança e configurações de certificado
 - Arquitetura de rede e configurações de VPC
 - Opções de armazenamento e tratamento de arquivos
 - Preferências de monitoramento e notificação
3. Faça upload do modelo modificado em seu próprio bucket do S3.
4. Implante o modelo personalizado usando o CloudFormation console ou AWS CLI.

Important

Ao personalizar modelos, certifique-se de manter as dependências entre os recursos e seguir as melhores práticas de segurança.

Testando sua implantação do AS2

Depois de implantar um servidor AS2 usando um modelo, você pode testar a configuração:

1. Verifique as saídas da CloudFormation pilha para ver exemplos de comandos e informações do endpoint.
2. Use o AWS CLI para enviar um arquivo de teste:

```
aws s3api put-object --bucket your-bucket-name --key test.txt --body test.txt  
aws transfer start-file-transfer --connector-id your-connector-id --send-file-  
paths /your-bucket-name/test.txt
```

3. Verifique a entrega do arquivo no bucket S3 de destino.
4. Verifique CloudWatch os registros para ver se o processamento e as respostas do MDN foram bem-sucedidos.

Para testes mais abrangentes, considere usar clientes AS2 de terceiros para enviar arquivos para seu servidor Transfer Family AS2.

Práticas recomendadas para implantação do modelo AS2

Siga estas melhores práticas ao usar CloudFormation modelos AS2:

Segurança

Use certificados fortes e alterne-os regularmente.

Implemente políticas de IAM com privilégios mínimos.

Restrinja o acesso à rede usando grupos de segurança.

Confiabilidade

Implemente em várias zonas de disponibilidade.

Implemente monitoramento e alertas para transferências com falha.

Configure novas tentativas automáticas para transferências malsucedidas.

desempenho

Escolha os tipos de instância apropriados para seu volume de transferência.

Implemente políticas de ciclo de vida do S3 para gerenciamento eficiente de arquivos.

Monitore e otimize as configurações de rede.

Otimização de custo

Use o auto-scaling para cargas de trabalho variáveis.

Implemente classes de armazenamento S3 para arquivos mais antigos.

Monitore e ajuste os recursos com base no uso real.

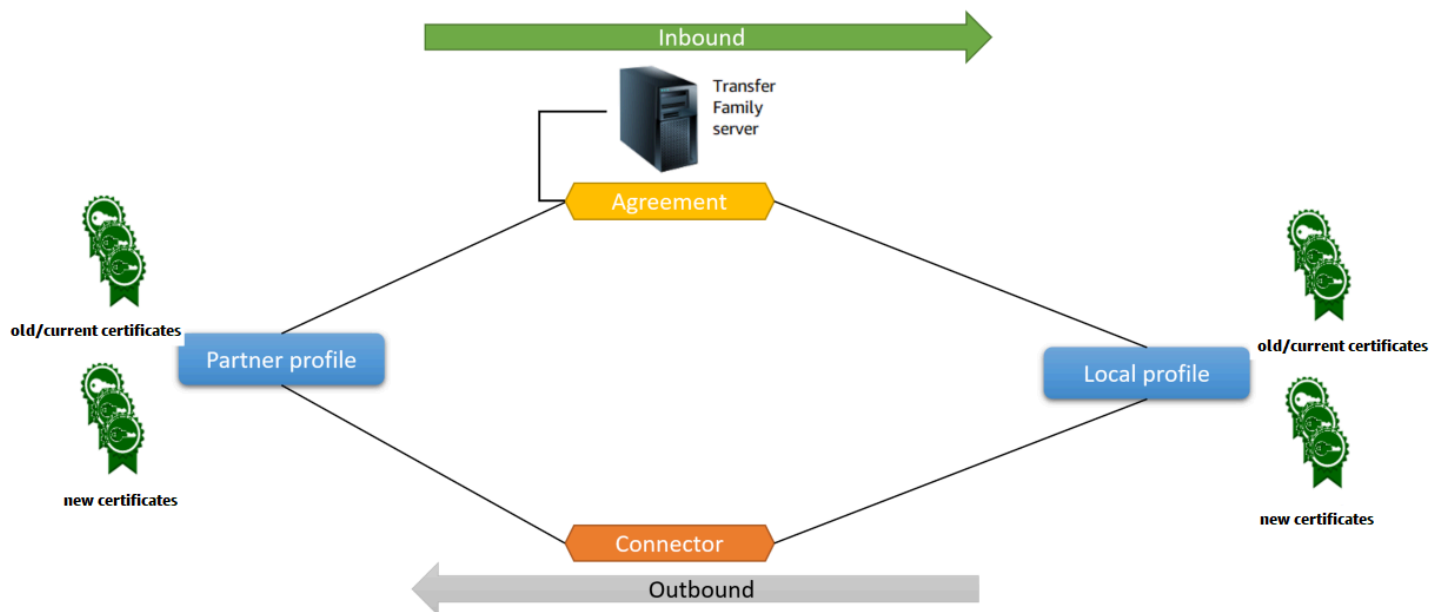
Configurar AS2

Para criar um AS2-enabled servidor, você também deve especificar os seguintes componentes:

- **Acordos** — Acordos bilaterais de parceiros comerciais, ou parcerias, definem o relacionamento entre as duas partes que estão trocando mensagens (arquivos). Para definir um contrato, o Transfer Family combina um servidor, um perfil local, um perfil de parceiro e informações do certificado. Os AS2-inbound processos da Transfer Family usam acordos.
- **Certificados** — Os certificados de chave pública (X.509) são usados na comunicação AS2 para criptografia e verificação de mensagens. Os certificados também são usados para terminais de conectores.
- **Perfis locais e perfis de parceiros** — Um perfil local define a organização ou “parte” local (servidor AS2-enabled Transfer Family). Da mesma forma, um perfil de parceiro define a organização parceira remota, externa à Transfer Family.

Embora não seja necessário para todos os AS2-enabled servidores, para transferências externas, você precisa de um conector. Um conector captura os parâmetros para uma conexão de saída. O conector é necessário para enviar arquivos para o AWS servidor externo do cliente.

O diagrama a seguir mostra a relação entre os objetos AS2 envolvidos nos processos de entrada e saída.



Para um exemplo completo de configuração AS2, consulte [Configurando uma configuração AS2](#).

Tópicos

- [Configurações AS2](#)
- [Cotas e limitações AS2](#)
- [Recursos e capacidades AS2](#)

Configurações AS2

Este tópico descreve as configurações, os atributos e as capacidades suportadas para transferências que usam o protocolo Applicability Statement 2 (AS2), incluindo as cifras e resumos aceitos.

Assinatura, criptografia, compressão, MDN

Para transferências de entrada e de saída, os seguintes itens são obrigatórios ou opcionais:

- Criptografia – Obrigatório (para transporte HTTP, que é o único método de transporte suportado atualmente). Mensagens não criptografadas só são aceitas se forem encaminhadas por um TLS-terminating proxy, como um Application Load Balancer (ALB), e X-Forwarded-Proto: https o cabeçalho estiver presente.
- Assinatura — Opcional
- Compressão — Opcional (o único algoritmo de compactação atualmente suportado é ZLIB)

- Aviso de disposição de mensagens (MDN) — Opcional

Cifras

As cifras a seguir são suportadas para transferências de entrada e saída:

- AES128_CBC
- AES192_CBC
- AES256_CBC
- 3DES (somente para compatibilidade com versões anteriores)

Resumos

Os seguintes resumos são suportados:

- Assinatura de entrada e MDN — SHA1, SHA256, SHA384, SHA512
- Assinatura de saída e MDN — SHA1, SHA256, SHA384, SHA512

MDN

Para respostas MDN, determinados tipos são suportados, como segue:

- Transferências de entrada — síncronas e assíncronas
- Transferências de saída — síncronas e assíncronas
- Protocolo de transferência de correio simples (SMTP) (e-mail MDN) – Não suportado

Transportes

- Transferências de entrada — HTTP é o único transporte atualmente suportado e você deve especificá-lo explicitamente.

Note

Se precisar usar HTTPS para transferências de entrada, você poderá encerrar o TLS em um Application Load Balancer ou Network Load Balancer. Isso está descrito em [Receba mensagens AS2 por HTTPS](#).

- Transferências de saída — Se você fornecer uma URL HTTP, também deverá especificar um algoritmo de criptografia. Se você fornecer um URL HTTPS, terá a opção de especificar NONE para seu algoritmo de criptografia.

Cotas e limitações AS2

Esta seção discute cotas e limitações do AS2

Tópicos

- [Cotas AS2](#)
- [Cotas para lidar com segredos](#)
- [Limitações conhecidas](#)

Cotas AS2

As cotas a seguir estão em vigor para transferências de arquivos AS2. Para solicitar um aumento para uma cota ajustável, consulte as [AWS service \(Serviço da AWS\) cotas](#) no Referência geral da AWS.

Cotas AS2

Nome	Padrão	Ajustável
Número máximo de arquivos por solicitação de saída	10	Não
Número máximo de solicitações de saída por segundo	100	Não
Número máximo de solicitações de entrada por segundo	100	Não
Largura de banda máxima de saída por conta (as solicitações SFTP e AS2 de saída contribuem para esse valor)	50 MB por segundo	Não

Cotas para lidar com segredos

AWS Transfer Family faz chamadas AWS Secrets Manager em nome de clientes AS2 que estão usando a autenticação básica. Além disso, o Secrets Manager faz chamadas para AWS KMS.

Note

Essas cotas não são específicas para o uso de segredos para Transfer Family: elas são compartilhadas entre todos os serviços do seu Conta da AWS.

Para o Secrets Manager `GetSecretValue`, a cota aplicável é a taxa combinada de solicitações `DescribeSecret` e de `GetSecretValue` API, conforme descrito em [AWS Secrets Manager cotas](#).

Secrets Manager **GetSecretValue**

Nome	Valor	Description
Taxa combinada de solicitações <code>DescribeSecret</code> e de <code>GetSecretValue</code> API	Cada região compatível: 10.000 por segundo	O máximo de transações por segundo para operações <code>DescribeSecret</code> de <code>GetSecretValue</code> API combinadas.

Para AWS KMS, as seguintes cotas se aplicam. `Decrypt` Para obter detalhes, consulte [Solicitar cotas para cada operação de AWS KMS API](#)

AWS KMS **Decrypt**

Nome da cota	Valor padrão (solicitações por segundo)
Taxa de solicitação de operações criptográficas (simétricas)	Essas cotas compartilhadas variam de acordo com Região da AWS e com o tipo de AWS KMS chave usada na solicitação. Cada cota é calculada separadamente. 5.500 (compartilhado) 10.000 (compartilhado) nas seguintes regiões:

Nome da cota	Valor padrão (solicitações por segundo)
	• Leste dos EUA (Ohio), us-east-2 • Ásia-Pacífico (Singapura), ap-southeast-1 • Ásia-Pacífico (Sydney), ap-southeast-2 • Ásia-Pacífico (Tóquio), ap-northeast-1 • Europa (Frankfurt), eu-central-1 • Europa (Londres), eu-west-2 • 50.000 (compartilhadas) nas seguintes regiões: • Leste dos EUA (Norte da Virgínia), us-east-1 • Oeste dos EUA (Oregon), us-west-2 • Europa (Irlanda), eu-west-1
Cotas de solicitação de armazenamento de chaves personalizadas  Note Esta cota só se aplica se você estiver usando um repositório de chaves externo.	As cotas de solicitação de armazenamento de chaves personalizadas são calculadas separadamente para cada armazenamento de chaves personalizadas. • 1.800 (compartilhados) para cada armazenamento de AWS CloudHSM chaves • 1.800 (compartilhado) para cada repositório de chaves externo

Limitações conhecidas

- Server-side O TCP keep-alive não é suportado. A conexão expira após 350 segundos de inatividade, a menos que o cliente envie pacotes keep-alive.
- Para que um contrato ativo seja aceito pelo serviço e apareça nos CloudWatch registros da Amazon, as mensagens devem conter cabeçalhos AS2 válidos.
- [O servidor que está recebendo mensagens do AWS Transfer Family AS2 deve suportar o atributo de proteção do algoritmo Cryptographic Message Syntax \(CMS\) para validar assinaturas de](#)

[mensagens, conforme definido na RFC 6211](#). Este atributo não é suportado em alguns produtos IBM Sterling mais antigos.

- IDs de mensagem duplicados resultam em uma processed/Warning: mensagem de documento duplicado.
- O comprimento da chave para certificados AS2 deve ser de pelo menos 2.048 bits e no máximo 4.096.
- Ao enviar mensagens AS2 ou mDNS assíncrono para o endpoint HTTPS de um parceiro comercial, as mensagens ou mDNS devem usar um certificado SSL válido assinado por uma autoridade de certificação (CA) publicamente confiável. Self-signed atualmente, os certificados são suportados somente para transferências externas.
- O endpoint deve suportar o protocolo TLS versão 1.2 e um algoritmo criptográfico permitido pela política de segurança (conforme descrito em [Políticas de segurança para AWS Transfer Family servidores](#)).
- Vários anexos e mensagens de troca de certificados (CEM) do AS2 versão 1.2 não são suportados atualmente.
- Atualmente, a autenticação básica é suportada apenas para mensagens de saída.
- Você pode anexar um fluxo de trabalho de processamento de arquivos a um servidor Transfer Family que usa o protocolo AS2: no entanto, as mensagens AS2 não executam fluxos de trabalho conectados ao servidor.

Recursos e capacidades AS2

As tabelas a seguir listam os recursos e capacidades disponíveis para recursos do Transfer Family que usam AS2.

Recursos AS2

O Transfer Family oferece os seguintes recursos para AS2.

Recurso	Apoiado por AWS Transfer Family
Certificação Drummond	Sim
AWS CloudFormation apoio	Sim
CloudWatchMétricas da Amazon	Sim

Recurso	Apoiado por AWS Transfer Family
SHA-2 algoritmos criptográficos	Sim
Support para Amazon S3	Sim
Suporte para o Amazon EFS	Não
Mensagens agendadas	Sim ¹
AWS Transfer Family Fluxos de trabalho gerenciados	Não
Mensagens de troca de certificados (CEM)	Não
TLS mútua (mTLS)	Não
Support para certificados autoassinados	Sim

1. Mensagens agendadas de saída disponíveis por meio de [AWS Lambda funções de agendamento usando a Amazon EventBridge](#)

Capacidades de envio e recebimento AS2

A tabela a seguir fornece uma lista dos recursos de envio e recebimento do AWS Transfer Family AS2.

Recurso	Entrada: recebimento com servidor	Saída: envio com conector
Transporte criptografado TLS (HTTPS)	Sim ¹	Sim
Non-TLS Transporte (HTTP)	Sim	Sim ²
MDN síncrono	Sim	Sim
Compressão de mensagens	Sim	Sim
MDN assíncrono	Sim	Sim

Recurso	Entrada: recebimento com servidor	Saída: envio com conector
Endereço IP estático	Sim	Sim
Traga seu próprio endereço IP	Sim	Não
Vários anexos de arquivo	Não	Não
Autenticação básica	Não	Sim
Reinício do AS2	Não aplicável	Não
Confiabilidade AS2	Não	Não
Assunto personalizado por mensagem	Não aplicável	Não

1. Transporte criptografado TLS de entrada disponível com Network Load Balancer (NLB) ou Application Load Balancer (ALB)
2. Transporte não TLS de saída disponível somente quando a criptografia está habilitada

Gerenciar certificados AS2

Este tópico discute como importar e gerenciar certificados AS2. A importação de certificados é a primeira etapa do processo AS2 para Transfer Family.

1. Importar certificados
2. [Crie perfis AS2](#)
3. [Crie um servidor AS2](#)
4. [Crie um contrato AS2](#)
5. [Configurar conectores AS2](#)

Importar certificados AS2

O processo Transfer Family AS2 usa chaves de certificado para criptografia e assinatura das informações transferidas. Os parceiros podem usar a mesma chave para ambas as finalidades ou

uma chave separada para cada uma. Se você tiver chaves de criptografia comuns mantidas sob custódia por um terceiro confiável para que os dados possam ser descriptografados em caso de desastre ou violação de segurança, recomendamos ter chaves de assinatura separadas. Ao usar chaves de assinatura separadas (que você não deposita em garantia), você não compromete os recursos de não repúdio de suas assinaturas digitais.

 Note

O comprimento da chave para certificados AS2 deve ser de pelo menos 2.048 bits e no máximo 4.096.

Os pontos a seguir detalham como os certificados AS2 são usados durante o processo.

- AS2 de entrada
 - O parceiro comercial envia sua chave pública para o certificado de assinatura, e essa chave é importada para o perfil do parceiro.
 - A parte local envia a chave pública para seus certificados de criptografia e assinatura. Em seguida, o parceiro importa a chave ou as chaves privadas. A parte local pode enviar chaves de certificado separadas para assinatura e criptografia, ou pode optar por usar a mesma chave para ambas as finalidades.
- AS2 de saída
 - O parceiro envia a chave pública para seu certificado de criptografia, e essa chave é importada para o perfil do parceiro.
 - A parte local envia a chave pública do certificado para assinatura e importa a chave privada do certificado para assinatura.
 - Se você estiver usando HTTPS, poderá importar um certificado TLS (Transport Layer Security) autoassinado.

Para obter detalhes sobre como criar certificados, consulte [the section called “Etapa 1: Criar os certificados para AS2”](#).

Este procedimento explica como importar certificados usando o console Transfer Family. Se você quiser usar o AWS CLI em vez disso, consulte [the section called “Etapa 2: Importar certificados como recursos de certificados do Transfer Family”](#).

Para especificar um AS2-enabled certificado

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, em Parceiros comerciais AS2, escolha Certificados.
3. Escolha Importar certificado.
4. Na seção Configuração do certificado, em Descrição do certificado, insira um nome facilmente identificável para o certificado. Certifique-se de que você possa identificar a finalidade do certificado por meio de sua descrição. Além disso, escolha a função para o certificado.
5. Na seção Uso do certificado, escolha a finalidade desse certificado. Ele pode ser usado para criptografia, assinatura ou ambos.

Dica: se você escolher Criptografia e assinatura para o uso, o Transfer Family cria dois certificados idênticos (cada um com seu próprio ID): um com um valor de uso de ENCRYPTION e outro com um valor de uso de SIGNING.

6. Na seção Conteúdo do certificado, forneça um certificado público de um parceiro comercial ou as chaves públicas e privadas de um certificado local.

Preencha a seção Conteúdo do certificado com os detalhes apropriados.

- Se você escolher o Self-signed certificado, não fornecerá a cadeia de certificados.
 - Cole o texto do certificado e sua cadeia no campo Certificado e cadeia de certificados.
 - Se esse certificado for um certificado local, cole sua chave privada.
7. Escolha Importar certificado para concluir o processo e salvar os detalhes do certificado importado.

Note

Os certificados TLS só podem ser importados como um certificado público do parceiro. Se você selecionar Certificado público de um parceiro e, em seguida, selecionar Transport Layer Security (TLS) para o uso, receberá um aviso. Além disso, os certificados TLS devem ser autoassinados (ou seja, você deve selecionar Certificado autoassinado para importar um certificado TLS).

Alternância de certificados AS2

Frequentemente, os certificados são válidos por um período de seis meses a um ano. Talvez você tenha configurado perfis que deseja manter por mais tempo. Para facilitar isso, o Transfer Family fornece rotação de certificados. É possível especificar vários certificados para um perfil, permitindo que você continue usando o perfil por vários anos. O Transfer Family usa certificados para assinatura (opcional) e criptografia (obrigatória). É possível especificar um único certificado para ambas as finalidades, se quiser.

A rotação de certificados é o processo de substituição de um certificado antigo expirado por um certificado mais recente. A transição é gradual para evitar a interrupção das transferências em que um parceiro no contrato ainda não configurou um novo certificado para transferências externas ou pode estar enviando cargas assinadas ou criptografadas com um certificado antigo durante um período em que um certificado mais novo também pode estar em uso. O período intermediário em que os certificados antigos e novos são válidos é chamado de período de carência.

X.509 os certificados têm `Not Before` e `Not After` datas. No entanto, esses parâmetros podem não fornecer controle suficiente para os administradores. O Transfer Family fornece configurações `Active Date` e `Inactive Date` para controlar qual certificado é usado para cargas de saída e qual é aceito para cargas de entrada.

Monitoramento da expiração do certificado

A Transfer Family publica uma CloudWatch métrica da Amazon `DaysUntilExpiry` depois de importar um certificado. A métrica emite o número de dias entre a data atual e a data especificada `InactiveDate` no certificado. A métrica é encontrada no `Transfer AWS` namespace no painel de CloudWatch métricas.

Essa métrica sempre terá uma dimensão métrica para `CertificateId`, opcionalmente, incluirá uma dimensão `Descrição`, se fornecida pelo cliente no certificado. Para obter mais informações sobre dimensões CloudWatch métricas, consulte [Dimensão](#) na Referência CloudWatch da API.

Note

Após a importação de um Certificado do Transfer Family, pode levar até um dia inteiro para emitir essa métrica para a conta do cliente.

Você pode usar essa métrica para criar CloudWatch alarmes que o notificam quando os certificados estão prestes a expirar.

A seleção do certificado de saída usa o valor máximo anterior à data da transferência como um `Inactive Date`. Os processos de entrada aceitam certificados dentro da faixa de `Not Before` e `Not After` e dentro da faixa de `Active Date` e `Inactive Date`.

Exemplo de rotação de certificados

A tabela a seguir descreve uma forma possível de configurar dois certificados para um único perfil.

Dois certificados em rotação

Nome	NOT BEFORE (controlado pela autoridade certificadora)	ACTIVE DATE (definido pelo Transfer Family)	INACTIVE DATE (definido pelo Transfer Family)	NOT AFTER (definido pela autoridade de certificação)
Cert1 (certificado antigo)	01/11/2019	2020-01-01	2020-12-31	2024-01-01
Cert2 (certificado mais recente)	01-11-2020	2020-06-01	2021-06-01	2025-01-01

Observe o seguinte:

- Quando você especifica um `Active Date` e `Inactive Date` para um certificado, o intervalo deve estar dentro do intervalo entre `Not Before` e `Not After`.
- Recomendamos que você configure vários certificados para cada perfil, certificando-se de que o intervalo de datas ativo de todos os certificados combinados cubra a quantidade de tempo durante a qual você deseja usar o perfil.
- Recomendamos que você especifique algum tempo de carência entre o momento em que seu certificado antigo se torna inativo e o momento em que seu certificado mais novo se torna ativo. No exemplo anterior, o primeiro certificado não se torna inativo até 31/12/2020, enquanto o segundo certificado se torna ativo em 01/06/2020, fornecendo um período de carência de 6 meses. Durante o período de 01/06/2020 a 31/12/2020, ambos os certificados estão ativos.

Crie perfis AS2

Este tópico discute como criar perfis para uso no processo AS2. Um perfil local define a organização ou “parte” local (servidor AS2-enabled Transfer Family). Da mesma forma, um perfil de parceiro define a organização parceira remota, externa à Transfer Family.

1. [Importar certificados AS2](#)
2. Crie perfis AS2
3. [Crie um servidor AS2](#)
4. [Crie um contrato AS2](#)
5. [Configurar conectores AS2](#)

Use esse procedimento para criar perfis locais e de parceiros. Este procedimento explica como criar perfis AS2 usando o console Transfer Family. Se você quiser usar o AWS CLI em vez disso, consulte [the section called “Etapa 3: Crie perfis para você e seu parceiro comercial”](#).

Para criar um perfil AS2

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, em AS2 Trading Partners, escolha Perfis e, em seguida, escolha Criar perfil.
3. Na seção Configuração do perfil, insira o ID AS2 para o perfil. Esse valor é usado para os cabeçalhos HTTP específicos do protocolo AS2 `as2-from` e `as2-to` para identificar a parceria comercial, que determina os certificados a serem usados e assim por diante.
4. Na seção Tipo de perfil, escolha Perfil local ou Perfil de parceiro.
5. Na seção Certificados, escolha um ou mais certificados no menu suspenso.

Dica: Se você quiser importar um certificado que não esteja listado no menu suspenso, selecione Importar um novo certificado. Isso abre uma nova janela do navegador na tela Importar certificado. Para obter o procedimento de importação de certificados, consulte [Importar certificados AS2](#).

6. (Opcional) Na seção Etiquetas, especifique um ou mais pares chave-valor para ajudar a identificar esse perfil.
7. Escolha Criar perfil para concluir o processo e salvar o novo perfil.

Crie um servidor AS2

Este tópico fornece instruções para criar um servidor AS2-enabled Transfer Family usando o console ou um CloudFormation modelo. Para um exemplo completo de configuração AS2, consulte [Configurando uma configuração AS2](#). Depois de criar um servidor AS2, você pode adicionar um contrato ao servidor.

1. [Importar certificados AS2](#)
2. [Crie perfis AS2](#)
3. Crie um servidor AS2
4. [Crie um contrato AS2](#)
5. [Configurar conectores AS2](#)

Tópicos

- [Crie um servidor AS2 usando o console Transfer Family](#)
- [Use um modelo para criar uma pilha de demonstração do Transfer Family AS2](#)
- [Crie um contrato AS2](#)

Crie um servidor AS2 usando o console Transfer Family

Este procedimento explica como criar um AS2-enabled servidor usando o console Transfer Family. Se você quiser usar o AWS CLI em vez disso, consulte [the section called “Etapa 4: Criar um servidor Transfer Family que usa o protocolo AS2”](#).

Note

Você pode anexar um fluxo de trabalho de processamento de arquivos a um servidor Transfer Family que usa o protocolo AS2: no entanto, as mensagens AS2 não executam fluxos de trabalho conectados ao servidor.

Para criar um AS2-enabled servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, escolha Servidores e Criar servidor.

3. Na página Escolher protocolos, selecione AS2 (Declaração de Aplicabilidade 2) e escolha Avançar.
4. Na página Escolha um provedor de identidade, escolha Avançar.

 Note

Para o AS2, você não pode escolher um provedor de identidade porque a autenticação básica não é suportada pelo protocolo AS2. Em vez disso, você controla o acesso por meio de grupos de segurança de nuvem privada virtual (VPC).

5. Na página Escolher uma função do endpoint, faça o seguinte:

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID





[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

Cancel

Previous

Next

- a. Em Tipo de endpoint, escolha Hospedado no VPC para hospedar o endpoint do seu servidor. Para obter informações sobre como configurar seu VPC-hosted endpoint, consulte [Crie um servidor em uma VPC \(virtual private cloud\)](#).

 Note

Os endpoints acessíveis publicamente não são compatíveis com o protocolo AS2. Para tornar seu endpoint da VPC acessível pela Internet, escolha Voltado para a internet em Acesso e, em seguida, forneça seus endereços IP elásticos.

- b. Para Acesso, escolha uma das seguintes opções:
- Interno — Escolha essa opção para fornecer acesso de dentro de sua VPC e de VPC-connected ambientes, como um data center local ou VPN. Direct Connect
 - Voltado para a Internet — Escolha essa opção para fornecer acesso pela Internet e de dentro de sua VPC e VPC-connected ambientes, como um data center local ou VPN. Direct Connect
- Se você escolher Voltado para a internet, forneça seus endereços IP elásticos quando solicitado.
- c. Para VPC, escolha uma VPC existente ou escolha Criar VPC para criar uma nova VPC.
- d. Para FIPS ativado, mantenha a caixa de seleção FIPS habilitado endpoint desmarcada.

 Note

FIPS-enabled os endpoints não são suportados pelo protocolo AS2.

- e. Escolha Próximo.
6. Na página Escolha um domínio, escolha Amazon S3 para armazenar e acessar seus arquivos como objetos usando o protocolo selecionado.

Escolha Próximo.

7. Na página Configurar detalhes adicionais, escolha as configurações necessárias.

 Note

Se você estiver configurando outros protocolos junto com o AS2, todas as configurações de detalhes adicionais se aplicam. No entanto, para o protocolo AS2, as únicas configurações que se aplicam são aquelas nas seções de CloudWatch registro e Tags. Embora a configuração de uma função de CloudWatch registro seja opcional, é altamente recomendável configurá-la para que você possa ver o status de suas mensagens e solucionar problemas de configuração.

8. Na página Revisar e criar, revise suas escolhas para se certificar de que estão corretas.

- Se você quiser editar qualquer uma das suas configurações, escolha Editar ao lado da etapa que você deseja alterar.

 Note

Se você editar uma etapa, recomendamos que revise cada etapa após a etapa que você escolheu editar.

- Se você não tiver alterações, escolha Criar servidor para criar seu servidor. Você será direcionado à página Servidores, exibida a seguir, onde seu novo servidor estará listado.

Pode levar vários minutos até que o status do seu novo servidor mude para Online. Nesse momento, seu servidor poderá realizar operações de arquivo para seus usuários.

Use um modelo para criar uma pilha de demonstração do Transfer Family AS2

Fornecemos um CloudFormation modelo independente para criar rapidamente um servidor AS2-enabled Transfer Family. O modelo configura o servidor com um endpoint da VPC público da Amazon, certificados, perfis locais e de parceiro, um contrato e um conector.

O modelo básico do servidor AS2 cria os seguintes recursos:

- Um servidor AS2-enabled Transfer Family com um endpoint VPC
- Perfis AS2 locais e de parceiros com certificados
- Um acordo entre os perfis

- Um bucket Amazon S3 para armazenamento de arquivos
- Funções e políticas obrigatórias do IAM
- CloudWatch configuração de registro

Antes de usar este modelo, observe o seguinte:

- Se você criar uma pilha a partir deste modelo, você será cobrado pelos recursos AWS usados.
- O modelo cria vários certificados e os coloca AWS Secrets Manager para armazená-los com segurança. Você pode excluir esses certificados do Secrets Manager se quiser, porque você é cobrado pelo uso desse serviço. A exclusão desses certificados no Secrets Manager não os exclui do servidor Transfer Family. Portanto, a funcionalidade da pilha de demonstração não é afetada. No entanto, para certificados que você vai usar com um servidor AS2 de produção, talvez você queira usar o Secrets Manager para gerenciar e alternar periodicamente seus certificados armazenados.
- Recomendamos que você use o modelo somente como base e principalmente para fins de demonstração. Se você quiser usar essa pilha de demonstração na produção, recomendamos que você modifique o código YAML do modelo para criar uma pilha mais robusta. Por exemplo, crie certificados em nível de produção e crie uma função AWS Lambda que você possa usar na produção.

Para criar um servidor AS2-enabled Transfer Family a partir de um CloudFormation modelo

1. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. No painel de navegação à esquerda, selecione Pilhas.
3. Selecione Criar pilha e, depois, Com novos recursos (padrão).
4. Na seção Pré-requisito - Preparar modelo, escolha Escolher um modelo existente.
5. Copie esse link, [modelo de demonstração do AS2](#), e cole-o no campo URL do Amazon S3.
6. Escolha Próximo.
7. Na página Especificar detalhes da pilha, nomeie sua pilha e especifique os seguintes parâmetros:
 - Em AS2, insira valores para ID AS2 local e IDv AS2 do parceiro ou aceite os padrões `local` e `partner`, respectivamente.
 - Em Rede, insira um valor para o IP CIDR de entrada do grupo de segurança ou aceite o padrão, `0.0.0.0/0`.

 Note

Esse valor, no formato CIDR, especifica quais endereços IP são permitidos para tráfego de entrada no servidor AS2. O valor padrão, `0.0.0.0/0`, permite todos os endereços IP.

- Em Geral, insira um valor para Prefixo ou aceite o padrão, `transfer-as2`. Esse prefixo é colocado antes de qualquer nome de recurso criado pela pilha. Por exemplo, se você usar o prefixo padrão, seu bucket do Amazon S3 será nomeado `transfer-as2-amzn-s3-demo-bucket`.
8. Escolha Próximo. Na página Configurar opções de pilha, selecione Próximo novamente.
 9. Revise os detalhes da pilha que você está criando e escolha Criar pilha.

 Note

Na parte inferior da página, em Capacidades, você deve reconhecer que isso CloudFormation pode criar recursos AWS Identity and Access Management (IAM).

Depois que a pilha for criada, você poderá enviar uma mensagem AS2 de teste do servidor parceiro para o servidor local do Transfer Family usando o AWS Command Line Interface (AWS CLI). Um exemplo de AWS CLI comando para enviar uma mensagem de teste é criado junto com todos os outros recursos na pilha.

Para usar esse exemplo de comando, acesse a guia Saídas da sua pilha e copie o.

`TransferExampleAs2Command` Em seguida, você pode executar o comando usando o AWS CLI. Se você ainda não instalou o AWS CLI, consulte [Instalando ou atualizando a versão mais recente do AWS CLI](#) no Guia do AWS Command Line Interface Usuário.

O comando de amostra tem o formato a seguir:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt && aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId --send-file-paths /amzn-s3-demo-bucket/test.txt
```

 Note

Sua versão desse comando contém os valores reais dos recursos *amzn-s3-demo-bucket* e *TransferConnectorId* em sua pilha.

Esse exemplo de comando consiste em dois comandos separados que são encadeados usando a string `&&`.

O primeiro comando cria um novo arquivo de texto vazio no seu bucket:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt
```

Em seguida, o segundo comando usa o conector para enviar o arquivo do perfil do parceiro para o perfil local. O servidor Transfer Family tem um contrato configurado que permite que o perfil local aceite mensagens do perfil do parceiro.

```
aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId  
--send-file-paths /amzn-s3-demo-bucket/test.txt
```

Depois de executar o comando, você pode acessar seu bucket do Amazon S3 (*amzn-s3-demo-bucket*) e visualizar o conteúdo. Se o comando for bem-sucedido, você deverá visualizar os seguintes objetos do no bucket:

- `processed/` – Essa pasta contém um arquivo JSON que descreve o arquivo transferido e a resposta do MDN.
- `processing/` – Essa pasta contém arquivos temporariamente à medida que eles estão sendo processados, mas após a conclusão da transferência, essa pasta deve estar vazia.
- *server-id/* – Essa pasta é nomeada com base no ID do servidor Transfer Family. Ela contém `from-partner` (essa pasta é nomeada dinamicamente, com base na ID AS2 do parceiro), que por si só contém as pastas `failed/`, `processed/`, e `processing/`. A pasta *server-id/* `from-partner`/`processed/` contém uma cópia do arquivo de texto transferido e os arquivos JSON e MDN correspondentes.
- `test.txt` – Esse objeto é o arquivo (vazio) que foi transferido.

Crie um contrato AS2

Os contratos estão associados aos servidores Transfer Family. Eles especificam os detalhes dos parceiros comerciais que usam o protocolo AS2 para trocar mensagens ou arquivos usando o Transfer Family, para transferências de entrada — enviando arquivos AS2 de uma fonte externa de propriedade do parceiro para um servidor Transfer Family.

Este procedimento explica como criar contratos AS2 usando o console Transfer Family. Se você quiser usar o AWS CLI em vez disso, consulte [the section called “Etapa 5: criar um acordo entre você e seu parceiro”](#).

Para criar um contrato para um servidor Transfer Family

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, selecione Servidores e escolha um servidor que use o protocolo AS2.

Como alternativa, desde que você tenha pelo menos um servidor Transfer Family que use o protocolo AS2, selecione Acordos para receber mensagens no menu AS2 Trading Partners. Em seguida, na tela Criar contrato, selecione o servidor AS2 ao qual você deseja associar esse contrato.

3. Na página de detalhes do servidor, role para baixo até a seção Acordos.
4. Escolha Adicionar acordo.
5. Preencha os parâmetros do contrato, da seguinte forma:
 - a. Na seção Contrato, insira um nome descritivo. Certifique-se de que você possa identificar a finalidade do contrato pelo nome. Além disso, defina o Status do contrato: Ativo (selecionado por padrão) ou Inativo.
 - b. Na seção Configurações de comunicação, escolha um perfil local e um perfil de parceiro. Além disso, escolha se deseja ou não impor a assinatura de mensagens.
 - Por padrão, o Enforce Message Signing está ativado, o que significa que o Transfer Family rejeita mensagens não assinadas do seu parceiro comercial para este contrato.
 - Desmarque essa configuração para permitir que a Transfer Family aceite mensagens não assinadas do seu parceiro comercial para este contrato.
 - c. Na seção Configuração do diretório da caixa de entrada, forneça as seguintes informações.

- Determine se deseja ou não selecionar Especificar diretórios separados para armazenar suas mensagens AS2, arquivos MDN e arquivos de status JSON.
- Se você selecionar essa opção, você especifica locais separados para arquivos de carga útil, arquivos com falha, arquivos MDN, arquivos de status e arquivos temporários.
- Se você desmarcar essa opção, todos os arquivos AS2 entrarão no local especificado para o diretório base.
- Para o S3 Bucket, escolha um bucket Amazon S3.
- Em Prefixo, você pode inserir um prefixo (pasta) a ser usado para armazenar arquivos no bucket.

Por exemplo, se você inserir **amzn-s3-demo-bucket** para seu bucket e **incoming** para seu prefixo, seus arquivos AS2 serão salvos na **/amzn-s3-demo-bucket/incoming** pasta.

- Para a função AWS do IAM, escolha uma função que possa acessar o bucket que você especificou.
 - Em Preservar nome do arquivo, escolha se deseja preservar os nomes dos arquivos originais para cargas de mensagens AS2 recebidas.
 - Se você selecionar essa configuração, o nome do arquivo fornecido pelo seu parceiro comercial será preservado quando o arquivo for salvo no Amazon S3.
 - Se você desmarcar essa configuração, quando o Transfer Family salvar o arquivo, o nome do arquivo será ajustado, conforme descrito em. [Nomes e localizações dos arquivos](#)
- d. (Opcional) Adicione etiquetas na seção Etiquetas.
- e. Depois de inserir todas as informações do contrato, escolha Criar contrato.

O novo contrato aparece na seção Acordos da página de detalhes do servidor.

Configurar conectores AS2

O objetivo de um conector é estabelecer um relacionamento entre parceiros comerciais para transferências externas — enviando arquivos AS2 de um servidor Transfer Family para um destino externo de propriedade do parceiro. Para o conector, você especifica a parte local, o parceiro remoto e seus certificados (criando perfis locais e de parceiros).

Depois de instalar um conector, é possível transferir informações para seus parceiros comerciais. Cada servidor AS2 recebe três endereços IP estáticos. Os conectores AS2 usam esses endereços IP para enviar mDNS assíncrono para seus parceiros comerciais via AS2.

 Note

O tamanho da mensagem recebida por um parceiro comercial não corresponderá ao tamanho do objeto no Amazon S3. Essa discrepância ocorre porque a mensagem AS2 envolve o arquivo em um envelope antes do envio. Portanto, o tamanho do arquivo pode aumentar, mesmo se o arquivo for enviado com compactação. Portanto, certifique-se de que o tamanho máximo do arquivo do parceiro comercial seja maior que o tamanho do arquivo que você está enviando.

1. [Importar certificados AS2](#)
2. [Crie perfis AS2](#)
3. [Crie um servidor AS2](#)
4. [Crie um contrato AS2](#)
5. Crie um conector AS2

Crie um conector AS2

Este procedimento explica como criar conectores AS2 usando o AWS Transfer Family console. Se você quiser usar o AWS CLI em vez disso, consulte [the section called “Etapa 6: criar um conector entre você e seu parceiro”](#).

Para criar um conector AS2

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, escolha Conectores para enviar mensagens, no menu AS2 Trading Partners e, em seguida, escolha Criar conector AS2.
3. Na seção Configuração do conector, especifique as seguintes informações:
 - URL – insira o URL para conexões de saída.
 - Modo de endereçamento IP — Escolha somente IPv4 (padrão) para usar endereços IPv4 exclusivamente ou para oferecer suporte Dual-stack a IPv6 e IPv4. No modo de pilha dupla,

o conector prefere IPv6 quando a resolução DNS retorna resultados IPv6 e usa IPv4 quando somente resultados de DNS IPv4 são retornados.

- Função de acesso — Escolha o Amazon Resource Name (ARN) da função AWS Identity and Access Management (IAM) a ser usada. Assegure que esta função fornece acesso de leitura e gravação ao diretório principal do local do arquivo usado na solicitação do `StartFileTransfer`. Além disso, certifique-se de que a função forneça acesso de leitura e gravação ao diretório pai dos arquivos com os quais você pretende enviar com `StartFileTransfer`.

 Note

Se você estiver usando a autenticação básica para seu conector, a função de acesso exigirá a permissão `secretsmanager:GetSecretValue` para o segredo. Se o segredo for criptografado usando uma chave gerenciada pelo cliente Chave gerenciada pela AWS em vez da chave de entrada AWS Secrets Manager, a função também precisará da `kms:Decrypt` permissão para essa chave. Se você nomear seu segredo com o prefixo `aws/transfer/`, poderá adicionar a permissão necessária com um caractere curinga (*), conforme mostrado em [Exemplo de permissão para criar segredos](#).

- Função de registro (opcional) — Escolha a função do IAM que o conector usará para enviar eventos aos seus CloudWatch registros.
4. Na seção Configuração do AS2, escolha os perfis local e de parceiro, os algoritmos de criptografia e assinatura e se deseja compactar as informações transferidas. Observe o seguinte:
- O Content-Type parâmetro Preserve S3 está ativado por padrão.

Quando definido, o Transfer Family usa o Amazon S3 Content-Type que está associado a objetos no S3 em vez de ter o tipo de conteúdo mapeado com base na extensão do arquivo. Desmarque essa configuração se quiser que o serviço mapeie o tipo de conteúdo para suas mensagens AS2 com base na extensão do arquivo, em vez de usar o tipo de conteúdo do objeto S3.

- Para o algoritmo de criptografia, não escolha, `DES_EDE3_CBC` a menos que você precise oferecer suporte a um cliente antigo que o exija, pois é um algoritmo de criptografia fraco.
- O Assunto é usado como o atributo do cabeçalho `subject` HTTP nas mensagens AS2 que estão sendo enviadas com o conector.

- Se você optar por criar um conector sem um algoritmo de criptografia, deverá especificar HTTPS como seu protocolo.
5. Na seção Autenticação básica, especifique as informações a seguir.
- Para enviar credenciais de login junto com mensagens de saída, selecione Habilitar autenticação básica. Se você não quiser enviar nenhuma credencial com mensagens de saída, mantenha a opção Ativar autenticação básica desmarcada.
 - Se você estiver usando a autenticação, escolha ou crie um segredo.
 - Para criar um novo segredo, escolha Criar um novo segredo e insira um nome de usuário e uma senha. Essas credenciais devem corresponder ao usuário que se conecta ao endpoint do parceiro.

The screenshot shows the 'Basic authentication' configuration section. It includes a checkbox to 'Enable Basic authentication - optional' with a description: 'Select this option to authenticate with your trading partner's host using username and password credentials.' Below this is the 'Basic authentication credentials' section, which has two radio button options: 'Create a new secret' (selected) and 'Choose an existing secret'. Under 'Create a new secret', there are input fields for 'Username' (containing 'test-user') and 'Password' (masked with dots). At the bottom, a light blue information box contains a note: 'Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.'

- Para usar um segredo existente, escolha Escolher um segredo existente, e escolha um segredo no menu suspenso. Para obter detalhes sobre como criar um segredo formatado corretamente no Secrets Manager, consulte [Habilitar a autenticação básica para conectores AS2](#).

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret

☒ Choose an existing secret

Choose a secret

aws/transfer/...
SFTP connector...

aws/transfer/sftp-connector1
Secret key ...

aws/transfer/c...

You must provide AWS Transfer Family with permission to use the secret key.

6. Na seção de configuração do MDN, especifique as seguintes informações:
 - Solicitar MDN: você tem a opção de exigir que seu parceiro comercial envie um MDN a você depois de receber sua mensagem pelo AS2.
 - MDN assinado: você tem a opção de exigir que a assinatura do mDNS. Essa opção estará disponível apenas se você tiver selecionado Solicitar MDN.
7. Depois de confirmar todas as configurações, escolha Criar conector AS2 para criar o conector.

A página Conectores é exibida com o ID do novo conector adicionado à lista. Para visualizar os detalhes de seus conectores, consulte [Exibir detalhes do conector AS2](#).

Algoritmos de conector AS2

Quando você cria um conector AS2, os seguintes algoritmos de segurança são anexados ao conector.

Tipo	Algoritmo
Cifras TLS	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Tipo	Algoritmo
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Autenticação básica para conectores AS2

Ao criar ou atualizar um servidor Transfer Family que usa o protocolo AS2, você pode adicionar a autenticação básica para mensagens de saída. Para isso, adicione informações de autenticação a um conector.

Note

A autenticação básica está disponível somente se você estiver usando HTTPS.

Para usar a autenticação no seu conector, selecione Habilitar autenticação básica na seção Autenticação básica. Depois de ativar a autenticação básica, você pode optar por criar um segredo ou usar um. Em ambos os casos, as credenciais no segredo são enviadas com mensagens de saída que usam esse conector. As credenciais devem corresponder ao usuário que está tentando se conectar ao endpoint remoto do parceiro comercial.

A captura de tela a seguir mostra a opção Ativar autenticação básica selecionada e Criar um novo segredo escolhido. Depois de fazer essas escolhas, você pode inserir um nome de usuário e uma senha para o segredo.

A captura de tela a seguir mostra a opção Ativar autenticação básica selecionada e Escolher um segredo existente escolhido. O seu segredo deve estar no formato correto, como descrito em [Habilitar a autenticação básica para conectores AS2](#).

Habilitar a autenticação básica para conectores AS2

Ao habilitar a autenticação básica para conectores AS2, é possível criar um novo segredo no console Transfer Family ou usar um segredo criado por você em AWS Secrets Manager. Em ambos os casos, seu segredo é armazenado no Secrets Manager.

Tópicos

- [Crie um novo segredo no console](#)
- [Usar um segredo existente da](#)
- [Crie um segredo em AWS Secrets Manager](#)

Crie um novo segredo no console

Ao criar um conector no console, é possível criar um novo segredo.

Para criar um novo segredo, escolha Criar um novo segredo e insira um nome de usuário e uma senha. Essas credenciais devem corresponder ao usuário que se conecta ao endpoint do parceiro.

Basic authentication Info
☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials Info
Choose the username and password credentials that will be used to authenticate with your trading partner's host.
☒ Create a new secret
☐ Choose an existing secret

Username

Password

 Update the [access role associated with your connector](#)  to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

Note

Quando você cria um novo segredo no console, o nome do segredo segue esta convenção de nomenclatura: `/aws/transfer/connector-id`, onde **connector-id** está o ID do

conector que você está criando. Considere isso quando estiver tentando localizar o segredo AWS Secrets Manager.

Usar um segredo existente da

Ao criar um conector no console, é possível especificar um segredo existente.

Para usar um segredo existente, escolha *Escolher um segredo existente*, e escolha um segredo no menu suspenso. Para obter detalhes sobre como criar um segredo formatado corretamente no Secrets Manager, consulte [Crie um segredo em AWS Secrets Manager](#).

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret

☒ Choose an existing secret

Choose a secret

- aws/transfer/...
SFTP connector...
- aws/transfer/sftp-connector1
Secret key ...
- aws/transfer/c-...

Crie um segredo em AWS Secrets Manager

O procedimento a seguir descreve como criar um segredo apropriado para uso com o conector AS2.

Note

A autenticação básica está disponível somente se você estiver usando HTTPS.

Para armazenar credenciais de usuário no Secrets Manager para autenticação AS2 Basic

1. Faça login no Console de gerenciamento da AWS e abra o AWS Secrets Manager console em <https://console.aws.amazon.com/secretsmanager/>.

2. No painel de navegação à esquerda, selecione Segredos.
3. Na página Segredos, escolha Armazenar um novo segredo.
4. Na página Escolher tipo de segredo, em Tipo de segredo, escolha Outro tipo de segredo.
5. Na seção Key/value de pares, escolha a Key/valueguia.
 - Chave — Insira **Username**.
 - Valor – insira o nome do usuário autorizado a se conectar ao servidor do parceiro.
6. Se você quiser fornecer uma senha, escolha Adicionar linha e, na seção de Key/value pares, escolha a Key/valueguia.

Escolha Adicionar linha e, na seção Key/value de pares, escolha a Key/valueguia.

- Chave — Insira **Password**.
 - valor – Insira uma senha para o usuário.
7. Se você quiser fornecer uma chave privada, escolha Adicionar linha e, na seção de Key/value pares, escolha a Key/valueguia.
 - Chave — Insira **PrivateKey**.
 - valor — insira uma chave privada para o usuário. Esse valor deve ser armazenado no formato OpenSSH e deve corresponder à chave pública armazenada para esse usuário no servidor remoto.
 8. Escolha Próximo.
 9. Na página Configurar segredo, insira um nome e uma descrição para seu segredo. Recomendamos utilizar o prefixo **aws/transfer/** para o nome. Por exemplo, é possível dar ao seu segredo o nome de **aws/transfer/connector-1**.
 10. Escolha Próximo e aceite os padrões na página Configurar alternância. Em seguida, escolha Próximo.
 11. Na página Revisão, escolha Armazenar para criar e armazenar o segredo.

Depois de criar o segredo, é possível escolhê-lo ao criar um conector (consulte [Configurar conectores AS2](#)). Na etapa em que você habilita a autenticação básica, escolha o segredo na lista suspensa de segredos disponíveis.

Exibir detalhes do conector AS2

Você pode encontrar uma lista de detalhes e propriedades de um AWS Transfer Family conector AS2 no AWS Transfer Family console. As propriedades de um conector AS2 incluem URL, funções, perfis, MDNs, tags e métricas de monitoramento.

Esse é o procedimento para visualizar os detalhes do conector.

Como visualizar detalhes do conector

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerda, escolha Conectores.
3. Escolha o identificador na coluna ID do conector para ver a página de detalhes do conector selecionado.

Você pode alterar as propriedades do conector AS2 na página de detalhes do conector escolhendo Editar.

The screenshot displays the AWS Transfer Family console interface for an AS2 connector. At the top, there's a breadcrumb 'C-' followed by a redacted ID and a 'Delete' button. Below this, the 'Connector configuration' section includes an 'Info' link and an 'Edit' button. It lists the 'Name' as 'my-as2-connector' and the 'URL' as 'https://www.example.com'. It also shows the 'Access role' as a redacted role and the 'Logging role' as 'AWSTransferLoggingAccess'. The 'Communication settings' section shows 'AS2-From header' and 'AS2-To header' as redacted. The 'AS2 configuration' section includes an 'Info' link, an 'Edit' button, and settings for 'Local profile' (redacted), 'Partner profile' (redacted), 'Preserve S3 Content-Type' (Enabled), 'Compression' (Enabled), 'Message Subject' (View), 'Encryption algorithm' (AES128_CBC), and 'Signing algorithm' (SHA384). The 'MDN configuration' section includes an 'Info' link, an 'Edit' button, and settings for 'Request MDN' (Enabled), 'Signed MDN' (Default to message signing algorithm: SHA384), and 'Synchronization' (Enabled).

Connector configuration Info Edit

Name
my-as2-connector

URL
<https://www.example.com>

Access role
[Redacted]

Logging role
AWSTransferLoggingAccess

Communication settings Info

AS2-From header
[Redacted]

AS2-To header
[Redacted]

AS2 configuration Info Edit

Local profile
[Redacted]

Partner profile
[Redacted]

Preserve S3 Content-Type
Enabled

Compression
Enabled

Message Subject
View

Encryption algorithm
AES128_CBC

Signing algorithm
SHA384

MDN configuration Info Edit

Request MDN
Enabled

Signed MDN
Default to message signing algorithm: SHA384

Synchronization
Enabled

Basic authentication [Info](#)[Edit](#)**Basic authentication**

✓ Enabled

Secretaws/transfer/c- [REDACTED] [Copy](#)**Egress IP details** [Info](#)

Service managed static IP addresses of this connector

[Copy](#) 23.23.130.9[Copy](#) 44.196.109.11[Copy](#) 3.219.16.7**Tags (1)**[Manage tags](#)

Use tags to organize, search, and filter your Connectors. We recommend adding a tag with 'Name' as the key and a unique string as the value to easily identify your Connector.

< 1 >

Key	Value
Name	my-as2-connector

AS2 Monitoring

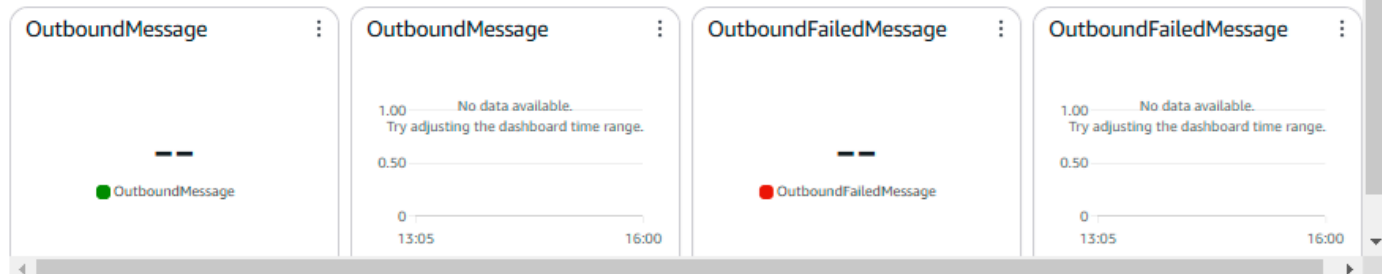
3h

1d

1w

[Calendar](#)

UTC timezone

[Refresh](#)[Filter](#)[More](#)**Note**

Você pode obter muitas dessas informações, embora em um formato diferente, executando o seguinte comando AWS Command Line Interface (AWS CLI) :

```
aws transfer describe-connector --connector-id your-connector-id
```

Para obter mais informações, consulte [DescribeConnector](#) na Referência da API.

Enviando e recebendo mensagens AS2

Esta seção descreve os processos para enviar e receber mensagens AS2. Ele também fornece detalhes sobre nomes de arquivos e locais associados às mensagens AS2.

A tabela a seguir lista os algoritmos de criptografia disponíveis para mensagens AS2 e quando você pode usá-los.

Algoritmo de criptografia	HTTP	HTTPS	Observações
AES128_CBC	Sim	Sim	
AES192_CBC	Sim	Sim	
AES256_CBC	Sim	Sim	
DES_EDE3_CBC	Sim	Sim	Use esse algoritmo somente se precisar oferecer suporte a um cliente antigo que o exija, pois é um algoritmo de criptografia fraco.
NONE	Não	Sim	Se você estiver enviando mensagens para um servidor Transfer Family, só poderá selecionar NONE se estiver usando um Application Load Balancer (ALB).

Tópicos

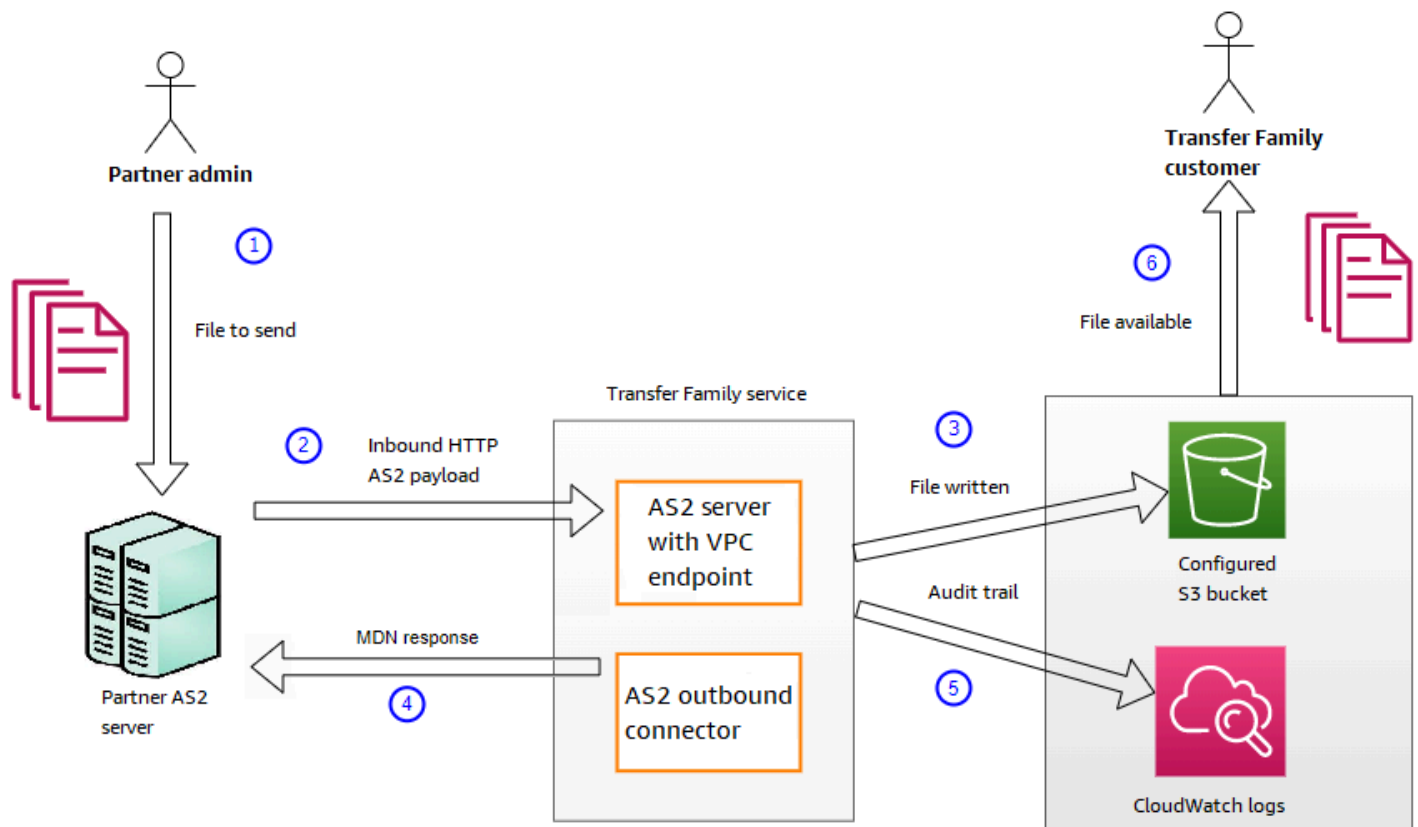
- [Processo de recebimento de mensagens AS2](#)

- [Enviando e recebendo mensagens AS2 por HTTPS](#)
- [Transferindo arquivos usando um conector AS2](#)
- [Nomes e localizações dos arquivos](#)
- [Códigos de status](#)
- [Arquivos JSON de amostra](#)

Processo de recebimento de mensagens AS2

O processo de entrada é definido como uma mensagem ou arquivo que está sendo transferido para o seu AWS Transfer Family servidor. A sequência das mensagens de entrada é a seguinte:

1. Um processo administrativo ou automatizado inicia uma Transferência de Arquivos AS2 no servidor AS2 remoto do parceiro.
2. O servidor AS2 remoto do parceiro assina e criptografa o conteúdo do arquivo e, em seguida, envia uma solicitação HTTP POST para um endpoint de entrada AS2 hospedado no Transfer Family.
3. Usando os valores configurados para o servidor, parceiros, certificados e contrato, o Transfer Family descriptografa e verifica a carga do AS2. O conteúdo do arquivo é armazenado no armazenamento de arquivos configurado do Amazon S3.
4. A resposta MDN assinada é retornada em linha com a resposta HTTP ou de forma assíncrona por meio de uma solicitação HTTP POST separada para o servidor de origem.
5. Uma trilha de auditoria é escrita para a Amazon CloudWatch com detalhes sobre a troca.
6. O arquivo descriptografado está disponível em uma pasta chamada `inbox/processed`.



Enviando e recebendo mensagens AS2 por HTTPS

Esta seção descreve como configurar um servidor Transfer Family que usa o protocolo AS2 para enviar e receber mensagens por HTTPS.

Tópicos

- [Envie mensagens AS2 por HTTPS](#)
- [Receba mensagens AS2 por HTTPS](#)

Envie mensagens AS2 por HTTPS

Para enviar mensagens AS2 usando HTTPS, crie um conector com as seguintes informações:

- Para o URL, especifique um URL HTTPS
- Para o algoritmo de criptografia, selecione qualquer um dos algoritmos disponíveis.

 Note

Para enviar mensagens para um servidor Transfer Family sem usar criptografia (ou seja, você seleciona o algoritmo NONE de criptografia), você deve usar um Application Load Balancer (ALB).

- Forneça os valores restantes para o conector, conforme descrito em [Configurar conectores AS2](#).

Receba mensagens AS2 por HTTPS

AWS Transfer Family Atualmente, os servidores AS2 fornecem apenas transporte HTTP pela porta 5080. No entanto, você pode encerrar o TLS em um balanceador de carga de rede ou aplicativo na frente do endpoint VPC do servidor Transfer Family usando uma porta e um certificado de sua escolha. Com essa abordagem, você pode fazer com que as mensagens AS2 recebidas usem HTTPS.

Pré-requisitos

- O VPC deve estar na mesma Região da AWS do servidor do Transfer Family.
- As sub-redes da sua VPC devem estar dentro das zonas de disponibilidade nas quais você deseja usar o servidor.

 Note

Cada servidor Transfer Family pode suportar até três zonas de disponibilidade.

- Aloque até três endereços IP Elastic na mesma região do seu servidor. Ou você pode optar por trazer seu próprio intervalo de endereços IP (BYOIP).

 Note

O número de endereços IP elásticos deve corresponder ao número de zonas de disponibilidade que você usa com os endpoints do servidor.

Você pode configurar um Network Load Balance (NLB) ou um Application Load Balancer (ALB). A tabela a seguir lista os prós e os contras de cada abordagem.

A tabela abaixo fornece as diferenças nos recursos quando você usa um NLB versus um ALB para encerrar o TLS.

Recurso	Network Load Balancer (NLB)	Application Load Balancer (ALB)
Latência	Menor latência à medida que opera na camada de rede.	Maior latência à medida que opera na camada do aplicativo.
Compatibilidade com IP estático	Pode anexar endereços IP elásticos que podem ser estáticos.	Não é possível anexar endereços IP elásticos: fornece um domínio cujos endereços IP subjacentes podem mudar.
Roteamento avançado	Não suporta roteamento avançado.	Suporta roteamento avançado. Pode injetar o X-Forwarded-Proto cabeçalho necessário para AS2 sem criptografia. Esse cabeçalho está descrito X-Forwarded-Proto no site developer.mozilla.org .
TLS/SSL rescisão	Suporta TLS/SSL rescisão	Suporta TLS/SSL rescisão
TLS mútua (mTLS)	Atualmente, o Transfer Family não suporta o uso de um NLB para mTLS	Support para mTLS

Configure NLB

Este procedimento descreve como configurar um Network Load Balancer (NLB) voltado para a Internet em sua VPC.

Para criar um Network Load Balancer e definir o endpoint da VPC do servidor como o destino do balanceador de carga

1. Abra o console do Amazon Elastic Compute Cloud em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Balanceadores de carga e, em seguida, escolha Criar balanceador de carga.
3. Em Network Load Balancer, escolha Criar.
4. Na seção Configurações básicas, insira as seguintes informações:
 - Em Nome, insira um nome descritivo para o balanceador de carga.
 - Para Esquema, escolha Internet-facing.
 - Em Tipo de endereço IP, selecione IPv4.
5. Na seção Mapeamento de rede, insira as seguintes informações:
 - Em VPC, escolha a nuvem privada virtual (VPC) que você criou.
 - Em Mapeamentos, escolha as zonas de disponibilidade associadas às sub-redes públicas que estão disponíveis na mesma VPC que você usa com os endpoints do servidor.
 - Para o endereço IPv4 de cada sub-rede, escolha um dos endereços IP elásticos alocados.
6. Na seção Receptores e roteamento, insira as seguintes informações:
 - Para Protocolos, escolha TLS.
 - Em Porta, insira **5080**.
 - Em Ação padrão, escolha Criar grupo de destino. Para obter detalhes sobre a criação de um novo grupo-alvo, consulte [Para criar um grupo de destino](#).

Depois de criar um grupo-alvo, insira seu nome no campo Ação padrão.

7. Na seção Configurações do ouvinte seguro, escolha seu certificado na área SSL/TLS Certificado padrão.
8. Escolha Criar balanceador de carga para criar seu NLB.
9. (Opcional, mas recomendado) Ative os logs de acesso do Network Load Balancer para manter uma trilha de auditoria completa, conforme descrito em [Logs de acesso do Network Load Balancer](#).

Recomendamos esta etapa porque a conexão TLS é encerrada no NLB. Portanto, o endereço IP de origem refletido nos grupos de CloudWatch log AS2 do Transfer Family é o endereço IP privado do NLB, em vez do endereço IP externo do seu parceiro comercial.

Configure ALB

Este procedimento descreve como configurar um Application Load Balancer (ALB) em sua VPC.

Para criar um Application Load Balancer e definir o VPC endpoint do servidor como destino do balanceador de carga

1. Abra o console do Amazon Elastic Compute Cloud em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Balanceadores de carga e, em seguida, escolha Criar balanceador de carga.
3. Em Application Load Balancer, escolha Create (Criar).
4. No console do ALB, crie um novo ouvinte HTTP na porta 443 (HTTPS).
5. (Opcional). Se você quiser configurar a autenticação mútua (mTLS), defina as configurações de segurança e um armazenamento confiável.
 - a. Anexe seu SSL/TLS certificado ao ouvinte.
 - b. Em Tratamento de certificados do cliente, selecione Autenticação mútua (mTLS).
 - c. Escolha Verificar com um repositório confiável.
 - d. Em Configurações avançadas do mTLS, escolha ou crie um repositório confiável fazendo o upload de seus certificados CA.
6. Crie um novo grupo-alvo e adicione os endereços IP privados dos endpoints do servidor Transfer Family AS2 como destinos na porta 5080. Para obter detalhes sobre a criação de um novo grupo-alvo, consulte [Para criar um grupo de destino](#).
7. Configure verificações de saúde para que o grupo-alvo use o protocolo HTTP na porta 5080.
8. Crie uma nova regra para encaminhar o tráfego HTTPS do ouvinte para o grupo-alvo.
9. Configure o ouvinte para usar seu SSL/TLS certificado.

Depois de configurar o balanceador de carga, os clientes se comunicam com o balanceador de carga por meio do receptor de porta personalizado. Em seguida, o balanceador de carga se comunica com o servidor pela porta 5080.

Para criar um grupo de destino

1. Depois de escolher Criar grupo-alvo no procedimento anterior, você será direcionado para a página Especificar detalhes do grupo de destino para um novo grupo-alvo.

2. Na seção Configurações básicas, insira as seguintes informações.

- Em Escolher um tipo de destino, escolha Endereços IP.
- Em Nome do grupo de destino, insira um nome para o grupo de destino.
- Para Protocolo, sua seleção depende de você estar usando um ALB ou um NLB.
 - Para um Network Load Balancer (NLB), escolha TCP
 - Para um Application Load Balancer (ALB), escolha HTTP
- Em Porta, insira **5080**.
- Em Tipo de endereço IP, selecione IPv4.
- Em VPC, escolha a VPC criada para o servidor Transfer Family AS2.

3. Na seção Verificações de saúde, escolha o protocolo de verificação de saúde.

- Para um ALB, escolha HTTP
- Para um NLB, escolha TCP

4. Escolha Próximo.

5. Na página Registrar alvos, insira as seguintes informações:

- Em Rede, confirme se a VPC que você criou para o servidor Transfer Family AS2 foi especificada.
- Para o endereço IPv4, insira o endereço IPv4 privado dos endpoints do servidor Transfer Family AS2.

Se você tiver mais de um endpoint para seu servidor, escolha Adicionar endereço IPv4 para adicionar outra linha para inserir outro endereço IPv4. Repita esse processo até inserir os endereços IP privados de todos os endpoints do seu servidor.

- Verifique se as portas estão definidas como **5080**.
- Escolha Incluir como pendente abaixo para adicionar suas entradas à seção Revisar metas.

6. Na seção Revisar alvos, revise seus alvos IP.

7. Escolha Criar grupo-alvo e, em seguida, volte ao procedimento anterior para criar seu NLB e insira o novo grupo-alvo onde indicado.

Teste o acesso ao servidor a partir de um endereço IP elástico

Conecte-se ao servidor pela porta personalizada usando um endereço IP elástico ou o nome DNS do Network Load Balancer.

Important

Gerencie o acesso ao seu servidor a partir de endereços IP do cliente usando as [listas de controle de acesso à rede \(ACL da rede\)](#) para as sub-redes configuradas no balanceador de carga. As permissões da Network ACL são definidas no nível da sub-rede, portanto, as regras se aplicam a todos os recursos que usam a sub-rede. Não é possível controlar o acesso de endereços IP de clientes usando grupos de segurança, porque o tipo de destino do balanceador de carga é definido como endereços IP em vez de Instâncias. Portanto, o balanceador de carga não preserva endereços IP de origem. Se as [verificações de integridade do Network Load Balancer](#) falharem, isso significa que o balanceador de carga não pode se conectar ao endpoint do servidor. Para solucionar esse problema, verifique o seguinte:

- Confirme se o [grupo de segurança associado ao endpoint](#) do servidor permite conexões de entrada das sub-redes configuradas no balanceador de carga. O balanceador de carga deve ser capaz de se conectar ao endpoint do servidor pela porta 5080.
- Confirme se o estado do servidor está online.

Transferindo arquivos usando um conector AS2

Os conectores AS2 estabelecem um relacionamento entre parceiros comerciais para transferências de mensagens AS2 de um servidor Transfer Family para um destino externo de propriedade do parceiro.

Você pode usar o Transfer Family para enviar mensagens AS2 referenciando o ID do conector e os caminhos para os arquivos, conforme ilustrado no seguinte comando `start-file-transfer` AWS Command Line Interface (AWS CLI):

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \  
--send-file-paths "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-source-  
bucket/myfile2.txt"
```

Para obter detalhes dos conectores, execute o seguinte comando:

```
aws transfer list-connectors
```

O comando `list-connectors` retorna os IDs do conector, os URLs e nomes do recurso da Amazon (ARNs) dos seus conectores.

Para retornar as propriedades de um conector específico, execute o comando a seguir com o ID que você deseja usar:

```
aws transfer describe-connector --connector-id your-connector-id
```

O comando `describe-connector` retorna todas as propriedades do conector, incluindo URL, funções, perfis, avisos de disposição de mensagens (MDNs), tags e métricas de monitoramento.

Você pode confirmar que o parceiro recebeu os arquivos com êxito visualizando os arquivos JSON e MDN. Esses arquivos são nomeados de acordo com as convenções descritas em [Nomes e localizações dos arquivos](#). Se você configurou uma função de registro ao criar o conector, também poderá verificar seus CloudWatch registros quanto ao status das mensagens AS2.

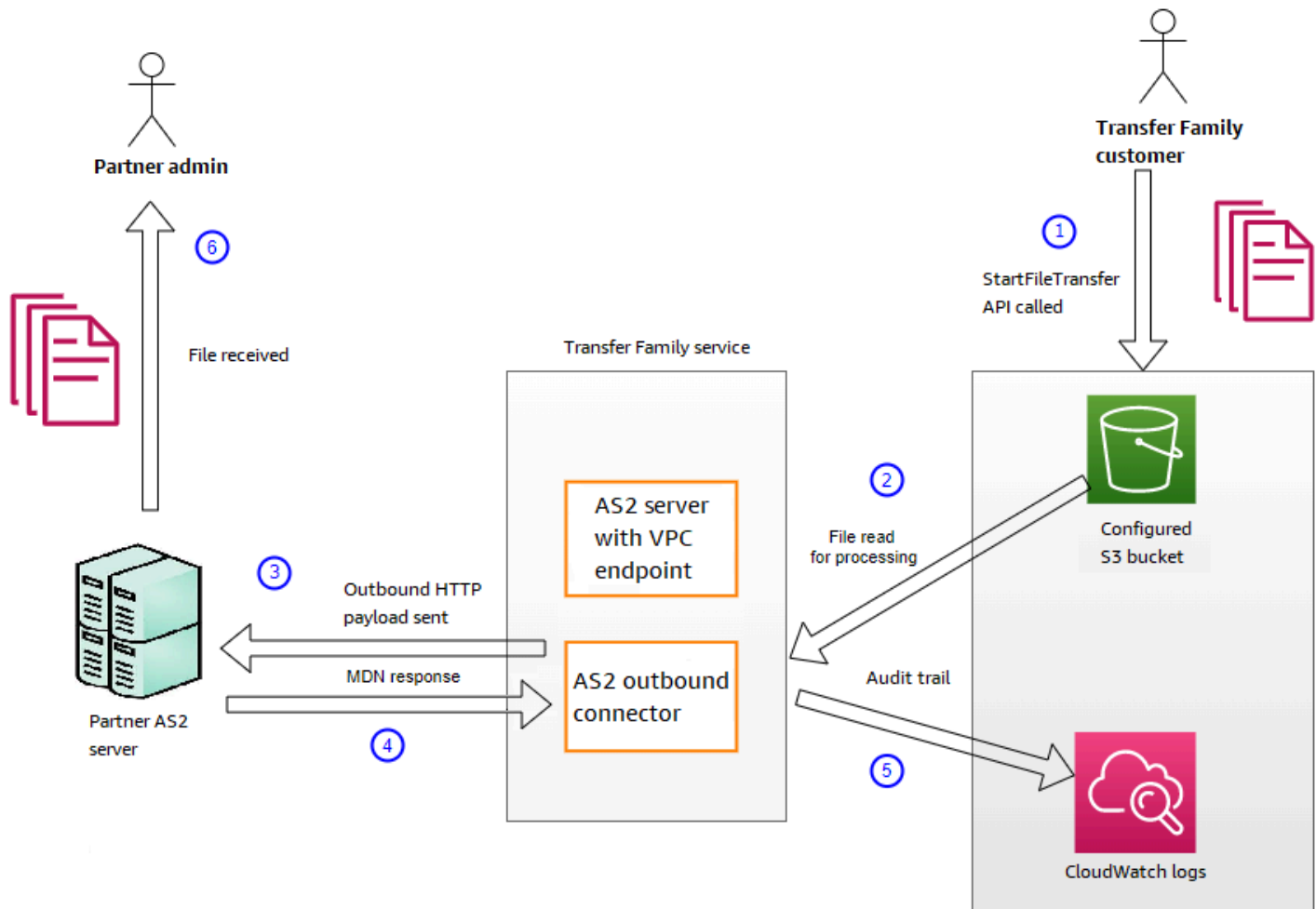
Para ver os detalhes do conector AS2, consulte [Exibir detalhes do conector AS2](#). Para obter mais informações sobre como criar conectores AS2, consulte [Configurar conectores AS2](#).

Para enviar uma mensagem de saída AS2

O processo de saída é definido como uma mensagem ou arquivo enviado AWS para um cliente ou serviço externo. A sequência das mensagens de saída é a seguinte:

1. Um administrador chama o comando `start-file-transfer` AWS Command Line Interface (AWS CLI) ou a operação `StartFileTransfer` da API. Essa operação faz referência a uma configuração `connector`.
2. O Transfer Family detecta uma nova solicitação de arquivo e localiza o arquivo. O arquivo é compactado, assinado e criptografado.
3. Um cliente HTTP de transferência executa uma solicitação HTTP POST para transmitir a carga para o servidor AS2 do parceiro.
4. O processo retorna a resposta MDN assinada, em linha com a resposta HTTP (MDN síncrona ou assíncrona).
5. À medida que o arquivo se move entre os diferentes estágios de transmissão, o processo entrega o recibo da resposta do MDN e os detalhes do processamento ao cliente.

6. O servidor AS2 remoto disponibiliza o arquivo descryptografado e verificado para o administrador parceiro.



O processamento AS2 suporta muitos dos protocolos RFC 4130, com foco em casos de uso comuns e integração com implementações de servidores existentes AS2-enabled . Para obter detalhes sobre as configurações suportadas, consulte [Configurações AS2](#).

Nomes e localizações dos arquivos

Esta seção discute as convenções de nomenclatura de arquivos para transferências AS2.

Para Transferência de Arquivos de entrada, observe o seguinte:

- Você especifica o diretório base em um contrato. O diretório base é o nome do bucket do Amazon S3 combinado com um prefixo, se houver. Por exemplo, `./amzn-s3-demo-bucket/AS2-folder`

- Se um arquivo de entrada for processado com êxito, o arquivo (e o arquivo JSON correspondente) será salvo na pasta /processed. Por exemplo, `./amzn-s3-demo-bucket/AS2-folder/processed`

O arquivo JSON contém os seguintes campos:

- agreement-id
 - as2-from
 - as2-to
 - as2-message-id
 - transfer-id
 - client-ip
 - connector-id
 - failure-message
 - file-path
 - message-subject
 - mdn-message-id
 - mdn-subject
 - requester-file-name
 - requester-content-type
 - server-id
 - status-code
 - failure-code
 - transfer-size
- Se um arquivo de entrada não puder ser processado com êxito, o arquivo (e o arquivo JSON correspondente) será salvo na pasta /failed. Por exemplo, `./amzn-s3-demo-bucket/AS2-folder/failed`
 - O arquivo transferido é armazenado na pasta processed como `original_filename.messageId.original_extension`. Ou seja, o ID da mensagem para a transferência é anexado ao nome do arquivo, antes da extensão original.
 - Um arquivo JSON é criado e salvo como `original_filename.messageId.original_extension.json`. Além do ID da mensagem que está sendo adicionado, a string `.json` é anexada ao nome do arquivo transferido.

- Um arquivo de Aviso de Disposição de Mensagens (MDN) é criado e salvo como *original_filename.messageId.original_extension.mdn*. Além do ID da mensagem que está sendo adicionado, a string .mdn é anexada ao nome do arquivo transferido.
- Se houver um arquivo de entrada chamado `ExampleFileInS3Payload.dat`, os seguintes arquivos serão criados:
 - Arquivo –
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
 - JSON –
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
 - MDN –
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`

Para transferências de saída, a nomenclatura é semelhante, com a diferença de que não há arquivo de mensagem de entrada e, além disso, a ID de transferência da mensagem transferida é adicionada ao nome do arquivo. O ID de transferência é retornado pela operação API `StartFileTransfer` (ou quando outro processo ou script chama essa operação).

- O `transfer-id` é um identificador associado a uma Transferência de Arquivos. Todas as solicitações que fazem parte de uma `StartFileTransfer` chamada compartilham um `transfer-id`.
- O diretório base é o mesmo que o caminho que você usa para o arquivo de origem. Ou seja, o diretório base é o caminho que você especifica na operação ou no `start-file-transfer` AWS CLI comando da `StartFileTransfer` API. Por exemplo:

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-bucket/AS2-folder/  
file-to-send.txt
```

Se você executar esse comando, os arquivos MDN e JSON serão salvos em `/amzn-s3-demo-bucket/AS2-folder/processed` (para transferências bem-sucedidas) ou `/amzn-s3-demo-bucket/AS2-folder/failed` (para transferências malsucedidas).

- Um arquivo JSON é criado e salvo como *original_filename.transferId.messageId.original_extension.json*.
- Um arquivo MDN é criado e salvo como *original_filename.transferId.messageId.original_extension.mdn*.

- Se houver um arquivo de saída chamado `ExampleFileOutTestOutboundSyncMdn.dat`, os seguintes arquivos serão criados:
 - JSON – `ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.json`
 - MDN – `ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.mdn`

Você também pode verificar os CloudWatch registros para ver os detalhes de suas transferências, incluindo as que falharam.

Códigos de status

A tabela a seguir lista todos os códigos de status que podem ser registrados nos CloudWatch registros quando você ou seu parceiro enviam uma mensagem AS2. Diferentes etapas de processamento de mensagens se aplicam a diferentes tipos de mensagens e são destinadas somente ao monitoramento. Os estados COMPLETED e FAILED representam a etapa final do processamento e são visíveis nos arquivos JSON.

Código	Description	Processamento concluído?
PROCESSANDO	A mensagem está sendo convertida em seu formato final. Por exemplo, as etapas de descompressão e descrição têm esse status.	Não
MDN_TRANSMITEM	O processamento de mensagens está enviando uma resposta MDN.	Não
MDN_RECEIVE	O processamento de mensagens está recebendo uma resposta MDN.	Não
CONCLUÍDO	O processamento da mensagem foi concluído com êxito. Esse estado inclui	Sim

Código	Description	Processamento concluído?
	quando um MDN é enviado para uma mensagem de entrada ou para verificação de mensagens enviadas pelo MDN.	
FAILED	O processamento da mensagem falhou. Para obter uma lista de códigos de erro, consulte Códigos de erro AS2 .	Sim

Arquivos JSON de amostra

Esta seção lista exemplos de arquivos JSON para transferências de entrada e saída, incluindo arquivos de amostra para transferências bem-sucedidas e transferências que falham.

Exemplo de arquivo de saída que foi transferido com sucesso:

```
{
  "requester-content-type": "application/octet-stream",
  "message-subject": "File xyzTest from MyCompany_OID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_OID",
  "connector-id": "c-c21c63ceaaf34d99b",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 3198,
  "mdn-message-id": "OPENAS2-11072022063009+0000-df865189-1450-435b-9b8d-d8bc0cee97fd@PartnerA_OID_MyCompany_OID",
  "mdn-subject": "Message be18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa has been accepted",
  "as2-to": "PartnerA_OID",
  "transfer-id": "dedf4601-4e90-4043-b16b-579af35e0d83",
  "file-path": "/amzn-s3-demo-bucket/as2testcell10000/openAs2/TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa",
  "timestamp": "2022-07-11T06:30:10.791274Z"
}
```

Exemplo de arquivo de saída que foi transferido sem sucesso:

```
{
  "failure-code": "HTTP_ERROR_RESPONSE_FROM_PARTNER",
  "status-code": "FAILED",
  "requester-content-type": "application/octet-stream",
  "subject": "Test run from Id da86e74d6e57464aae1a55b8596bad0a to partner
9f8474d7714e476e8a46ce8c93a48c6c",
  "transfer-size": 3198,
  "requester-file-name": "openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "as2-message-id": "9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "failure-message": "http://Test123456789.us-east-1.elb.amazonaws.com:10080 returned
status 500 for message with ID 9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "transfer-id": "07bd3e07-a652-4cc6-9412-73ffdb97ab92",
  "connector-id": "c-056e15cc851f4b2e9",
  "file-path": "/amzn-s3-demo-bucket-4c1tq6ohjt9y/as2IntegCell10002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "timestamp": "2022-07-11T21:17:24.802378Z"
}
```

Exemplo de arquivo de entrada que foi transferido com sucesso:

```
{
  "requester-content-type": "application/EDI-X12",
  "subject": "File openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat sent from MyCompany
to PartnerA",
  "client-ip": "10.0.109.105",
  "requester-file-name": "openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat",
  "as2-from": "MyCompany_OID",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 1050,
  "mdn-subject": "Message Disposition Notification",
  "as2-message-id": "OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID",
  "as2-to": "PartnerA_OID",
  "agreement-id": "a-f5c5cbea5f7741988",
  "file-path": "processed/openAs2TestInboundAsyncMdn-
necco-5Ab6bTfC0.OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID.dat",
  "server-id": "s-5f7422b04c2447ef9",
  "timestamp": "2022-07-11T23:36:36.105030Z"
}
```

Exemplo de arquivo de entrada que foi transferido sem sucesso:

```
{
  "failure-code": "INVALID_REQUEST",
  "status-code": "FAILED",
  "subject": "Sending a request from InboundHttpClientTests",
  "client-ip": "10.0.117.27",
  "as2-message-id": "testFailedLogs-TestRunConfig-Default-inbound-direct-
integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "as2-to": "0beff6af56c548f28b0e78841dce44f9",
  "failure-message": "Unsupported date format: 2022/123/456T",
  "agreement-id": "a-0ceec8ca0a3348d6a",
  "as2-from": "ab91a398aed0422d9dd1362710213880",
  "file-path": "failed/01187f15-523c-43ac-9fd6-51b5ad2b08f3.testFailedLogs-
TestRunConfig-Default-inbound-direct-integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "server-id": "s-0582af12e44540b9b",
  "timestamp": "2022-07-11T06:30:03.662939Z"
}
```

Personalize cabeçalhos HTTP para mensagens AS2

Ao enviar mensagens AS2 para parceiros comerciais, talvez seja necessário personalizar os cabeçalhos HTTP para atender a requisitos específicos ou aprimorar a compatibilidade com a configuração do servidor AS2 do seu parceiro. Esse CloudFormation modelo cria uma infraestrutura para habilitar cabeçalhos HTTP personalizados para mensagens AS2 enviadas. AWS Transfer Family Ele configura um Amazon API Gateway e uma função Lambda para atuar como proxy, permitindo a modificação dinâmica dos cabeçalhos exigidos pelos servidores AS2 dos parceiros comerciais.

Use esse modelo para fazer o seguinte:

- Adicione cabeçalhos HTTP personalizados às mensagens AS2 de saída
- Substituir valores de cabeçalho padrão por valores personalizados

Important

Tenha cuidado ao substituir os valores de cabeçalho padrão, pois isso pode causar falhas no envio: alguns cabeçalhos AS2 são necessários.

- Garanta a compatibilidade com parceiros comerciais que tenham requisitos específicos de cabeçalho

Visão geral do modelo

O modelo cria os seguintes componentes principais:

- Uma função Lambda que processa e encaminha mensagens AS2
- Um Amazon API Gateway para expor a função Lambda
- Funções e permissões do IAM para a função Lambda
- Recursos condicionais para suporte a HTTPS

O arquivo de modelo está disponível aqui: [Modelo de cabeçalhos HTTP dinâmicos](#).

Como funciona

1. O Amazon API Gateway recebe mensagens AS2 recebidas de AWS Transfer Family
2. A solicitação é encaminhada para a função Lambda.
3. A função Lambda processa a solicitação, adicionando ou modificando cabeçalhos conforme necessário.
4. A solicitação modificada é então encaminhada para o servidor AS2 do parceiro.
5. A resposta do servidor do parceiro é retornada por meio do Lambda e do Amazon API Gateway para AWS Transfer Family

Recursos principais

- Modificação dinâmica do cabeçalho: permite a personalização do cabeçalho do assunto e a adição de outros cabeçalhos necessários.
- Protocol Support: funciona com os protocolos HTTP e HTTPS.
- Configuração flexível: permite a especificação do host, porta e caminho do parceiro.

Detalhes da implantação

O modelo implementa os seguintes componentes principais:

Função do Lambda

O núcleo da solução é uma função Node.js Lambda que:

- Recebe solicitações do Amazon API Gateway
- Modifica os cabeçalhos com base na configuração e nos dados da solicitação recebida
- Encaminha a solicitação modificada para o servidor AS2 do parceiro
- Lida com os protocolos HTTP e HTTPS
- Inclui tratamento e registro de erros

Amazon API Gateway

Uma API HTTP está configurada para:

- Receba mensagens AS2 recebidas
- Encaminhe solicitações para a função Lambda
- Retorne as respostas para AWS Transfer Family

Parâmetros do modelo

Insira as informações para os parâmetros do modelo da seguinte forma. Observe que todos esses parâmetros são cadeias de caracteres.

- `Environment`: esse parâmetro é usado para nomear os recursos que o modelo cria: se eles são destinados a um ambiente de desenvolvimento ou produção. Os valores válidos são `dev` e `prod`.
- `PartnerHost`: o endereço IP ou nome do host do servidor parceiro AS2.
- `PartnerPort`: o número da porta do servidor parceiro AS2. Se não for especificado, o padrão é 80 para HTTP e 443 para HTTPS.
- `PartnerPath`: o caminho para o endpoint AS2 no servidor parceiro
- `ProtocolType`: o protocolo a ser usado para a comunicação AS2: os valores válidos são HTTP e HTTPS.

Recursos condicionais

Para suporte a HTTPS, o modelo cria condicionalmente:

- Uma camada Lambda para certificados CA
- HTTPS-specific configuração na função Lambda

Implantação e uso

Para personalizar cabeçalhos HTTP AS2 usando um modelo CloudFormation

1. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. No painel de navegação à esquerda, selecione Pilhas.
3. Selecione Criar pilha e, depois, Com novos recursos (padrão).
4. Na seção Pré-requisito - Preparar modelo, escolha Escolher um modelo existente.
5. Copie esse link, [modelo de cabeçalhos HTTP dinâmicos](#), e cole-o no campo URL do Amazon S3.
6. Escolha Próximo.
7. Preencha os detalhes do parâmetro com suas informações. Eles estão detalhados em [Parâmetros do modelo](#).
8. Escolha Próximo. Na página Configurar opções de pilha, selecione Próximo novamente.
9. Revise os detalhes da pilha que você está criando e escolha Criar pilha.

Note

Na parte inferior da página, em Capacidades, você deve reconhecer que isso CloudFormation pode criar recursos AWS Identity and Access Management (IAM).

Depois de implantar essa CloudFormation pilha:

1. Observe a URL do endpoint do Amazon API Gateway fornecida nas saídas da pilha.
2. Atualize seu AWS Transfer Family conector existente para usar esse novo endpoint do Amazon API Gateway.
3. A solução agora manipulará mensagens AS2, adicionando ou modificando cabeçalhos conforme configurado.

 Warning

Modifique apenas o cabeçalho do assunto ou adicione cabeçalhos que seu parceiro espera explicitamente. Alterar outros cabeçalhos pode causar falhas na transferência.

Monitoramento do uso do AS2

Você pode monitorar a atividade do AS2 usando a Amazon CloudWatch e AWS CloudTrail. Para ver outras métricas do servidor Transfer Family, consulte [CloudWatch Registro na Amazon para AWS Transfer Family servidores](#).

Métricas AS2

Métrica	Description
InboundMessage	O número total de mensagens AS2 recebidas com êxito de um parceiro comercial. Unidades: contagem Período: 5 minutos
InboundFailedMessage	O número total de mensagens AS2 que não foram recebidas com êxito de um parceiro comercial. Ou seja, um parceiro comercial enviou uma mensagem, mas o servidor Transfer Family não conseguiu processá-la com êxito. Unidades: contagem Período: 5 minutos
OutboundMessage	O número total de mensagens AS2 enviadas com sucesso do servidor Transfer Family para um parceiro comercial. Unidades: contagem

Métrica	Description
	Período: 5 minutos
OutboundFailedMessage	O número total de mensagens AS2 que foram enviadas sem sucesso a um parceiro comercial . Ou seja, elas foram enviados do servidor Transfer Family, mas não foram recebidas com sucesso pelo parceiro comercial. Unidades: contagem Período: 5 minutos
DaysUntilExpiry	O número de dias até a expiração de um certificado é determinado pelo InactiveD ate definido no certificado durante a importação. Unidades: contagem Dimensões:CertificateId , Descripti on (se fornecido) Período: 1 dia Para obter mais informações, consulte Alternância de certificados AS2.

Códigos de status AS2

A tabela a seguir lista todos os códigos de status que podem ser registrados nos CloudWatch registros quando você ou seu parceiro enviam uma mensagem AS2. Diferentes etapas de processamento de mensagens se aplicam a diferentes tipos de mensagens e são destinadas somente ao monitoramento. Os estados COMPLETED e FAILED representam a etapa final do processamento e são visíveis nos arquivos JSON.

Código	Description	Processamento concluído?
PROCESSANDO	A mensagem está sendo convertida em seu formato final. Por exemplo, as etapas de descompressão e descriptografia têm esse status.	Não
MDN_TRANSMITEM	O processamento de mensagens está enviando uma resposta MDN.	Não
MDN_RECEIVE	O processamento de mensagens está recebendo uma resposta MDN.	Não
CONCLUÍDO	O processamento da mensagem foi concluído com êxito. Esse estado inclui quando um MDN é enviado para uma mensagem de entrada ou para verificação de mensagens enviadas pelo MDN.	Sim
FAILED	O processamento da mensagem falhou. Para obter uma lista de códigos de erro, consulte Códigos de erro AS2 .	Sim

Códigos de erro AS2

A tabela a seguir lista e descreve os códigos de erro que você pode receber das transferências de arquivos AS2.

Códigos de erro AS2

Código	Erro	Descrição e resolução
ACCESS_DENIED	- Acesso negado. Verifique se sua função de acesso possui as permissões necessárias. - Caminho de arquivo inválido <i>send-file-path</i> - Falha ao obter credenciais com ErrorCode: <i>error-code</i>	Ocorre ao lidar com uma solicitação StartFileTransfer em que qualquer uma das SendFilePaths não é válida ou está malformada. Ou seja, falta o nome do bucket do Amazon S3 no caminho ou o caminho inclui caracteres que não são válidos. Também ocorre se Transfer Family não assumir a função de acesso ou de logging. Certifique-se de que o caminho contenha um nome de bucket e um nome de chave válidos do Amazon S3.
AGREEMENT_NOT_FOUND	Não foi possível encontrar o acordo.	O acordo não foi encontrado ou está associado a um perfil inativo. Atualize o contrato no servidor Transfer Family para incluir perfis ativos.
CONNECTOR_NOT_FOUND	O conector ou configuração relacionada não foi encontrado.	O conector não foi encontrado ou está associado a um perfil inativo. Atualize o conector para incluir perfis ativos.

Código	Erro	Descrição e resolução
CREDENTIALS_RETRIEVAL_FAILED	1. Segredo não encontrado no Secrets Manager. 2. Não é possível acessar o Secrets Manager. 3. Falha ao descriptografar o segredo no Secrets Manager. 4. Não é possível obter o valor secreto devido ao controle de utilização.	Para autenticação AS2 Basic, o segredo deve ser formatado corretamente. As resoluções a seguir correspondem aos erros listados na coluna anterior. 1. Certifique-se de que o ID secreto esteja correto. 2. Certifique-se de que a função de acesso tenha as permissões apropriadas para ler o segredo. A função de acesso deve fornecer acesso de leitura e gravação ao diretório principal do local do arquivo usado na solicitação <code>StartFileTransfer</code> . Além disso, certifique-se de que a função forneça acesso de leitura e gravação ao diretório pai dos arquivos com os quais você pretende enviar com <code>StartFileTransfer</code> . 3. Se uma chave gerenciada pelo cliente estiver sendo usada para o segredo, certifique-se de que a função de acesso tenha permissões para a chave AWS Key Management Service (AWS KMS).

Código	Erro	Descrição e resolução
		4. Para as cotas aplicáveis, consulte Cotas para lidar com segredos .
DECOMPRESSION_FAILED	Falha ao descompactar a mensagem.	O arquivo enviado está corrompido ou o algoritmo de compactação não é válido. Reenvie a mensagem e verifique se a compactação ZLIB é usada ou reenvie a mensagem sem a compactação habilitada.
DECRYPT_FAILED	Falha ao descriptografar a mensagem. <i>message-ID</i> Certifique-se de que o parceiro tenha a chave de criptografia pública correta.	Falha na decodificação. Confirme se o parceiro enviou uma carga usando um certificado válido e se a criptografia foi executada usando um algoritmo de criptografia válido.
DECRYPT_FAILED_INVALID_SMIME_FORMAT	Não é possível analisar o MimePart envelopado.	A carga MIME está corrompida ou está em um formato SMIME não suportado. O remetente deve certificar-se de que o formato que está usando é compatível e, em seguida, reenviar a carga.

Código	Erro	Descrição e resolução
DECRYPT_FAILED_NO_DECRYPTION_KEY_FOUND	Nenhuma chave decriptografia correspondente encontrada.	O perfil do parceiro não tinha um certificado atribuído que correspondesse à mensagem ou os certificados que correspondiam à mensagem expiraram ou não são mais válidos. Você deve atualizar o perfil do parceiro e garantir que ele contenha um certificado válido.
DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG	Descriptografia de carga útil SMIME solicitada usando algoritmo não suportado com ID: <i>encryption-ID</i>	O remetente remoto enviou uma carga AS2 com um algoritmo de criptografia não suportado. O remetente deve escolher um algoritmo de criptografia compatível com AWS Transfer Family.
DUPLICATE_MESSAGE	Etapa duplicada ou processada duas vezes.	A carga tem uma etapa de processamento duplicada. Por exemplo, existem duas etapas de criptografia. Reenvie a mensagem com uma única etapa de assinatura, compactação e criptografia.

Código	Erro	Descrição e resolução
ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND	Nenhum certificado de criptografia pública válido foi encontrado no perfil: <i>local-profile-ID</i>	O Transfer Family está tentando criptografar uma mensagem de saída, mas nenhum certificado de criptografia foi encontrado para o perfil local. Opções de resolução: • Certifique-se de que o perfil local tenha um certificado e uma chave privada para criptografia anexados. • Certifique-se de que o certificado de criptografia esteja ativo no momento.
ENCRYPTION_FAILED	Falha ao criptografar o arquivo <i>file-name</i> .	O arquivo a ser enviado não está disponível para criptografia. Verifique se o arquivo está no local AS2 esperado e se AWS Transfer Family tem permissão para ler o arquivo.
FILE_SIZE_TOO_LARGE	O tamanho do arquivo é muito grande.	Isso ocorre ao enviar ou receber um arquivo que excede o limite de tamanho de arquivo.

Código	Erro	Descrição e resolução
HTTP_ERROR_RESPONSE_FROM_PARTNER	<i>partner-URL</i> retornou o status 400 para mensagem com ID= <i>message-ID</i> .	A comunicação com o servidor AS2 do parceiro retornou um código de resposta HTTP inesperado. O parceiro pode ser capaz de fornecer mais diagnósticos a partir dos registros do servidor AS2.
INSUFFICIENT_MESSAGE_SECURITY_UNENCRYPTED	A criptografia é necessária.	O parceiro enviou uma mensagem não criptografada para Transfer Family, o que não é suportado. O remetente deve usar uma carga criptografada.
INVALID_ENDPOINT_PROTOCOL	Somente HTTP e HTTPS são compatíveis.	Você deve especificar HTTP ou HTTPS como o protocolo na configuração do conector AS2.

Código	Erro	Descrição e resolução
INVALID_REQUEST	- Há um problema com o cabeçalho da mensagem. - Não foi possível analisar o JSON secreto. O JSON secreto não correspondeu ao formato esperado. - O segredo deve ser uma string JSON. - O nome de usuário não deve conter dois pontos. O nome de usuário não deve conter caracteres de controle. O nome de usuário deve conter apenas caracteres ASCII. A senha não deve conter caracteres de controle. A senha deve conter apenas caracteres ASCII.	Esse erro tem várias causas. As resoluções a seguir correspondem aos erros listados na coluna anterior. - Verifique os campos <code>as2-from</code> e <code>as2-to</code>. Certifique-se de que a ID da mensagem original esteja correta para o formato MDN. Verifique também se o formato de ID da mensagem não está faltando nenhum cabeçalho AS2. - Certifique-se de que o valor secreto corresponda ao formato documentado, conforme descrito em Habilitar a autenticação básica para conectores AS2. - Certifique-se de que o segredo seja fornecido como uma string e não como um binário. - Faça a correção necessária no nome de usuário ou senha.

Código	Erro	Descrição e resolução
INVALID_URL_FORMAT	Formato de URL inválido: <i>URL</i>	Isso ocorre quando você está enviando uma mensagem de saída usando um conector configurado com uma URL incorreta. Certifique-se de que o conector esteja configurado com uma URL HTTP ou HTTPS válida.
MDN_RESPONSE_INDICATES_AUTHENTICATION_FAILED	Não aplicável	O destinatário não consegue autenticar o remetente. O parceiro comercial retorna um MDN para Transfer Family com o modificador de disposição Error: authentication-failed.
MDN_RESPONSE_INDICATES_DECOMPRESSION_FAILED	Não aplicável	Isso ocorre quando o receptor não consegue descompactar o conteúdo da mensagem. O parceiro comercial retorna um MDN Transfer Family com o modificador de disposição Error: authentication-failed.
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	Não aplicável	O destinatário não consegue decifrar o conteúdo da mensagem. O parceiro comercial retorna um MDN para Transfer Family com o modificador de disposição Error: authentication-failed.

Código	Erro	Descrição e resolução
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	Não aplicável	O destinatário espera que a mensagem seja assinada ou criptografada, mas não está. O parceiro comercial retorna um MDN para Transfer Family com o modificador de disposição Error: insufficient-message-security. Ative a and/or criptografia de assinatura no conector para atender às expectativas do parceiro comercial.
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	Não aplicável	O receptor não pode verificar a integridade do conteúdo. O parceiro comercial retorna um MDN para Transfer Family com o modificador de disposição Error: integrity-check-failed.
PATH_NOT_FOUND	Não foi possível criar o diretório <i>file-path</i> . O caminho principal não pôde ser encontrado.	A Transfer Family está tentando criar um diretório no bucket Amazon S3 do cliente, mas o bucket não foi encontrado. Certifique-se de que cada caminho mencionado no StartFileTransfer comando contenha o nome de um bucket existente.

Código	Erro	Descrição e resolução
SEND_FILE_NOT_FOUND	Caminho do arquivo <i>file-path</i> não encontrado.	O Transfer Family não consegue localizar o arquivo na operação de envio do arquivo. Verifique se o diretório inicial e o caminho configurados são válidos e se o Transfer Family tem permissões de leitura para o arquivo.
SERVER_NOT_FOUND	Não foi possível encontrar o servidor associado à mensagem.	A Transfer Family não conseguiu encontrar o servidor ao receber uma mensagem. Isso pode acontecer se o servidor for excluído durante o processamento de uma mensagem recebida.
SERVER_NOT_ONLINE	O servidor não <i>server-ID</i> está online.	O servidor Transfer Family está off-line. Inicie o servidor para que ele possa receber e processar mensagens.
SIGNING_FAILED	Falha ao assinar o arquivo.	O arquivo a ser enviado não está disponível para assinatura ou a assinatura não pôde ser executada. Verifique se o arquivo está no local AS2 esperado e se AWS Transfer Family tem permissão para ler o arquivo.

Código	Erro	Descrição e resolução
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	Nenhum certificado encontrado para o perfil: <i>local-pro file-ID</i> .	Tentando assinar uma mensagem de saída, mas nenhum certificado de assinatura foi encontrado para o perfil local. Opções de resolução: • Certifique-se de que o perfil local tenha um certificado e uma chave privada para assinatura anexados. • Verifique se o certificado de assinatura está ativo no momento.
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	Não foi possível resolver o nome do host para endereços IP.	O Transfer Family não consegue executar a resolução de DNS para endereço IP no servidor DNS público que está configurado no conector AS2. Atualize o conector para apontar para um URL de parceiro válido.
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	A conexão com o endpoint atingiu o tempo limite.	O Transfer Family não pode estabelecer uma conexão de soquete com o servidor AS2 do parceiro configurado. Verifique se o servidor AS2 do parceiro está disponível no endereço IP configurado.

Código	Erro	Descrição e resolução
UNABLE_TO_RESOLVE_HOSTNAME	Não foi possível resolver o nome do host <i>hostname</i> .	O servidor Transfer Family não conseguiu resolver o nome do host do parceiro usando um servidor DNS público. Verifique se o host configurado está registrado e se o registro DNS teve tempo de ser publicado.
VERIFICATION_FAILED	A verificação da assinatura falhou para a mensagem AS2 <i>message-ID</i> ou um código MIC não correspondeu.	Verifique se o certificado de assinatura do remetente corresponde aos certificados de assinatura do perfil remoto. Verifique também se os algoritmos MIC são compatíveis com AWS Transfer Family.

Código	Erro	Descrição e resolução
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	- Nenhum certificado público correspondente à assinatura da mensagem foi encontrado no perfil:<i>partner-profile-ID</i> . - Não é possível obter certificados para um perfil inexistente:.. <i>partner-profile-ID</i> - Nenhum certificado válido foi encontrado no perfil:<i>partner-profile-ID</i> .	AWS Transfer Family está tentando verificar a assinatura de uma mensagem recebida, mas nenhum certificado de assinatura correspondente foi encontrado para o perfil do parceiro. Opções de resolução: - Certifique-se de que o perfil do parceiro tenha um certificado de assinatura anexado. - Verifique se o certificado está ativo no momento. - Certifique-se de que o certificado seja o certificado de assinatura correto para o parceiro.

Monitoramento da expiração do certificado

AWS Transfer Family monitora automaticamente as datas de expiração dos certificados AS2 e publica uma CloudWatch métrica da Amazon para ajudá-lo a rastrear quando os certificados estão prestes a expirar. Isso permite que você gerencie proativamente as renovações de certificados e evite interrupções no serviço.

DaysUntilExpiry métrica

Quando você importa um certificado para uso do AS2, o Transfer Family cria automaticamente uma CloudWatch métrica chamada `DaysUntilExpiry`. Essa métrica rastreia o número de dias restantes até o certificado expirar com base no `InactiveDate` que você especificou ao importar o certificado.

Detalhes métricos:

- Nome da métrica: `DaysUntilExpiry`
- Namespace: `AWS/Transfer`
- Dimensões: `CertificateId` (sempre presentes), `Description` (se fornecidas durante a importação do certificado)
- Unidades: Contagem (dias)
- Frequência: Publicado diariamente

Important

Após a importação de um certificado, o Transfer Family pode levar até um dia inteiro para emitir essa métrica para sua conta.

O valor da métrica diminui em um a cada dia à medida que o certificado se aproxima da data de inatividade. Por exemplo, se um certificado tiver 30 dias até a expiração, a métrica mostrará 30, 29 no dia seguinte e assim por diante.

Práticas recomendadas para monitoramento de certificados

Siga estas melhores práticas ao configurar o monitoramento de expiração de certificados:

- Defina vários limites de alerta: crie alarmes para diferentes períodos de tempo (por exemplo, 30 dias, 14 dias e 7 dias antes da expiração) para fornecer tempo adequado para a renovação do certificado.
- Use estatísticas apropriadas: use a `Maximum` estatística ao criar alarmes para garantir que você capture o valor métrico mais recente.
- Configure as ações de alarme adequadas: configure notificações para alertar os membros apropriados da equipe que podem renovar os certificados.
- Teste seus alertas: teste regularmente seu sistema de notificação para garantir que os alertas sejam entregues corretamente.
- Documente seu processo: mantenha a documentação sobre o processo de renovação do certificado e quem é responsável pelos diferentes certificados.

Exemplo de configurações de alarme

Aqui estão alguns exemplos de configurações de alarme para diferentes cenários de notificação:

Aviso de expiração de 30 dias

Crie um alarme que seja acionado quando um certificado tiver 30 dias ou menos até a expiração:

- Métrica: DaysUntilExpiry
- Estatística: máxima
- Período: 1 dia
- Limite: 30
- Comparação: menor ou igual ao limite
- Tratamento de dados perdidos: trate os dados perdidos como algo bom (sem violação)

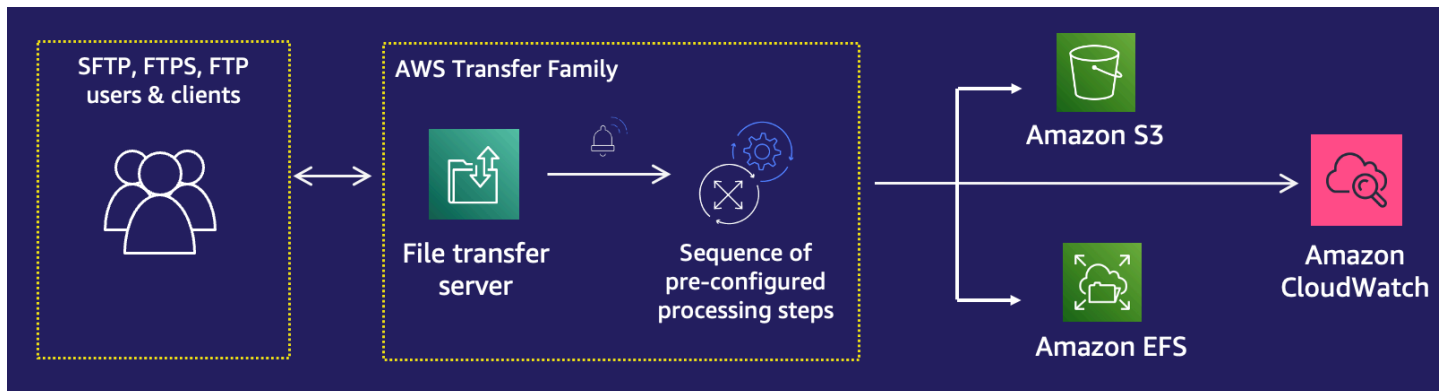
Aviso crítico de expiração de 7 dias

Crie um alarme crítico que será acionado quando um certificado tiver 7 dias ou menos até a expiração:

- Métrica: DaysUntilExpiry
- Estatística: máxima
- Período: 1 dia
- Limite: 7
- Comparação: menor ou igual ao limite
- Tratamento de dados perdidos: trate os dados perdidos como algo bom (sem violação)

AWS Transfer Family fluxos de trabalho gerenciados

AWS Transfer Family suporta fluxos de trabalho gerenciados para processamento de arquivos. Com fluxos de trabalho gerenciados, você pode iniciar um fluxo de trabalho após a transferência de um arquivo por SFTP, FTPS ou FTP. Usando esse recurso, você pode atender de forma segura e econômica aos requisitos de conformidade para trocas de arquivos entre empresas (B2B), coordenando todas as etapas necessárias para o processamento de arquivos. Além disso, você se beneficia de auditoria e visibilidade de ponta a ponta.



Ao orquestrar as tarefas de processamento de arquivos, os fluxos de trabalho gerenciados ajudam você a pré-processar os dados antes que eles sejam consumidos pelos aplicativos posteriores. Essas tarefas de processamento de arquivos podem incluir:

- Mover arquivos para pastas específicas do usuário.
- Descriptografar arquivos como parte de um fluxo de trabalho.
- Marcar arquivos.
- Executar o processamento personalizado criando e anexando uma AWS Lambda função a um fluxo de trabalho.
- Envio de notificações quando um arquivo foi transferido com sucesso. (Para uma postagem no blog que detalha esse caso de uso, consulte [Personalizar notificações de entrega de arquivos usando fluxos de trabalho AWS Transfer Family gerenciados](#).)

Para replicar e padronizar rapidamente tarefas comuns de processamento de arquivos pós-upload abrangendo várias unidades de negócios em sua organização, você pode implantar fluxos de trabalho usando a infraestrutura como código (IaC). Você pode especificar um fluxo de trabalho gerenciado a ser iniciado em arquivos que são carregados na íntegra. Você também pode especificar um fluxo de trabalho gerenciado diferente a ser iniciado em arquivos que foram

carregados apenas parcialmente devido a uma desconexão prematura da sessão. Built-in o tratamento de exceções ajuda você a reagir rapidamente aos resultados do processamento de arquivos, ao mesmo tempo em que oferece controle sobre como lidar com falhas. Além disso, cada etapa do fluxo de trabalho produz logs detalhados, que você pode auditar para rastrear a linhagem dos dados.

Para começar, realize as seguintes tarefas:

1. Configure seu fluxo de trabalho para conter ações de pré-processamento, como cópia, marcação e outras etapas com base em seus requisitos. Para mais detalhes, consulte [Criar um fluxo de trabalho](#).
2. Configure uma função de execução, que o Transfer Family usa para executar o fluxo de trabalho. Para mais detalhes, consulte [Políticas do IAM para fluxos de trabalho](#).
3. Mapeie o fluxo de trabalho para um servidor, para que, na chegada do arquivo, as ações especificadas nesse fluxo de trabalho sejam avaliadas e iniciadas em tempo real. Para mais detalhes, consulte [Configurar e executar um fluxo de trabalho](#).

Informações relacionadas

- Para monitorar suas execuções de fluxo de trabalho, consulte [Usando CloudWatch métricas para servidores Transfer Family](#).
- Para obter logs detalhados de execução e informações sobre solução de problemas, consulte [Solucione erros relacionados ao fluxo de trabalho usando a Amazon CloudWatch](#).
- O Transfer Family fornece uma postagem no blog e um workshop que orientam você na criação de uma solução de transferência de arquivos. Essa solução usa AWS Transfer Family SFTP/FTPS endpoints gerenciados e Amazon Cognito e DynamoDB para gerenciamento de usuários.

A postagem do blog está disponível em [Usando o Amazon Cognito como provedor de identidade com AWS Transfer Family o Amazon S3](#). Você pode ver os detalhes do workshop [aqui](#).

- Consulte [Fluxos de trabalho gerenciados pelo AWS Transfer Family](#) para obter uma breve introdução aos fluxos de trabalho do Transfer Family.
- [O workshop a seguir fornece laboratórios práticos para criar fluxos de trabalho totalmente automatizados e orientados por eventos envolvendo transferência de arquivos de ou para servidores SFTP externos para o Amazon S3 e pré-processamento e pós-processamento comuns desses arquivos: workshop MFT. Event-driven](#)

Este vídeo fornece um resumo desse workshop.

Tópicos

- [Criar um fluxo de trabalho](#)
- [Usar etapas predefinidas](#)
- [Use etapas personalizadas de processamento de arquivos](#)
- [Políticas do IAM para fluxos de trabalho](#)
- [Tratamento de exceções para um fluxo de trabalho](#)
- [Monitore a execução do fluxo](#)
- [Criar um fluxo de trabalho a partir de um modelo](#)
- [Remover um fluxo de trabalho de um servidor Transfer Family](#)
- [Restrições e limitações de fluxos de trabalho gerenciados](#)

Para obter mais ajuda para começar a usar fluxos de trabalho gerenciados, consulte os seguintes recursos:

- AWS Transfer Family vídeo de demonstração [de fluxos de trabalho gerenciados](#)
- Publicação do blog sobre [como criar uma plataforma de transferência de arquivos nativa em nuvem usando AWS Transfer Family fluxos de trabalho](#)

Criar um fluxo de trabalho

Você pode criar um fluxo de trabalho gerenciado usando o Console de gerenciamento da AWS, conforme descrito neste tópico. Para tornar o processo de criação do fluxo de trabalho o mais fácil possível, painéis de ajuda contextual estão disponíveis para a maioria das seções do console.

Um fluxo de trabalho tem dois tipos de etapas:

- Etapas nominais — As etapas nominais são etapas de processamento de arquivos que você deseja aplicar aos arquivos recebidos. Se você selecionar mais de uma etapa nominal, cada etapa será processada em uma sequência linear.
- Exception-handling etapas — Os manipuladores de exceções são etapas de processamento de arquivos AWS Transfer Family executadas caso alguma etapa nominal falhe ou resulte em erros de validação.

Criar um fluxo de trabalho

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, selecione Fluxos de trabalho.
3. Na página Fluxos de trabalho, escolha Criar um fluxo de trabalho.
4. Na página Criar fluxo de trabalho, insira uma descrição. Essa descrição aparece na página Fluxos de trabalho.
5. Na seção Etapas nominais, escolha Adicionar etapa. Adicione uma ou mais etapas.
 - a. Escolha um tipo de etapa entre as opções disponíveis. Para obter mais informações sobre as várias etapas, consulte [the section called “Usar etapas predefinidas”](#).
 - b. Escolha Próximo e configure os parâmetros para a etapa.
 - c. Escolha Próximo e, em seguida, revise os detalhes da etapa.
 - d. Escolha Criar etapa para adicionar a etapa e continuar.
 - e. Continue adicionando etapas conforme necessário. O número máximo de etapas em um fluxo de trabalho é 8.
 - f. Depois de adicionar todas as etapas nominais necessárias, role para baixo até a seção Manipuladores de exceções — opcional e escolha Adicionar etapa.

Note

Para que você seja informado sobre falhas em tempo real, recomendamos que você configure manipuladores de exceções e etapas a serem executadas quando seu fluxo de trabalho falhar.

6. Para configurar manipuladores de exceções, adicione etapas da mesma maneira descrita anteriormente. Se um arquivo fizer com que qualquer etapa gere uma exceção, seus manipuladores de exceções serão invocados um por um.
7. (Opcional) Role para baixo até a seção Tags e adicione tags ao seu fluxo de trabalho.
8. Reveja a configuração e selecione Criar fluxo de trabalho.

Important

Depois de criar um fluxo de trabalho, você não poderá editá-lo, portanto, revise a configuração com cuidado.

Configurar e executar um fluxo de trabalho

Antes de executar um fluxo de trabalho, você precisa associá-lo a um servidor Transfer Family.

Para configurar o Transfer Family para executar um fluxo de trabalho em arquivos enviados

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, selecione Servidores.
 - Para adicionar o fluxo de trabalho a um servidor existente, escolha o servidor que você deseja usar para seu fluxo de trabalho.
 - Como alternativa, crie um novo servidor e adicione o fluxo de trabalho a ele. Para obter mais informações, consulte [Configurando um endpoint de servidor SFTP, FTPS ou FTP](#).
3. Na página de detalhes do servidor, role para baixo até a seção Detalhes adicionais e escolha Editar.

Note

Por padrão, os servidores não têm fluxos de trabalho associados. Você usa a seção Detalhes adicionais para associar um fluxo de trabalho ao servidor selecionado.

4. Na página Editar detalhes adicionais, na seção Fluxos de trabalho gerenciados, selecione um fluxo de trabalho a ser executado em todos os carregamentos.

Note

Se você ainda não tiver um fluxo de trabalho, escolha Criar um novo fluxo de trabalho para criar um.

- a. Escolha o ID do fluxo de trabalho a ser usado.
- b. Escolha uma função de execução. Esta é a função que o Transfer Family assume ao executar as etapas do fluxo de trabalho. Para obter mais informações, consulte [Políticas do IAM para fluxos de trabalho](#). Escolha Salvar.

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w-

Create a new Workflow

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w-

Create a new Workflow

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

Note

Se você não quiser mais que um fluxo de trabalho seja associado ao servidor, você pode remover a associação. Para obter detalhes, consulte [Remover um fluxo de trabalho de um servidor Transfer Family](#).

Para executar um fluxo de trabalho

Para executar um fluxo de trabalho, você carrega um arquivo em um servidor Transfer Family que você configurou com um fluxo de trabalho associado.

Note

Sempre que você remove um fluxo de trabalho de um servidor e o substitui por um novo ou atualiza a configuração do servidor (o que afeta a função de execução de um fluxo de trabalho), você deve esperar aproximadamente 10 minutos antes de executar o novo fluxo de trabalho. O servidor do Transfer Family armazena em cache os detalhes do fluxo de trabalho e leva 10 minutos para que o servidor atualize o cache.

Além disso, você deve sair de qualquer sessão ativa de SFTP e, em seguida, fazer login novamente após o período de espera de 10 minutos para ver as alterações.

Example

```
# Execute a workflow
> sftp bob@s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com

Connected to s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com.
sftp> put doc1.pdf
Uploading doc1.pdf to /amzn-s3-demo-bucket/home/users/bob/doc1.pdf
doc1.pdf                                     100% 5013KB
 601.0KB/s   00:08
sftp> exit
>
```

Depois que seu arquivo for carregado, a ação definida será executada em seu arquivo. Por exemplo, se seu fluxo de trabalho contiver uma etapa de cópia, o arquivo será copiado para o local que você definiu nessa etapa. Você pode usar o Amazon CloudWatch Logs para rastrear as etapas executadas e seu status de execução.

Visualizar detalhes do fluxo de trabalho

Você pode ver detalhes sobre fluxos de trabalho criados anteriormente ou sobre execuções de fluxo de trabalho. Para ver esses detalhes, você pode usar o console ou o AWS Command Line Interface (AWS CLI).

Console

Visualizar detalhes do fluxo de trabalho

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, selecione Fluxos de trabalho.
3. Na página Fluxos de trabalho, escolha um fluxo de trabalho.

A página de detalhes do fluxo de trabalho é aberta.

The screenshot shows the AWS Transfer Family console interface. On the left is a navigation sidebar with options like Servers, Connectors, AS2 Trading Partners, Certificates, Profiles, Workflows (selected), Feature Spotlight, What's New, Documentation, About servers, and About SFTP connectors. The main content area displays details for a specific workflow 'W-1234567890abcdef0'. It includes a 'Description' section with the name 'Test my workflow' and a description 'Test workflow A'. Below this is a 'Nominal steps (1)' section with a table containing one step: a TAG step named 'tag_step'. There is also an 'Exception handlers (1)' section with a table containing one handler: a DELETE handler named 'delete_if_exception'. The 'In-flight executions (0)' section shows a search bar and a table with no data, indicating no executions are currently running. At the bottom, there is a 'Tags (1)' section with a 'Manage tags' button.

CLI

Para visualizar detalhes do fluxo de trabalho, use o comando da CLI `describe-workflow`, conforme mostrado no exemplo a seguir. Substitua o ID de fluxo de trabalho `w-1234567890abcdef0` pelos seus próprios valores. Para obter mais informações, consulte [describe-workflow](#) na Referência de comandos do AWS CLI .

```
# View Workflow details
> aws transfer describe-workflow --workflow-id w-1234567890abcdef0
{
  "Workflow": {
    "Arn": "arn:aws:transfer:us-east-1:111122223333:workflow/w-1234567890abcdef0",
    "WorkflowId": "w-1234567890abcdef0",
    "Name": "Copy file to shared_files",
    "Steps": [
      {
```

```

        "Type": "COPY",
        "CopyStepDetails": {
          "Name": "Copy to shared",
          "FileLocation": {
            "S3FileLocation": {
              "Bucket": "amzn-s3-demo-bucket",
              "Key": "home/shared_files/"
            }
          }
        }
      ],
      "OnException": {}
    }
  }
}

```

Se seu fluxo de trabalho foi criado como parte de uma AWS CloudFormation pilha, você pode gerenciar o fluxo de trabalho usando o CloudFormation console (<https://console.aws.amazon.com/cloudformation>).

The screenshot shows the AWS Transfer Family Workflows console. At the top, there's a breadcrumb trail: [Transfer Family](#) > [Workflows](#) > [w-...](#). Below this, the workflow name 'W-...' is displayed with a 'Delete' button. A blue information banner states: 'This workflow belongs to the AWS CloudFormation stack **stack-transfer-notifications-blog**. [Manage this stack](#) on the CloudFormation console.'

The 'Description' section shows the workflow name 'W-...' and its status 'Stack-managed'. To the right, there's a 'Workflow description' section with the text 'Workflow for blogpost'.

The 'Nominal steps (4) Info' section contains a table with the following data:

Number	Description	Type	Configuration
1	Lambda	CUSTOM	Details
2	CopyFile	COPY	Details
3	TagFileNotified	TAG	Details
4	DeleteOriginalSourceFile	DELETE	Details

Usar etapas predefinidas

Ao criar um fluxo de trabalho, você pode optar por adicionar uma das seguintes etapas predefinidas discutidas neste tópico. Você também pode escolher adicionar suas próprias etapas de processamento de arquivos. Para obter mais informações, consulte [the section called “Use etapas personalizadas de processamento de arquivos”](#).

Tópicos

- [Copiar arquivo](#)
- [Descriptografar arquivo](#)
- [Arquivo de marcação](#)
- [Excluir arquivo](#)
- [Variáveis nomeadas para fluxos de trabalho](#)
- [Exemplo para marcar e excluir fluxo de trabalho](#)

Copiar arquivo

Uma etapa de cópia do arquivo cria uma cópia do arquivo carregado em um novo local do Amazon S3. Atualmente, você pode usar uma etapa de cópia de arquivo somente com o Amazon S3.

A etapa de cópia do arquivo a seguir copia os arquivos para a test pasta em *amzn-s3-demo-destination-bucket*.

Se a etapa de cópia do arquivo não for a primeira etapa do seu fluxo de trabalho, você poderá especificar o Local do arquivo. Ao especificar o local do arquivo, você pode copiar o arquivo usado na etapa anterior ou o arquivo original que foi carregado. Você pode usar esse recurso para fazer várias cópias do arquivo original e, ao mesmo tempo, manter o arquivo de origem intacto para arquivamento e retenção de logs. Para ver um exemplo, consulte [Exemplo para marcar e excluir fluxo de trabalho](#).

Configure copy parameters

Step name

File location

Select the file location to use as an input for this step

☒ Copy the file created from previous step to a new location

Input file is selected from the previous step's output

☐ Copy the original source file to a new location

Originally uploaded file

Destination bucket name

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

☐ Overwrite existing

Informe o bucket e os principais detalhes

Você deve fornecer o nome do bucket e uma chave para o destino da etapa de cópia do arquivo. A chave pode ser um nome de caminho ou um nome de arquivo. O fato de a chave ser tratada como um nome de caminho ou nome de arquivo é determinado pelo fato de você terminar a chave com o caractere de barra (/).

Se o caractere final for /, seu arquivo será copiado para a pasta e seu nome não será alterado. Se o caractere final for alfanumérico, o arquivo enviado será renomeado para o valor-chave. Nesse caso,

se um arquivo com esse nome já existir, o comportamento dependerá da configuração do campo Substituir existente.

- Se Substituir existente for selecionado, o arquivo existente será substituído pelo arquivo que está sendo processado.
- Se a opção Substituir existente não estiver selecionada, nada acontecerá e o processamento do fluxo de trabalho será interrompido.

 Tip

Se as gravações simultâneas forem executadas no mesmo caminho de arquivo, isso poderá resultar em um comportamento inesperado ao substituir arquivos.

Por exemplo, se o valor da chave for `test/`, os arquivos enviados serão copiados para a pasta `test`. Se o valor da chave for `test/today` (e a opção Substituir existente estiver selecionada), todos os arquivos enviados serão copiados para um arquivo nomeado `today` na pasta `test`, e cada arquivo seguinte substituirá o anterior.

 Note

O Amazon S3 é compatível com buckets e objetos e não há nenhuma hierarquia. No entanto, você pode usar prefixos e delimitadores em nomes de chaves de objetos para sugerir uma hierarquia e organizar seus dados de forma semelhante às pastas.

Use uma variável nomeada em uma etapa de cópia do arquivo

Em uma etapa de cópia de arquivo, você pode usar uma variável para copiar dinamicamente seus arquivos em pastas específicas do usuário. Atualmente, você pode usar `${transfer:UserName}` ou `${transfer:UploadDate}` como uma variável para copiar arquivos para um local de destino para um determinado usuário que está fazendo o upload dos arquivos ou com base na data atual.

No exemplo a seguir, se o usuário `richard-roe` fizer upload de um arquivo, ele será copiado para a pasta `amzn-s3-demo-destination-bucket/richard-roe/processed/`. Se o usuário `mary-major` fizer upload de um arquivo, ele será copiado para a pasta `amzn-s3-demo-destination-bucket/mary-major/processed/`.

Configure parameters

Configure copy parameters

Step name

dynamic-copy

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UserName}/processed`

☐ Overwrite existing

Da mesma forma, você pode usar `${transfer:UploadDate}` como variável para copiar arquivos para um local de destino nomeado com a data atual. No exemplo a seguir, se você definir o destino como `${transfer:UploadDate}/processed` em 1º de fevereiro de 2022, os arquivos enviados serão copiados para a pasta `amzn-s3-demo-destination-bucket/2022-02-01/processed/`.

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UploadDate}/processed`

☐ Overwrite existing

Você também pode usar essas duas variáveis juntas, combinando suas funcionalidades. Por exemplo, você pode definir o prefixo da chave de destino como `folder/${transfer:UserName}/${transfer:UploadDate}/`, o que criaria pastas aninhadas, por exemplo. `folder/marymajor/2023-01-05/`

Permissões do IAM para a etapa de copiar

Para permitir que uma etapa de cópia seja bem-sucedida, certifique-se de que a função de execução do seu fluxo de trabalho contenha as seguintes permissões.

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
```

```
"Effect": "Allow",
"Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
],
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

Note

A permissão `s3:ListBucket` só é necessária se você não selecionar Substituir existente. Essa permissão verifica seu bucket para ver se já existe um arquivo com o mesmo nome. Se você selecionou Substituir existente, o fluxo de trabalho não precisa verificar o arquivo e pode simplesmente gravá-lo. Se seus arquivos do Amazon S3 tiverem tags, você precisará adicionar uma ou duas permissões à sua política do IAM.

- Adicione `s3:GetObjectTagging` para obter um arquivo Amazon S3 que não tenha versão.
- Adicione `s3:GetObjectVersionTagging` para obter um arquivo Amazon S3 que tenha versão.

Descriptografar arquivo

O blog AWS de armazenamento tem uma postagem que descreve como simplesmente descriptografar arquivos sem escrever nenhum código usando fluxos de trabalho do Transfer Family Managed, [criptografar e descriptografar](#) arquivos com PGP e AWS Transfer Family

Algoritmos de criptografia simétrica compatíveis

Para a decodificação PGP, o Transfer Family suporta algoritmos de criptografia simétrica que são usados para criptografar os dados reais do arquivo dentro dos arquivos PGP.

- Para obter informações detalhadas sobre os algoritmos de criptografia simétrica compatíveis, consulte [Algoritmos de criptografia simétrica PGP](#).

- Para obter informações sobre algoritmos de par de chaves PGP usados com esses algoritmos simétricos, consulte [Algoritmos de pares de chaves PGP](#)

Use a descryptografia PGP em seu fluxo de trabalho

O Transfer Family tem suporte integrado para descryptografia Pretty Good Privacy (PGP). Você pode usar a descryptografia PGP em arquivos enviados por SFTP, FTPS ou FTP para o Amazon Simple Storage Service (Amazon S3) ou o Amazon Elastic File System (Amazon EFS).

Para usar a descryptografia PGP, você deve criar e armazenar as chaves privadas PGP que serão usadas para descryptografar seus arquivos. Seus usuários podem então criptografar arquivos usando as chaves de criptografia PGP correspondentes antes de fazer o upload dos arquivos para o servidor Transfer Family. Depois de receber os arquivos criptografados, você pode descryptografar esses arquivos no seu fluxo de trabalho. Para ver um tutorial detalhado, consulte [Configurando um fluxo de trabalho gerenciado para descryptografar um arquivo](#).

Para obter informações sobre algoritmos e recomendações de PGP compatíveis, consulte [Algoritmos de criptografia e decodificação PGP](#)

Para usar a descryptografia PGP em seu fluxo de trabalho

1. Identifique um servidor Transfer Family para hospedar seu fluxo de trabalho ou crie um novo. Você precisa ter o ID do servidor antes de poder armazenar suas chaves PGP no AWS Secrets Manager com o nome secreto correto.
2. Armazene sua chave PGP AWS Secrets Manager com o nome secreto necessário. Para obter detalhes, consulte [Gerenciar chaves PGP](#). Os fluxos de trabalho podem localizar automaticamente a chave PGP correta a ser usada para descryptografia com base no nome secreto no Gerente secreto.

Note

Quando você armazena segredos no Secrets Manager, você Conta da AWS incorre em cobranças. Para obter mais informações sobre preços consulte [AWS Secrets Manager Pricing](#).

3. Criptografe um arquivo usando seu par de chaves PGP. (Para ver uma lista dos TLDs, consulte [Clientes PGP compatíveis](#).) Se você estiver usando a linha de comando, execute o seguinte comando: Para usar esse comando, substitua *username@example.com* pelo endereço de e-

mail que você usou para criar o par de chaves PGP. Substitua *testfile.txt* pelo nome do arquivo que você deseja criptografar.

```
gpg -e -r username@example.com testfile.txt
```

Important

Ao criptografar arquivos para uso com AWS Transfer Family fluxos de trabalho, sempre certifique-se de especificar um destinatário não anônimo usando o parâmetro. -

r A criptografia anônima (sem especificar um destinatário) pode causar falhas de decodificação no fluxo de trabalho porque o sistema não conseguirá identificar qual chave usar para decodificação. As informações de depuração desse problema estão disponíveis em. [Solucionar problemas de criptografia de destinatários anônimos](#)

4. Faça o upload do arquivo criptografado para o servidor Transfer Family.
5. Configure uma etapa de descriptografia em seu fluxo de trabalho. Para obter mais informações, consulte [Adicionar uma etapa de decodificação](#).

Adicionar uma etapa de decodificação

Uma etapa de descriptografia descriptografa um arquivo criptografado que foi carregado no Amazon S3 ou no Amazon EFS como parte do seu fluxo de trabalho. Para obter detalhes sobre como configurar a descriptografia, consulte [Use a descriptografia PGP em seu fluxo de trabalho](#).

Ao criar sua etapa de descriptografia para um fluxo de trabalho, você deve especificar o destino dos arquivos descriptografados. Você também deve selecionar se deseja substituir os arquivos existentes se um arquivo já existir no local de destino. Você pode monitorar os resultados do fluxo de trabalho de descriptografia e obter registros de auditoria para cada arquivo em tempo real usando o Amazon Logs. CloudWatch

Depois de escolher o tipo de Descriptografar arquivo para sua etapa, a página Configurar parâmetros é exibida. Preencha os valores da seção Configurar parâmetros de descriptografia do PGP.

As opções disponíveis são as seguintes:

- Nome da etapa — Insira um nome descritivo para a etapa.
- Local do arquivo — Ao especificar o local do arquivo, você pode descriptografar o arquivo usado na etapa anterior ou o arquivo original que foi carregado.

 Note

Esse parâmetro não estará disponível se essa etapa for a primeira etapa do fluxo de trabalho.

- Destino para arquivos descriptografados — Escolha um bucket do Amazon S3 ou um sistema de arquivos do Amazon EFS como destino para o arquivo descriptografado.
- Se você escolher o Amazon S3, deverá fornecer um nome de bucket de destino e um prefixo de chave de destino. Para parametrizar o prefixo da chave de destino por nome de usuário, insira `${transfer:UserName}` para Prefixo da chave de destino. Da mesma forma, para parametrizar o prefixo da chave de destino por data de carregamento, insira `${Transfer:UploadDate}` para Prefixo da chave de destino.
- Se você escolher o Amazon EFS, deverá fornecer um sistema de arquivos e um caminho de destino.

 Note

A opção de armazenamento escolhida aqui deve corresponder ao sistema de armazenamento usado pelo servidor Transfer Family ao qual esse fluxo de trabalho está associado. Caso contrário, você receberá um erro ao tentar executar esse fluxo de trabalho.

- Substituir existente — Se você fizer upload de um arquivo e já existir um arquivo com o mesmo nome de arquivo no destino, o comportamento dependerá da configuração desse parâmetro:
 - Se Substituir existente for selecionado, o arquivo existente será substituído pelo arquivo que está sendo processado.
 - Se a opção Substituir existente não estiver selecionada, nada acontecerá e o processamento do fluxo de trabalho será interrompido.

 Tip

Se as gravações simultâneas forem executadas no mesmo caminho de arquivo, isso poderá resultar em um comportamento inesperado ao substituir arquivos.

A captura de tela a seguir mostra um exemplo das opções que você pode escolher para a etapa de descriptografia do arquivo.

Step 1
Choose step type

Step 2
Configure parameters

Step 3
Review and create

Configure parameters

Configure PGP decryption parameters

Store your PGP private key(s) and passphrase(s) in AWS Secrets Manager. [Learn more](#)

 Refer to the [AWS Transfer Family pricing page](#) for pricing details. 

Step name

File location
Select the file location to use as an input for this step

☒ Apply on the file created from the previous step
Input file is selected from the previous step's output

☐ Apply on the original file
Originally uploaded file

Destination for decrypted files
Choose an S3 bucket or an EFS file system for storing decrypted files.

☒ Amazon S3
Store your decrypted files as Amazon S3 objects

☐ Amazon EFS
Store your decrypted files in an EFS file system

Destination bucket name

Destination key prefix
If you are decrypting files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize the destination prefix by username or upload date respectively.

☐ Overwrite existing
Overwrite if a file with the same file name already exists at the destination.

Descriptografar arquivo

488

Permissões do IAM para a etapa de descriptografar

Para permitir que uma etapa de descriptografia seja bem-sucedida, certifique-se de que a função de execução do seu fluxo de trabalho contenha as seguintes permissões.

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}, {
  "Sid": "Decrypt",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue",
  ],
  "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
}
```

Note

A permissão `s3:ListBucket` só é necessária se você não selecionar Substituir existente. Essa permissão verifica seu bucket para ver se já existe um arquivo com o mesmo nome. Se você selecionou Substituir existente, o fluxo de trabalho não precisa verificar o arquivo e pode simplesmente gravá-lo. Se seus arquivos do Amazon S3 tiverem tags, você precisará adicionar uma ou duas permissões à sua política do IAM.

- Adicione `s3:GetObjectTagging` para obter um arquivo Amazon S3 que não tenha versão.
- Adicione `s3:GetObjectVersionTagging` para obter um arquivo Amazon S3 que tenha versão.

Arquivo de marcação

Para marcar arquivos recebidos para processamento posterior, use uma etapa de marcação. Insira o valor da tag que você gostaria de atribuir aos arquivos recebidos. Atualmente, a operação de marcação é suportada somente se você estiver usando o Amazon S3 para o armazenamento do servidor Transfer Family.

O exemplo a seguir, a etapa de marcação atribui `scan_outcome` e `clean` como chave e valor da tag, respectivamente.

The screenshot shows a 'Configure tag parameters' dialog box. It has a 'Step name' field with the value 'tag scan'. Below it, the 'File location' section has two radio buttons: 'Tag the file created from previous step' (selected) and 'Tag the original source file'. The 'Tags' section has a table with two columns: 'Key' and 'Value'. The first row has 'scan_outcome' in the Key column and 'clean' in the Value column. At the bottom, there are 'Remove tag' and 'Add tag' buttons.

Key	Value
scan_outcome	clean

Para permitir que uma etapa de marcação seja bem-sucedida, certifique-se de que a função de execução do seu fluxo de trabalho contenha as seguintes permissões.

```
{
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
}
```

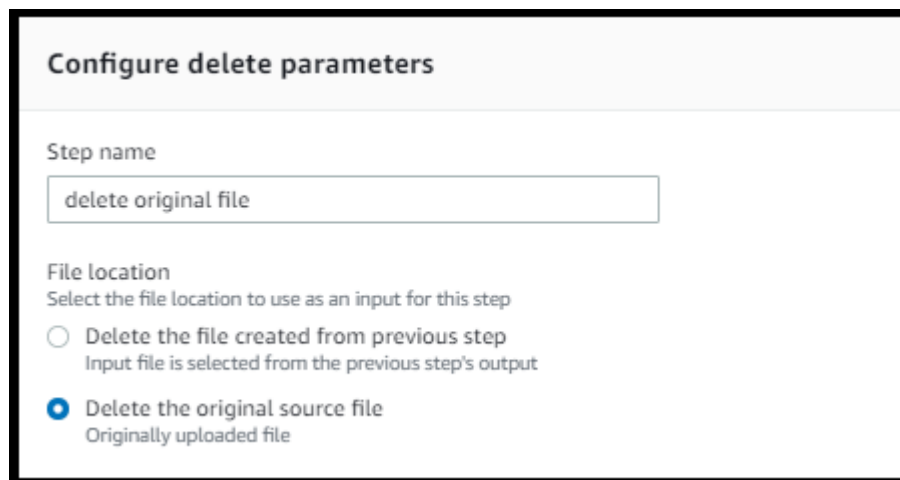
Note

Se seu fluxo de trabalho contiver uma etapa de marcação executada antes de uma etapa de cópia ou descryptografia, você precisará adicionar uma ou duas permissões à sua política do IAM.

- Adicione `s3:GetObjectTagging` para obter um arquivo Amazon S3 que não tenha versão.
- Adicione `s3:GetObjectVersionTagging` para obter um arquivo Amazon S3 que tenha versão.

Excluir arquivo

Para excluir um arquivo processado de uma etapa anterior do fluxo de trabalho ou excluir o arquivo originalmente carregado, use uma etapa de exclusão de arquivo.



Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

Para permitir que uma etapa de exclusão seja bem-sucedida, certifique-se de que a função de execução do seu fluxo de trabalho contenha as seguintes permissões.

```
{
    "Sid": "Delete",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObjectVersion",
        "s3:DeleteObject"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
* "
}
```

Variáveis nomeadas para fluxos de trabalho

Para etapas de cópia e descriptografia, você pode usar uma variável para executar ações dinamicamente. Atualmente, AWS Transfer Family oferece suporte às seguintes variáveis nomeadas.

- Use `${transfer:UserName}` para copiar ou descriptografar arquivos para um destino com base no usuário que está fazendo o upload dos arquivos.
- Use `${transfer:UploadDate}` para copiar ou descriptografar arquivos em um local de destino com base na data atual.

Exemplo para marcar e excluir fluxo de trabalho

O exemplo a seguir ilustra um fluxo de trabalho que marca os arquivos recebidos que precisam ser processados por um aplicativo downstream, como uma plataforma de análise de dados. Depois de marcar o arquivo de entrada, o fluxo de trabalho exclui o arquivo originalmente carregado para economizar nos custos de armazenamento.

Console

Exemplo para marcar e mover fluxo de trabalho

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, selecione Fluxos de trabalho.
3. Na página Fluxos de trabalho, escolha Criar um fluxo de trabalho.

4. Na página Criar fluxo de trabalho, insira uma descrição. Essa descrição aparece na página Fluxos de trabalho.
5. Adicione a primeira etapa (cópia).
 - a. Na seção Etapas nominais, escolha Adicionar etapa.
 - b. Escolha Copiar arquivo, e, em seguida, Próximo.
 - c. Insira o nome da etapa e selecione um bucket de destino e um prefixo de chave.

Step 1
Choose step type

Step 2
Configure parameters

Step 3
Review and create

Configure parameters

Configure copy parameters

Step name
copy-step-first-step

Destination bucket name
example-bucket ▼

Destination key prefix
If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.
test/

☐ Overwrite existing

- d. Escolha Próximo e, em seguida, revise os detalhes da etapa.
 - e. Escolha Criar etapa para adicionar a etapa e continuar.
6. Adicione a segunda etapa (tag).
 - a. Na seção Etapas nominais, escolha Adicionar etapa.
 - b. Escolha Marcar arquivo, e, em seguida, Próximo.
 - c. Insira um nome de etapa.
 - d. Em Local do arquivo, selecione Marcar o arquivo criado na etapa anterior.
 - e. Insira uma Chave e Valor.

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

- f. Escolha Próximo e, em seguida, revise os detalhes da etapa.
 - g. Escolha Criar etapa para adicionar a etapa e continuar.
7. Adicione a terceira etapa (excluir).
- a. Na seção Etapas nominais, escolha Adicionar etapa.
 - b. Escolha Excluir arquivo, e, em seguida, Próximo.

Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

- c. Insira um nome de etapa.

- d. Em Local do arquivo, selecione Excluir o arquivo de origem original.
 - e. Escolha Próximo e, em seguida, revise os detalhes da etapa.
 - f. Escolha Criar etapa para adicionar a etapa e continuar.
8. Reveja o fluxo de trabalho e selecione Criar fluxo de trabalho.

CLI

Exemplo para marcar e mover fluxo de trabalho

1. Salve o código a seguir em um arquivo; por exemplo, `tagAndMoveWorkflow.json`. Substitua cada *user input placeholder* por suas próprias informações.

```
[
  {
    "Type": "COPY",
    "CopyStepDetails": {
      "Name": "CopyStep",
      "DestinationFileLocation": {
        "S3FileLocation": {
          "Bucket": "amzn-s3-demo-bucket",
          "Key": "test/"
        }
      }
    }
  },
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "demo"
        }
      ],
      "SourceFileLocation": "${previous.file}"
    }
  },
  {
    "Type": "DELETE",
    "DeleteStepDetails":{
```

```
        "Name": "DeleteStep",
        "SourceFileLocation": "${original.file}"
    }
}
]
```

A primeira etapa copia o arquivo carregado para um novo local do Amazon S3. A segunda etapa adiciona uma tag (par de valor-chave) ao arquivo (`previous.file`) que foi copiado para o novo local. E, finalmente, a terceira etapa exclui o arquivo original (`original.file`).

2. Crie um fluxo de trabalho a partir do arquivo salvo. Substitua cada *user input placeholder* por suas próprias informações.

```
aws transfer create-workflow --description "short-description" --steps
file://path-to-file --region region-ID
```

Por exemplo:

```
aws transfer create-workflow --description "copy-tag-delete workflow" --steps
file://tagAndMoveWorkflow.json --region us-east-1
```

 Note

Para obter mais detalhes sobre o uso de arquivos para carregar parâmetros, consulte [Como carregar parâmetros de um arquivo](#).

3. Atualizar um servidor existente.

 Note

Essa etapa pressupõe que você já tenha um servidor Transfer Family e queira associar um fluxo de trabalho a ele. Se não, consulte [Configurando um endpoint de servidor SFTP, FTPS ou FTP](#). Substitua cada *user input placeholder* por suas próprias informações.

```
aws transfer update-server --server-id server-ID --region region-ID
```

```
--workflow-details '{"OnUpload":[{"WorkflowId": "workflow-ID", "ExecutionRole": "execution-role-ARN"}]}'
```

Por exemplo:

```
aws transfer update-server --server-id s-1234567890abcdef0 --region us-east-2  
--workflow-details '{"OnUpload":[{"WorkflowId": "w-  
abcdef01234567890", "ExecutionRole": "arn:aws:iam::111111111111:role/nikki-wolf-  
execution-role"}]}'
```

Use etapas personalizadas de processamento de arquivos

Ao usar uma etapa personalizada de processamento de arquivos, você pode trazer sua própria lógica de processamento de arquivos usando AWS Lambda. Na chegada do arquivo, um servidor Transfer Family invoca uma função do Lambda que contém uma lógica de processamento de arquivos personalizada, como criptografia de arquivos, verificação de malware ou verificação de tipos de arquivo incorretos. No exemplo a seguir, a função de destino AWS Lambda é usada para processar o arquivo de saída da etapa anterior.

Configure custom parameters

Step name
custom file processing step

File location
Select the file location to use as an input for this step

☒ Apply custom processing to the file created from previous step
Input file is selected from the previous step's output

☐ Apply custom processing to the original source file
Originally uploaded file

Target
am:aws:lambda:us-east-2:1234567... ▼

Timeout (seconds)
60

Note

Para obter um exemplo de função do Lambda, consulte [Exemplo de função do Lambda para uma etapa de fluxo de trabalho personalizada](#). Para eventos de exemplo (incluindo a localização dos arquivos passados para o Lambda), consulte [Exemplos de eventos enviados para AWS Lambda após o upload do arquivo](#).

Com uma etapa de fluxo de trabalho personalizada, você deve configurar a função Lambda para chamar a operação da [SendWorkflowStepState](#) API. `SendWorkflowStepState` notifica a execução do fluxo de trabalho de que a etapa foi concluída com status de sucesso ou falha. O status da operação da API `SendWorkflowStepState` invoca uma etapa do manipulador de exceções ou uma etapa nominal na sequência linear, com base no resultado da função do Lambda.

Se a função Lambda falhar ou atingir o tempo limite, a etapa falhará e você verá `StepErrored` nos seus CloudWatch registros. Se a função do Lambda fizer parte da etapa nominal e a função responder `SendWorkflowStepState` com `Status="FAILURE"` ou expirar, o fluxo continuará com as etapas do manipulador de exceções. Nesse caso, o fluxo de trabalho não continua executando as etapas nominais restantes (se houver). Consulte mais detalhes em [Tratamento de exceções para um fluxo de trabalho](#).

Ao chamar a operação da API `SendWorkflowStepState`, você deve enviar os seguintes parâmetros:

```
{
  "ExecutionId": "string",
  "Status": "string",
  "Token": "string",
  "WorkflowId": "string"
}
```

Você pode extrair `ExecutionId`, `Token`, e `WorkflowId` do evento de entrada que é passado quando a função do Lambda é executada (exemplos são mostrados nas seções a seguir). O valor de `Status` pode ser `SUCCESS` ou `FAILURE`.

Para poder chamar a operação da `SendWorkflowStepState` API a partir da sua função Lambda, você deve usar uma versão do AWS SDK que foi publicada após a introdução dos fluxos de [trabalho gerenciados](#).

Usando várias funções do Lambda consecutivamente

Quando você usa várias etapas personalizadas uma após a outra, a opção Local do arquivo funciona de forma diferente do que se você usasse apenas uma única etapa personalizada. O Transfer Family não suporta a devolução do Lambda-processed arquivo para ser usado como entrada na próxima etapa. Portanto, se você tiver várias etapas personalizadas configuradas para usar a opção `previous.file`, todas usarão o mesmo local de arquivo (o local do arquivo de entrada da primeira etapa personalizada).

Note

A configuração `previous.file` também funciona de forma diferente se você tiver uma etapa predefinida (marcar, copiar, descriptografar ou excluir) após uma etapa personalizada. Se a etapa predefinida estiver configurada para usar a configuração `previous.file`, a etapa predefinida usará o mesmo arquivo de entrada usado pela etapa personalizada. O arquivo processado da etapa personalizada não é passado para a etapa predefinida.

Acessar um arquivo após o processamento personalizado

Se você estiver usando o Amazon S3 como armazenamento e se seu fluxo de trabalho incluir uma etapa personalizada que executa ações no arquivo originalmente carregado, as etapas subsequentes não poderão acessar esse arquivo processado. Ou seja, qualquer etapa após a etapa personalizada não pode referenciar o arquivo atualizado a partir da saída da etapa personalizada.

Por exemplo, digamos que você tenha as três etapas a seguir no fluxo de trabalho.

- Etapa 1 — Faça o upload de um arquivo chamado `example-file.txt`.
- Etapa 2 — Invoque uma função do Lambda que muda o `example-file.txt` de alguma forma.
- Etapa 3 — Tente realizar um processamento adicional na versão atualizada do `example-file.txt`.

Se você configurar o `sourceFileLocation` da Etapa 3 para ser `${original.file}`, a Etapa 3 usará o local do arquivo original de quando o servidor carregou o arquivo para o armazenamento na Etapa 1. Se você estiver usando o `${previous.file}` na Etapa 3, a Etapa 3 reutiliza o local do arquivo que a Etapa 2 usou como entrada.

Portanto, a Etapa 3 causa um erro. Por exemplo, se a Etapa 3 tentar copiar o `example-file.txt` atualizado, você receberá o seguinte erro:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "NOT_FOUND",
    "errorMessage": "ETag constraint not met (Service: null; Status Code: 412; Error Code: null; Request ID: null; S3 Extended Request ID: null; Proxy: null)",
    "stepType": "COPY",
    "stepName": "CopyFile"
  },
}
```

Esse erro ocorre porque a etapa personalizada modifica a tag da entidade (ETag) para `example-file.txt`, portanto isso não corresponde ao arquivo original.

Note

Esse comportamento não ocorre se você estiver usando o Amazon EFS porque o Amazon EFS não usa tags de entidade para identificar arquivos.

Exemplos de eventos enviados para AWS Lambda após o upload do arquivo

Os exemplos a seguir mostram os eventos que são enviados AWS Lambda quando o upload de um arquivo é concluído. Um exemplo usa um servidor Transfer Family em que o domínio é configurado com o Amazon S3. O outro exemplo usa um servidor Transfer Family em que o domínio usa o Amazon EFS.

Custom step that uses an Amazon S3 domain

```
{
  "token": "MzI0Nzc4ZDktMGRmMi00MjFhLTgxMjUtYWZmZmRmODNkYjc0",
  "serviceMetadata": {
    "executionDetails": {
      "workflowId": "w-1234567890example",
      "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
    },
  },
  "transferDetails": {
```



```

        "sessionId": "36688ff5d2deda8c",
        "userName": "myuser",
        "serverId": "s-example1234567890"
    },
    "fileLocation": {
        "domain": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "path/to/mykey",
        "eTag": "d8e8fca2dc0f896fd7cb4cb0031ba249",
        "versionId": null
    }
}

```

Custom step that uses an Amazon EFS domain

```

{
  "token": "MTg0N2Y3N2UtNWl5Ny00ZmZlLTk5YTgtZTU3YzViYjllNmZm",
  "serviceMetadata": {
    "executionDetails": {
      "workflowId": "w-1234567890example",
      "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
    },
    "transferDetails": {
      "sessionId": "36688ff5d2deda8c",
      "userName": "myuser",
      "serverId": "s-example1234567890"
    }
  },
  "fileLocation": {
    "domain": "EFS",
    "fileSystemId": "fs-1234567",
    "path": "/path/to/myfile"
  }
}

```

Exemplo de função do Lambda para uma etapa de fluxo de trabalho personalizada

A função Lambda a seguir extrai as informações sobre o status de execução e, em seguida, chama a operação da [SendWorkflowStepState](#) API para retornar o status ao fluxo de trabalho

da etapa, ou seja. SUCCESS FAILURE Antes de sua função chamar a operação da API `SendWorkflowStepState`, você pode configurar o Lambda para realizar uma ação com base na lógica do seu fluxo de trabalho.

```
import json
import boto3

transfer = boto3.client('transfer')

def lambda_handler(event, context):
    print(json.dumps(event))

    # call the SendWorkflowStepState API to notify the workflow about the step's
    # SUCCESS or FAILURE status
    response = transfer.send_workflow_step_state(
        WorkflowId=event['serviceMetadata']['executionDetails']['workflowId'],
        ExecutionId=event['serviceMetadata']['executionDetails']['executionId'],
        Token=event['token'],
        Status='SUCCESS|FAILURE'
    )

    print(json.dumps(response))

    return {
        'statusCode': 200,
        'body': json.dumps(response)
    }
```

Permissões do IAM para a etapa de personalizar

Para permitir que uma etapa que chama o Lambda seja bem-sucedida, certifique-se de que a função de execução do seu fluxo de trabalho contenha as seguintes permissões.

```
{
  "Sid": "Custom",
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": [
    "arn:aws:lambda:region:account-id:function:function-name"
  ]
}
```

```
}
```

Políticas do IAM para fluxos de trabalho

Ao adicionar um fluxo de trabalho a um servidor, você deve selecionar uma função de execução. O servidor usa essa função ao executar o fluxo de trabalho. Se a função não tiver as permissões adequadas, não será AWS Transfer Family possível executar o fluxo de trabalho.

Esta seção descreve um conjunto possível de permissões AWS Identity and Access Management (IAM) que você pode usar para executar um fluxo de trabalho. Outros exemplos são descritos mais adiante neste tópico.

Note

Se seus arquivos do Amazon S3 tiverem tags, você precisará adicionar uma ou duas permissões à sua política do IAM.

- Adicione `s3:GetObjectTagging` para obter um arquivo Amazon S3 que não tenha versão.
- Adicione `s3:GetObjectVersionTagging` para obter um arquivo Amazon S3 que tenha versão.

Como criar uma função de execução para o seu fluxo de trabalho

1. Crie uma nova função do IAM e adicione a política AWS gerenciada `AWSTransferFullAccess` à função. Para obter mais informações sobre como criar um perfil do IAM, consulte [the section called “Criar uma política e um perfil do IAM”](#).
2. Crie outra política com as seguintes permissões e anexe-a ao seu perfil. Substitua cada *user input placeholder* por suas próprias informações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConsoleAccess",
      "Effect": "Allow",
      "Action": "s3:GetBucketLocation",
```

```

    "Resource": "*"
  },
  {
    "Sid": "ListObjectsInBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
  },
  {
    "Sid": "AllObjectActions",
    "Effect": "Allow",
    "Action": "s3:*Object",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Sid": "GetObjectVersion",
    "Effect": "Allow",
    "Action": "s3:GetObjectVersion",
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Sid": "Custom",
    "Effect": "Allow",
    "Action": [
      "lambda:InvokeFunction"
    ],
    "Resource": [
      "arn:aws:lambda:us-east-1:123456789012:function:function-name"
    ]
  },
  {
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
      "s3:PutObjectTagging",
      "s3:PutObjectVersionTagging"
    ],
    "Resource": [

```

```

        "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
}
]
}

```

3. Salve essa função e especifique-a como a função de execução ao adicionar um fluxo de trabalho a um servidor.

Note

Ao criar funções do IAM, AWS recomenda que você restrinja o acesso aos seus recursos o máximo possível para seu fluxo de trabalho.

relação de confiança no fluxo de trabalho

As funções de execução do fluxo de trabalho também exigem uma relação de confiança com `transfer.amazonaws.com`. Para estabelecer uma relação de confiança para AWS Transfer Family, consulte [Estabelecer um relacionamento de confiança](#).

Ao estabelecer sua relação de confiança, você também pode tomar medidas para evitar o problema substituto confuso. Para obter uma descrição desse problema, bem como exemplos de como evitá-lo, consulte [the section called “Cross-service prevenção delegada confusa”](#).

Exemplo de função de execução: descriptografar, copiar e marcar

Se você tiver fluxos de trabalho que incluem etapas de marcação, cópia e descriptografia, você pode usar a seguinte política do IAM. Substitua cada *user input placeholder* por suas próprias informações.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyRead",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging",

```

```

        "s3:GetObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
},
{
    "Sid": "CopyWrite",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
},
{
    "Sid": "CopyList",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
},
{
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
    "Condition": {
        "StringEquals": {
            "s3:RequestObjectTag/Archive": "yes"
        }
    }
},
{
    "Sid": "ListBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
},

```

```

{
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
},
{
  "Sid": "Decrypt",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue"
  ],
  "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/transfer/*"
}
]
}

```

Exemplo de função de execução: executar função e excluir

Neste exemplo, você tem um fluxo de trabalho que invoca uma AWS Lambda função. Se o fluxo de trabalho excluir o arquivo carregado e tiver uma etapa de manipulador de exceções para agir em caso de falha na execução do fluxo de trabalho na etapa anterior, use a seguinte política do IAM. Substitua cada *user input placeholder* por suas próprias informações.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Delete",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],

```

```

        "Resource": "arn:aws:s3::bucket-name"
    },
    {
        "Sid": "Custom",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": [
            "arn:aws:lambda:us-east-1:123456789012:function:function-name"
        ]
    }
]
}

```

Tratamento de exceções para um fluxo de trabalho

Se algum erro ocorrer durante a execução de um fluxo de trabalho, as etapas de tratamento de exceções que você especificou serão executadas. Você especifica as etapas de tratamento de erros para um fluxo de trabalho da mesma forma que especifica as etapas nominais para o fluxo de trabalho. Por exemplo, suponha que você tenha configurado o processamento personalizado em etapas nominais para validar os arquivos recebidos. Se a validação do arquivo falhar, uma etapa de tratamento de exceções poderá enviar um e-mail ao administrador.

O exemplo de fluxo de trabalho a seguir contém duas etapas:

- Uma etapa nominal que verifica se o arquivo carregado está no formato CSV
- Uma etapa de tratamento de exceções que envia um e-mail caso o arquivo carregado não esteja no formato CSV e a etapa nominal falhe

Para iniciar a etapa de tratamento de exceções, a AWS Lambda função na etapa nominal deve responder com. `Status="FAILURE"` Para obter mais informações sobre como tratar erros, consulte [the section called “Use etapas personalizadas de processamento de arquivos”](#).

w-1234567890abcdef0
Delete

Description

Name
Delete after upload

Workflow description
test-my-workflow

Nominal steps (1) Info

Number	Description	Type	Configuration
1	is-CSV	CUSTOM	Details

Exception handlers (1) Info

Number	Description	Type	Configuration
1	send-email	CUSTOM	Details

Monitore a execução do fluxo

A Amazon CloudWatch monitora seus AWS recursos e os aplicativos que você executa Nuvem AWS em tempo real. Você pode usar CloudWatch a Amazon para coletar e rastrear métricas, que são variáveis que você pode medir para seus fluxos de trabalho. Você pode visualizar métricas de fluxo de trabalho e registros consolidados usando a Amazon CloudWatch.

CloudWatch registro para um fluxo de trabalho

CloudWatch fornece auditoria e registro consolidados para o progresso e os resultados do fluxo de trabalho.

Veja os CloudWatch registros da Amazon para fluxos de trabalho

1. Abra o CloudWatch console da Amazon em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação à esquerda, escolha Logs e, em seguida, escolha Grupos de logs.
3. Na página Grupos de registros, na barra de navegação, escolha a região correta para seu AWS Transfer Family servidor.
4. Escolha o grupo de logs que corresponde ao seu servidor.

Por exemplo, se o ID do seu servidor for `s-1234567890abcdef0`, seu grupo de logs será `/aws/transfer/s-1234567890abcdef0`.

- Na página de detalhes do grupo de logs do seu servidor, os fluxos de log mais recentes são exibidos. Há dois fluxos de log para o usuário que você está explorando:
 - Um para cada sessão do File Transfer Protocol (SFTP) da Secure Shell (SSH).
 - Um para o fluxo de trabalho que está sendo executado no seu servidor. O formato do fluxo de logs do fluxo de trabalho é `username.workflowID.uniqueStreamSuffix`.

Por exemplo, se o seu usuário é `mary-major`, você terá os seguintes fluxos de logs:

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

 Note

Os identificadores alfanuméricos de 16 dígitos listados neste exemplo são fictícios. Os valores que você vê na Amazon CloudWatch são diferentes.

A página Eventos de log para o `mary-major-usa-east.1234567890abcdef0` exibe os detalhes de cada sessão do usuário, e o fluxo de logs para o `mary.w-abcdef01234567890.021345abcdef6789` contém os detalhes do fluxo de trabalho.

Veja a seguir um exemplo de fluxo de logs para o `mary.w-abcdef01234567890.021345abcdef6789`, com base em um fluxo de trabalho (`w-abcdef01234567890`) que contém uma etapa de cópia.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  }
}
```

```

    }
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
},
{
  "type": "StepStarted",
  "details": {
    "input": {
      "fileLocation": {
        "backingStore": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    },
    "stepType": "COPY",
    "stepName": "copyToShared"
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
},
{
  "type": "StepCompleted",
  "details": {
    "output": {},
    "stepType": "COPY",
    "stepName": "copyToShared"
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "server-id",

```

```
        "username": "mary",
        "sessionId": "session-id"
    },
    {
        "type": "ExecutionCompleted",
        "details": {},
        "workflowId": "w-abcdef01234567890",
        "executionId": "execution-id",
        "transferDetails": {
            "serverId": "s-server-id",
            "username": "mary",
            "sessionId": "session-id"
        }
    }
}
```

CloudWatch métricas para fluxos de trabalho

AWS Transfer Family fornece várias métricas para fluxos de trabalho. Você pode visualizar métricas de quantas execuções de fluxos de trabalho foram iniciadas, concluídas com êxito e falharam no minuto anterior. Todas as CloudWatch métricas do Transfer Family estão descritas em [Usando CloudWatch métricas para servidores Transfer Family](#).

Criar um fluxo de trabalho a partir de um modelo

Você pode implantar uma CloudFormation pilha que cria um fluxo de trabalho e um servidor a partir de um modelo. Esse procedimento contém um exemplo que você pode usar para implantar rapidamente um fluxo de trabalho.

Para criar uma CloudFormation pilha que cria um AWS Transfer Family fluxo de trabalho e um servidor

1. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. Salve o seguinte código em um arquivo.

YAML

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  SFTPServer:
    Type: 'AWS::Transfer::Server'
```

```

Properties:
  WorkflowDetails:
    OnUpload:
      - ExecutionRole: workflow-execution-role-arn
        WorkflowId: !GetAtt
          - TransferWorkflow
          - WorkflowId
  TransferWorkflow:
    Type: AWS::Transfer::Workflow
  Properties:
    Description: Transfer Family Workflows Blog
    Steps:
      - Type: COPY
        CopyStepDetails:
          Name: copyToUserKey
          DestinationFileLocation:
            S3FileLocation:
              Bucket: archived-records
              Key: ${transfer:UserName}/
            OverwriteExisting: 'TRUE'
      - Type: TAG
        TagStepDetails:
          Name: tagFileForArchive
          Tags:
            - Key: Archive
              Value: yes
      - Type: CUSTOM
        CustomStepDetails:
          Name: transferExtract
          Target: arn:aws:lambda:region:account-id:function:function-name
          TimeoutSeconds: 60
      - Type: DELETE
        DeleteStepDetails:
          Name: DeleteInputFile
          SourceFileLocation: '${original.file}'
    Tags:
      - Key: Name
        Value: TransferFamilyWorkflows

```

JSON

```

{
  "AWSTemplateFormatVersion": "2010-09-09",

```

```

"Resources": {
  "SFTPServer": {
    "Type": "AWS::Transfer::Server",
    "Properties": {
      "WorkflowDetails": {
        "OnUpload": [
          {
            "ExecutionRole": "workflow-execution-role-arn",
            "WorkflowId": {
              "Fn::GetAtt": [
                "TransferWorkflow",
                "WorkflowId"
              ]
            }
          ]
        }
      }
    }
  },
  "TransferWorkflow": {
    "Type": "AWS::Transfer::Workflow",
    "Properties": {
      "Description": "Transfer Family Workflows Blog",
      "Steps": [
        {
          "Type": "COPY",
          "CopyStepDetails": {
            "Name": "copyToUserKey",
            "DestinationFileLocation": {
              "S3FileLocation": {
                "Bucket": "archived-records",
                "Key": "${transfer:UserName}/"
              }
            },
            "OverwriteExisting": "TRUE"
          }
        },
        {
          "Type": "TAG",
          "TagStepDetails": {
            "Name": "tagFileForArchive",
            "Tags": [
              {
                "Key": "Archive",

```

```

        "Value": "yes"
      }
    ]
  },
  {
    "Type": "CUSTOM",
    "CustomStepDetails": {
      "Name": "transferExtract",
      "Target": "arn:aws:lambda:region:account-id:function:function-name",
      "TimeoutSeconds": 60
    }
  },
  {
    "Type": "DELETE",
    "DeleteStepDetails": {
      "Name": "DeleteInputFile",
      "SourceFileLocation": "${original.file}"
    }
  }
],
"Tags": [
  {
    "Key": "Name",
    "Value": "TransferFamilyWorkflows"
  }
]
}
}
}
}
}

```

3. Substitua os seguintes itens pelo seus próprios.

- Substitua *workflow-execution-role-arn* pelo ARN de uma função de execução de fluxo de trabalho real. Por exemplo, `arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`.
- Substitua `arn:aws:lambda:region:account-id:function:function-name` pelo ARN da sua função do Lambda. Por exemplo, `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`

4. Siga as instruções para implantar uma CloudFormation pilha a partir de um modelo existente em [Seleção de um modelo de pilha no Guia](#) do AWS CloudFormation usuário.

Depois que a pilha for implantada, você poderá ver detalhes sobre ela na guia Saídas no console. CloudFormation O modelo cria um novo servidor AWS Transfer Family SFTP que usa usuários gerenciados pelo serviço e um novo fluxo de trabalho e associa o fluxo de trabalho ao novo servidor.

Remover um fluxo de trabalho de um servidor Transfer Family

Se você associou um fluxo de trabalho a um servidor Transfer Family e agora deseja remover essa associação, pode fazer isso usando o console ou programaticamente.

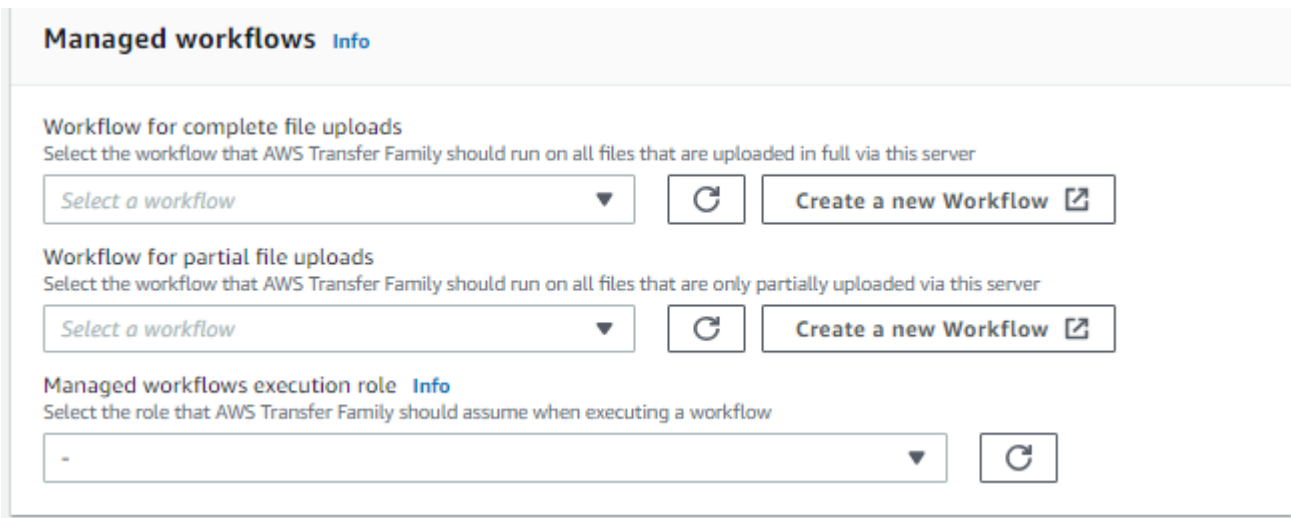
Console

Para remover um fluxo de trabalho de um servidor Transfer Family

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, selecione Servidores.
3. Escolha o identificador do servidor na coluna ID do servidor.
4. Na página de detalhes do servidor, role para baixo até a seção Detalhes adicionais e escolha Editar.
5. Na página Editar detalhes adicionais, na seção Fluxos de trabalho gerenciados, limpe as informações de todas as configurações:
 - Selecione o traço (-) na lista de fluxos de trabalho do Fluxo de trabalho para fazer upload completo dos arquivos.
 - Se já não estiver desmarcado, selecione o traço (-) na lista de fluxos de trabalho do Fluxo de trabalho para fazer upload parcial dos arquivos.
 - Selecione o traço (-) na lista de funções para a função de Execução de fluxos de trabalho gerenciados.

Se você não vê o traço, role para cima até vê-lo, pois é o primeiro valor em cada menu.

A tela deve ser algo semelhante ao exibido a seguir.



Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

Select a workflow ▼  [Create a new Workflow](#) 

Workflow for partial file uploads
Select the workflow that AWS Transfer Family should run on all files that are only partially uploaded via this server

Select a workflow ▼  [Create a new Workflow](#) 

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

- ▼ 

6. Role para baixo e selecione Salvar para salvar suas alterações.

CLI

Você usa a chamada `update-server` (ou `UpdateServer` para API) e fornece argumentos vazios para os parâmetros `OnUpload` e `OnPartialUpload`.

A partir do AWS CLI, execute o seguinte comando:

```
aws transfer update-server --server-id your-server-id --workflow-details  
'{"OnPartialUpload":[],"OnUpload":[]}'
```

Substitua *your-server-id* pelo ID do seu servidor. Por exemplo, se o ID do seu servidor for `s-01234567890abcdef`, o comando será o seguinte:

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details  
'{"OnPartialUpload":[],"OnUpload":[]}'
```

Restrições e limitações de fluxos de trabalho gerenciados

Restrições

Atualmente, as restrições a seguir se aplicam aos fluxos de trabalho de processamento pós-upload do AWS Transfer Family.

- Cross-account e AWS Lambda as funções entre regiões não são suportadas. No entanto, você pode copiar entre contas, desde que suas políticas AWS Identity and Access Management (IAM) estejam configuradas corretamente.
- Para todas as etapas do fluxo de trabalho, todos os buckets do Amazon S3 acessados pelo fluxo de trabalho devem estar na mesma região do próprio fluxo de trabalho.
- Para uma etapa de descritografia, o destino da descritografia deve corresponder à origem da região e do armazenamento secundário (por exemplo, se o arquivo a ser descritografado estiver armazenado no Amazon S3, o destino especificado também deverá estar no Amazon S3).
- Somente etapas personalizadas assíncronas são suportadas.
- Os tempos limite de etapa personalizados são aproximados. Ou seja, o tempo limite pode demorar um pouco mais do que o especificado. Além disso, o fluxo de trabalho depende da função do Lambda. Portanto, se a função for atrasada durante a execução, o fluxo de trabalho não estará ciente do atraso.
- Se você exceder seu limite de controle de utilização, o Transfer Family não adicionará operações de fluxo de trabalho à fila.
- Os fluxos de trabalho não são iniciados para arquivos com tamanho 0. Arquivos com tamanho maior que 0 iniciam o fluxo de trabalho associado.
- Você pode anexar um fluxo de trabalho de processamento de arquivos a um servidor Transfer Family que usa o protocolo AS2; no entanto, as mensagens AS2 não executam fluxos de trabalho conectados ao servidor.

Limitações

Além disso, os seguintes limites funcionais se aplicam aos fluxos de trabalho do Transfer Family:

- O número de fluxos de trabalho por região, por conta, é limitado a 10.
- O tempo limite máximo para etapas personalizadas é de 30 minutos.
- O número máximo de etapas em um fluxo de trabalho é 8.
- O número máximo de tags por fluxo de trabalho é 50.
- O número máximo de execuções simultâneas que contêm uma etapa de descritografia é 250 por fluxo de trabalho.
- Você pode armazenar no máximo 3 chaves privadas PGP por servidor Transfer Family por usuário.
- O tamanho máximo de um arquivo descritografado é 10 GB.

- Nós aceleramos a nova taxa de execução usando um sistema de [bucket de token](#) com uma capacidade de expansão de 100 e uma taxa de recarga de 1.
- Sempre que você remove um fluxo de trabalho de um servidor e o substitui por um novo ou atualiza a configuração do servidor (o que afeta a função de execução de um fluxo de trabalho), você deve esperar aproximadamente 10 minutos antes de executar o novo fluxo de trabalho. O servidor do Transfer Family armazena em cache os detalhes do fluxo de trabalho e leva 10 minutos para que o servidor atualize o cache.

Além disso, você deve sair de qualquer sessão ativa de SFTP e, em seguida, fazer login novamente após o período de espera de 10 minutos para ver as alterações.

Gerenciamento de servidores

Nesta seção, você pode encontrar informações sobre como visualizar uma lista dos seus servidores, como visualizar os detalhes do seu servidor, como editar os detalhes do seu servidor e como alterar a chave do host do seu SFTP-enabled servidor.

Tópicos

- [Exibir uma lista de servidores](#)
- [Excluir um servidor](#)
- [Exibir detalhes do servidor SFTP, FTPS e FTP](#)
- [Exibir detalhes do servidor AS2](#)
- [Suporte IPv6 para servidores Transfer Family](#)
- [Editar detalhes do servidor](#)
- [Editar a configuração do provedor de identidade](#)
- [Gerencie as chaves de host SFTP-enabled do seu servidor](#)
- [Monitoramento do uso no console](#)

Exibir uma lista de servidores

No AWS Transfer Family console, você pode encontrar uma lista de todos os seus servidores que estão localizados na AWS região que você escolheu.

Para encontrar uma lista dos seus servidores que existem em uma AWS região

- Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.

Se você tiver um ou mais servidores na AWS região atual, o console será aberto para mostrar uma lista dos seus servidores. Se não vir uma lista de servidores, verifique se você está na região correta. Você também pode escolher Servidores no painel de navegação.

Para obter mais informações sobre como visualizar os detalhes do servidor, consulte o [Exibir detalhes do servidor SFTP, FTPS e FTP](#).

Excluir um servidor

Este procedimento explica como excluir um servidor Transfer Family usando o AWS Transfer Family console ou AWS CLI.

Important

Você é cobrado por cada um dos protocolos habilitados para acessar seu endpoint até excluir o servidor.

Warning

A exclusão de um servidor resulta na exclusão de todos os seus usuários. Os dados no bucket que foram acessados usando o servidor não são excluídos e permanecem acessíveis aos usuários do AWS que têm privilégios nesses buckets do Amazon S3.

Console

Para excluir um servidor usando o console

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, selecione Servidores.
3. Marque a caixa de seleção do servidor que você deseja excluir.
4. Em Ações, escolha Excluir.
5. Na caixa de diálogo de confirmação exibida, insira a palavra **delete** e, em seguida, escolha Excluir para confirmar que deseja excluir o servidor.

O servidor é excluído da página Servidores e você não é mais cobrado por ele.

AWS CLI

Para excluir um servidor usando a CLI

1. (Opcional) Execute o comando a seguir para ver os detalhes do servidor que você deseja excluir permanentemente.

```
aws transfer describe-server --server-id your-server-id
```

Esse `describe-server` comando retorna todos os detalhes do seu servidor.

2. Execute o comando a seguir para excluir o servidor.

```
aws transfer delete-server --server-id your-server-id
```

Se for bem-sucedido, o comando excluirá o servidor e não retornará nenhuma informação.

Exibir detalhes do servidor SFTP, FTPS e FTP

Você pode encontrar uma lista de detalhes e propriedades de um AWS Transfer Family servidor individual. As propriedades do servidor incluem protocolos, provedor de identidade, status, tipo de endpoint, nome de host personalizado, endpoint, usuários, função de registro em log, chave de host do servidor e tags.

Para exibir detalhes do servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores.
3. Escolha o identificador na coluna ID do servidor para ver a página Detalhes do servidor, exibida a seguir.

Você pode alterar as propriedades do servidor nessa página escolhendo Editar. Para mais informações sobre como editar detalhes do servidor, consulte [Editar detalhes do servidor](#).

A página de detalhes dos servidores AS2 é um pouco diferente. Para servidores AS2, consulte [Exibir detalhes do servidor AS2](#).

Protocols

Protocols over which clients can connect to your server's endpoint

- SFTP

[Edit](#)

Identity provider

Identity provider type
Service managed

[Edit](#)

Note

Os valores de Descrição e Data de importação da chave do host do servidor são de setembro de 2022. Esses valores foram introduzidos para oferecer suporte ao atributo de várias chaves de host. Esse atributo exigia a migração de qualquer chave de host única que estivesse em uso antes da introdução de várias chaves de host.

O valor da Data da importação de uma chave de host do servidor migrado é definido como a data da última modificação do servidor. Ou seja, a data que você vê para sua chave de host migrada corresponde à data em que você modificou o servidor pela última vez de alguma forma, antes da migração da chave de host do servidor.

A única chave que foi migrada é a sua chave de host de servidor mais antiga ou única. Todas as chaves adicionais têm a data efetiva de quando você as importou. Além disso, a chave migrada tem uma descrição que facilita identificá-la como tendo sido migrada. A migração ocorreu entre 2 e 13 de setembro. A data efetiva da migração dentro desse intervalo depende da região do seu servidor.

Additional details[Edit](#)**Log group**[/aws/transfer/s-](#)**Logging role** [Info](#)

-

Security Policy [Info](#)

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

Domain

Amazon S3

Login display banner[View the display message](#)**Optimized directories** [Info](#)

ENABLED

SetStat option

Ignore

TLS session resumption

-

Passive IP

-

Exibir detalhes do servidor AS2

Você pode encontrar uma lista de detalhes e propriedades de um AWS Transfer Family servidor individual. As propriedades do servidor incluem protocolos, status e muito mais. Para servidores AS2, você também pode visualizar os endereços IP de saída MDN assíncronos do AS2.

Protocols

Edit

Protocols over which clients can connect to your server's endpoint

- AS2

Identity provider

Edit

 **AS2 Auth**
Basic authentication is not supported for AS2. Access can be controlled through VPC security groups.

Cada servidor AS2 recebe três endereços IP estáticos. Use esses endereços IP para enviar mDNS assíncrono para seus parceiros comerciais pelo AS2.

AS2 asynchronous MDN egress IP details

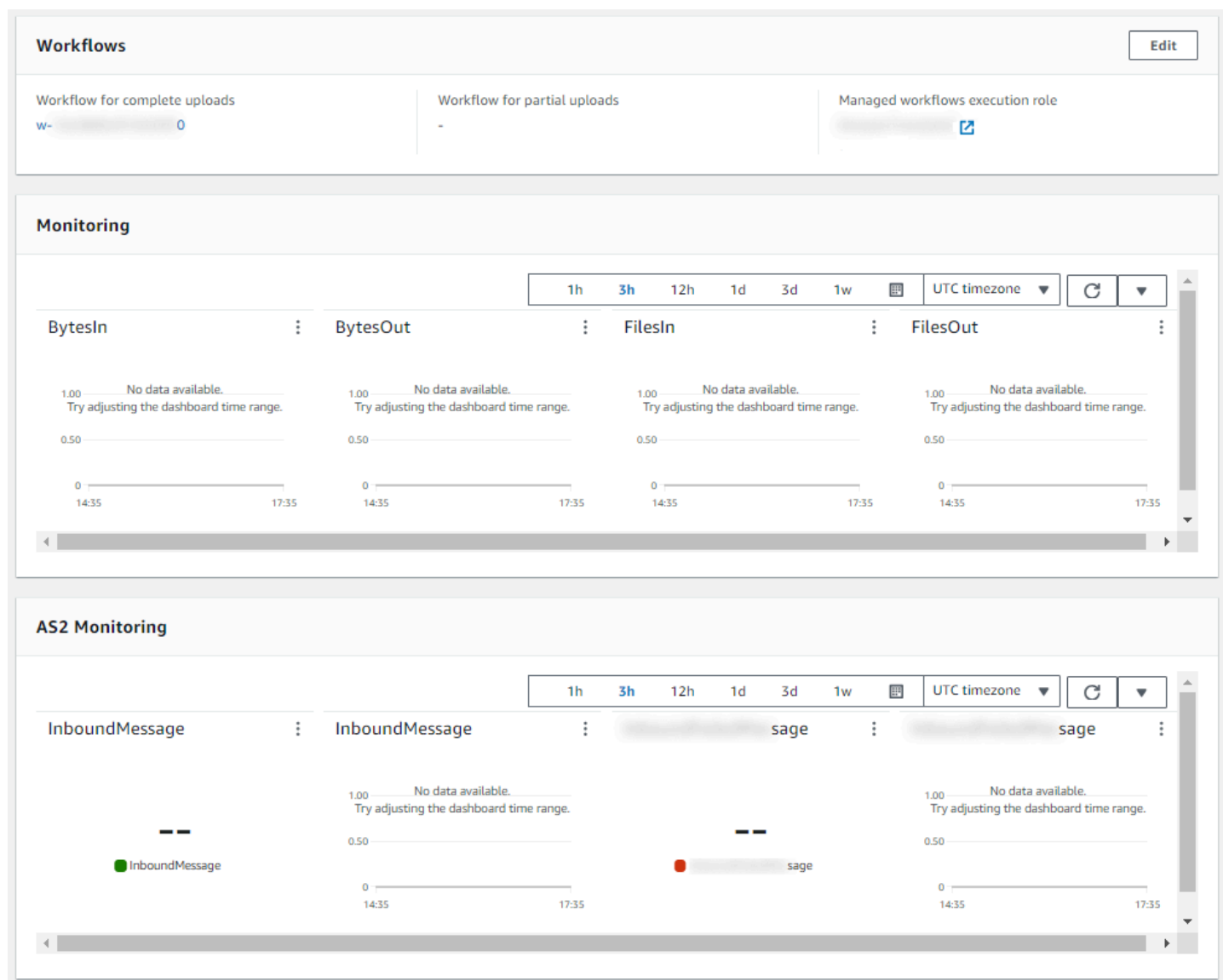
Below are the service managed static IP addresses used for sending your asynchronous MDNs to trading partners over AS2







A parte inferior da página de detalhes do servidor AS2 contém detalhes de qualquer fluxo de trabalho anexado e informações de monitoramento e marcação.



Suporte IPv6 para servidores Transfer Family

AWS Transfer Family suporta endpoints de pilha dupla (IPv4 e IPv6) para os seguintes recursos:

- Endpoints públicos SFTP
- Endpoints internos de VPC para todos os protocolos (SFTP/FTPS/FTP e AS2)
- Endpoints públicos para servidores AS2-enabled Transfer Family, usando as etapas fornecidas em [Usando um Application Load Balancer para conectividade de servidor AS2 de pilha dupla](#)
- Endpoints da API

Com o suporte de pilha dupla, seus endpoints Transfer Family podem se comunicar com clientes habilitados para IPv4 e IPv6. Isso permite que você faça a transição gradual de sistemas baseados em IPv4 para IPv6 sem precisar alternar de uma só vez, atender aos requisitos de conformidade com IPv6 e eliminar a necessidade de equipamentos de rede caros para lidar com a conversão de endereços entre IPv4 e IPv6. Para obter detalhes, consulte [DNS e endpoints](#) na Referência da AWS Transfer Family API. Para obter uma lista completa dos endpoints disponíveis, consulte [AWS Transfer Family endpoints e cotas](#) no. Referência geral da AWS

Limitações do IPv6

Atualmente, os seguintes recursos do Transfer Family não oferecem suporte a IPv6:

- VPC-Internet endpoints
- Tipo de endpoint VPC_ENDPOINT (obsoleto)

O protocolo FTPS suporta os comandos PASV e EPSV para solicitar uma porta de dados aberta para operações de listagem, obtenção e colocação de arquivos. No entanto, o PASV não funciona com IPv6 porque exige uma resposta. IPv4-specific O EPSV continua funcionando porque retorna somente as informações da porta.

Para usar o FTPS, recomendamos uma das seguintes opções:

- Configure seu cliente FTPS para usar o EPSV
- Use IPv4 em vez de IPv6

O SFTP suporta IPv4 e IPv6. Recomendamos usar SFTP em vez de FTPS ao trabalhar com endpoints de pilha dupla.

Configurando o IPv6 para servidores

Ao criar um novo servidor ou atualizar um servidor existente, você pode escolher o tipo de endereço IP:

- IPv4 (padrão): para compatibilidade com versões anteriores, o servidor só aceitará conexões IPv4.
- Dual-stack: O servidor aceitará conexões IPv4 e IPv6.

Para atualizar o tipo de endereço IP de um servidor existente:

1. Pare o servidor.
2. Edite os detalhes do endpoint.
3. Altere o tipo de endereço IP para Dual-stack.
4. Inicie o servidor .

 Note

Para VPC-Internet endpoints, o modo de pilha dupla não é suportado atualmente.

Usando um Application Load Balancer para conectividade de servidor AS2 de pilha dupla

Você pode habilitar a conectividade de pilha dupla (IPv4 e IPv6) com seu servidor AS2 usando um Application Load Balancer que tenha um endpoint voltado para o público. Isso permite que os parceiros comerciais se conectem ao seu servidor AS2 usando IPv4 ou IPv6.

Para configurar um Application Load Balancer de pilha dupla para seu servidor AS2

1. Crie uma VPC com as seguintes configurações:
 - Somente VPC
 - Entrada CIDR IPv4 manual
 - Amazon-provided Bloco CIDR IPv6
2. Crie pelo menos duas sub-redes em diferentes zonas de disponibilidade:
 - Adicione CIDRs IPv6 às sub-redes
 - Ao criar sub-redes, aloque somente um subconjunto dos endereços da VPC para deixar os IPv4/IPv6 endereços disponíveis para sub-redes adicionais
3. Crie um gateway de internet para a VPC.
4. Edite a tabela de rotas e adicione duas rotas:
 - Uma rota com destino `0.0.0.0/0`
 - Uma rota com destino `:::/0`
 - Defina os dois destinos de rota para o gateway de internet que você criou

5. Crie um AS2-enabled servidor na VPC que você criou na etapa 1. Certifique-se de especificar o `IpAddressType` como `DUALSTACK`.

Para obter detalhes sobre como criar um servidor Transfer Family que usa o protocolo AS2, consulte [Crie um servidor AS2](#).

6. Crie um grupo-alvo:

- Para Especificar detalhes do grupo, configure:
 - Tipo de destino: endereços IP
 - Nome: Insira um nome
 - Protocol: HTTP
 - Porta: 5080
 - VPC: selecione a VPC que você criou
 - Versão do protocolo: HTTP1
 - Verificações de saúde: use padrões
- Para alvos do Registro:
 - Insira o endereço IPv4 privado do seu servidor AS2
 - Escolha Incluir como pendente abaixo

7. Crie um Application Load Balancer:

- Insira um nome
- Para Esquema, escolha Internet-facing
- Para o tipo de endereço IP, escolha Dualstack
- Para mapeamento de rede:
 - Selecione a VPC que você criou
 - Selecione as zonas de disponibilidade nas quais você criou sub-redes
- Em Grupos de segurança, selecione um grupo de segurança que permita tráfego IPv4 e IPv6 de entrada de qualquer endereço IP na porta 80
- Para ouvintes e roteamento:
 - Protocol: HTTP
 - Port: 80
- ~~Ação padrão: encaminhar para o grupo-alvo que você criou~~
- Escolha Criar balanceador de carga

Depois de criar o Application Load Balancer, os parceiros comerciais podem usar seu nome DNS para enviar tráfego para seu servidor AS2. Essa configuração permite que seu servidor AS2 aceite conexões de clientes IPv4 e IPv6 por meio do Application Load Balancer de pilha dupla.

Editar detalhes do servidor

Depois de criar um AWS Transfer Family servidor, você pode editar a configuração do servidor.

Tópicos

- [Edite os protocolos de transferência de arquivo](#)
- [Edite o endpoint do servidor](#)
- [Edite sua configuração de registro em log](#)
- [Edite a política de segurança](#)
- [Altere o fluxo de trabalho gerenciado do seu servidor](#)
- [Altere os banners de exibição do seu servidor](#)
- [Coloque seu servidor online ou offline](#)

Para editar a configuração de um servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação à esquerda, selecione Servidores.
3. Escolha o identificador na coluna ID do servidor para ver a página Detalhes do servidor, exibida a seguir.

Você pode alterar as propriedades do servidor nessa página escolhendo Editar:

- Para alterar os protocolos, consulte [Edite os protocolos de transferência de arquivo](#).
- Para o provedor de identidade, agora você pode alternar entre qualquer tipo de provedor de identidade (gerenciado por serviço, AWS Directory Service ou provedor de identidade personalizado). Para obter detalhes sobre a alteração dos tipos de provedores de identidade e as informações necessárias para cada transição, consulte [Editar a configuração do provedor de identidade](#).
- Para alterar o tipo de endpoint ou o nome de host personalizado, consulte [Edite o endpoint do servidor](#).

- Para adicionar um contrato, você precisa primeiro adicionar o AS2 como um protocolo ao seu servidor. Para obter detalhes, consulte [Edite os protocolos de transferência de arquivo](#).
- Para gerenciar as chaves de host do seu servidor, consulte [Gerencie as chaves de host SFTP-enabled do seu servidor](#).
- Em Detalhes adicionais, você pode editar as seguintes informações:
 - Para alterar a função de registro em log, consulte [Edite sua configuração de registro em log](#).
 - Para alterar a política de segurança, consulte [Edite a política de segurança](#).
 - Para alterar a chave do host do servidor, consulte [Gerencie as chaves de host SFTP-enabled do seu servidor](#).
 - Para alterar o fluxo de trabalho gerenciado do seu servidor, consulte [Altere o fluxo de trabalho gerenciado do seu servidor](#).
 - Para editar os banners de exibição do seu servidor, consulte [Altere os banners de exibição do seu servidor](#).
- Em Configurações adicionais, você pode editar as seguintes informações:
 - SetStat opção: habilite essa opção para ignorar o erro gerado quando um cliente tenta usar SETSTAT em um arquivo que você está carregando em um bucket do Amazon S3. Para obter detalhes adicionais, consulte a SetStatOption documentação no [ProtocolDetails](#)tópico.
 - Retomada da sessão TLS: fornece um mecanismo para retomar ou compartilhar uma chave secreta negociada entre o controle e a conexão de dados para uma sessão FTPS. Para obter detalhes adicionais, consulte a TlsSessionResumptionMode documentação no [ProtocolDetails](#)tópico.
 - IP Passivo: indica o modo passivo, para protocolos FTP e FTPS. Insira um único endereço IPv4, como o endereço IP público de um firewall, roteador ou balanceador de carga. Para obter detalhes adicionais, consulte a PassiveIp documentação no [ProtocolDetails](#)tópico.

 Note

Evite colocar balanceadores de carga de rede (NLBs) ou gateways NAT na frente dos servidores. AWS Transfer Family Essa configuração aumenta os custos e pode causar problemas de desempenho. Para obter mais detalhes, consulte [Evite colocar NLBs e NATs na frente de AWS Transfer Family servidores](#)

- Para iniciar ou parar seu servidor, consulte [Coloque seu servidor online ou offline](#).

- Para excluir um servidor, consulte [Excluir um servidor](#).
- Para editar as propriedades de um usuário, consulte [Gerenciar controles de acesso](#).

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider

[Edit](#)

Identity provider type
Service managed

Note

Os valores de Descrição e Data de importação da chave do host do servidor são de setembro de 2022. Esses valores foram introduzidos para oferecer suporte ao atributo de várias chaves de host. Esse atributo exigia a migração de qualquer chave de host única que estivesse em uso antes da introdução de várias chaves de host.

O valor da Data da importação de uma chave de host do servidor migrado é definido como a data da última modificação do servidor. Ou seja, a data que você vê para sua chave de host migrada corresponde à data em que você modificou o servidor pela última vez de alguma forma, antes da migração da chave de host do servidor.

A única chave que foi migrada é a sua chave de host de servidor mais antiga ou única. Todas as chaves adicionais têm a data efetiva de quando você as importou. Além disso, a chave migrada tem uma descrição que facilita identificá-la como tendo sido migrada. A migração ocorreu entre 2 e 13 de setembro. A data efetiva da migração dentro desse intervalo depende da região do seu servidor.

Additional details

[Edit](#)

Log group

/aws/transfer/s- [redacted] [↗](#)

Logging role

-

Security Policy

[Info](#)
TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

Domain

Amazon S3

Login display banner

[View the display message](#)

Optimized directories

[Info](#)
ENABLED

SetStat option

Ignore

TLS session resumption

-

Passive IP

-

Edite os protocolos de transferência de arquivo

No AWS Transfer Family console, você pode editar o protocolo de transferência de arquivos. O protocolo de transferência de arquivos conecta o cliente ao endpoint do seu servidor.

Para editar os protocolos

1. Na página Detalhes do servidor, escolha Editar ao lado de Protocolos.
2. Na página Edit protocols (Editar protocolos), marque ou desmarque a caixa de seleção do protocolo ou caixas de seleção para adicionar ou remover os seguintes protocolos de transferência de arquivos:
 - Secure Shell (SSH) Protocolo de transferência de arquivos (SFTP): transferência de arquivos por SSH

Para obter mais informações sobre SFTP, consulte [Crie um SFTP-enabled servidor](#).

- Protocolo de Transferência de Arquivos Segura (FTPS): transferência de arquivos com criptografia TLS.

Para obter mais informações sobre FTP, consulte [Crie um FTPS-enabled servidor](#).

- Protocolo de Transferência de Arquivos (FTP): transferência de arquivos não criptografados.

Para obter mais informações sobre FTPS, consulte [Crie um FTP-enabled servidor](#).

Note

Se você tiver um servidor existente habilitado somente para SFTP e quiser adicionar FTPS e FTP, deverá garantir que tem as configurações corretas de provedor de identidade e tipo de endpoint compatíveis com FTPS e FTP.

Edit protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

[Cancel](#)[Save](#)

Se você selecionar FTPS, deverá escolher um certificado armazenado no AWS Certificate Manager (ACM) que será usado para identificar seu servidor quando os clientes se conectarem a ele via FTPS.

Para solicitar um novo certificado público, consulte [Solicitar um certificado público](#) no Guia do usuário do AWS Certificate Manager .

Para importar um certificado existente para o ACM, consulte [Importar certificados para o ACM](#) no Guia do usuário do AWS Certificate Manager .

Para solicitar um certificado privado para usar FTPS por meio de endereços IP privados, consulte [Solicitar um certificado privado](#) no Guia do usuário do AWS Certificate Manager .

Os certificados com os seguintes algoritmos criptográficos e tamanhos de chave são compatíveis:

- RSA de 2048 bits (RSA_2048)
- RSA de 4096 bits (RSA_4096)
- Elliptic Prime Curve de 256 bits (EC_prime256v1)
- Elliptic Prime Curve de 384 bits (EC_secp384r1)
- Elliptic Prime Curve de 521 bits (EC_secp521r1)

 Note

O certificado deve ser um certificado válido da SSL/TLS X.509 versão 3 com FQDN ou endereço IP especificado e conter informações sobre o emissor.

3. Escolha Salvar. Você retorna à página Detalhes do servidor.

Edite o endpoint do servidor

No AWS Transfer Family console, você pode modificar o tipo de endpoint do servidor e o nome de host personalizado. Além disso, para VPC endpoints, você pode editar as informações da zona de disponibilidade.

Para editar os detalhes do endpoint do servidor

1. Na página Detalhes do servidor, escolha Editar ao lado de Detalhes do endpoint.
2. Antes de editar o tipo de endpoint, você deve primeiro parar o servidor. Em seguida, na página Editar configuração do endpoint, para Tipo de endpoint, você pode escolher um dos seguintes valores:
 - Público – esta opção torna seu servidor acessível pela Internet.
 - VPC – esta opção torna o servidor acessível na nuvem privada virtual (VPC). Para obter informações sobre VPC, consulte [Crie um servidor em uma VPC \(virtual private cloud\)](#).
3. Em Nome de host personalizado, escolha um dos seguintes:
 - Nenhum – se você não quiser usar um domínio personalizado, escolha Nenhum.

Você recebe um nome de host do servidor fornecido por AWS Transfer Family. O nome do host do servidor tem a forma de `serverId.server.transfer.regionId.amazonaws.com`.

- Alias de DNS do Amazon Route 53 – para usar um alias de DNS criado automaticamente para você no Route 53, escolha essa opção.
- Outro DNS – para usar um nome de host que você já possui em um serviço DNS externo, escolha Outro DNS.

Escolher o alias de DNS do Amazon Route 53 ou outro DNS especifica o método de resolução de nomes a ser associado ao endpoint do seu servidor.

Por exemplo, o seu domínio personalizado pode ser `sftp.inbox.example.com`. Um nome de host personalizado usa o nome DNS fornecido por você e que um serviço DNS pode resolver. Você pode usar o Route 53 como resolvidor de DNS ou usar o seu próprio provedor de serviço de DNS. Para saber como o AWS Transfer Family usa o Route 53 para rotear o tráfego do seu domínio personalizado para o endpoint do servidor, consulte [Trabalhar com nomes de host personalizados](#).

4. Para VPC endpoints, você pode alterar as informações no painel Zonas de disponibilidade.
5. Escolha Salvar. Você retorna à página Detalhes do servidor.

Edite sua configuração de registro em log

No AWS Transfer Family console, você pode alterar sua configuração de registro.

 Note

Se a Transfer Family criou uma função de CloudWatch registro do IAM para você quando você criou um servidor, a função do IAM será chamada `AWSTransferLoggingAccess`. Você pode usá-lo para todos os seus servidores Transfer Family.

Para editar sua configuração de registro em log

1. Na página Detalhes do servidor, escolha Editar ao lado de Detalhes adicionais.
2. Com base na sua configuração, escolha entre uma função de registro em log, um registro em log JSON estruturado ou ambos. Para obter mais informações, consulte [Atualizando registro em logs de um servidor](#).

Edite a política de segurança

Este procedimento explica como alterar a política de segurança do servidor Transfer Family usando o AWS Transfer Family console ou AWS CLI.

 Note

Se o seu endpoint for FIPS-enabled, você não poderá alterar a política de segurança FIPS para uma política de segurança não FIPS.

Console

Para editar a política de segurança usando o console

1. Na página Detalhes do servidor, escolha Editar ao lado de Detalhes adicionais.
2. Na seção Opções de algoritmo criptográfico, escolha uma política de segurança que contenha os algoritmos criptográficos habilitados para uso pelo seu servidor.

Para obter mais informações sobre as políticas de segurança, consulte [Políticas de segurança para AWS Transfer Family servidores](#).

3. Escolha Salvar.

Você retornará à página de detalhes do servidor, onde poderá ver a política de segurança atualizada.

AWS CLI

Para editar a política de segurança usando a CLI

1. Execute o comando a seguir para visualizar a política de segurança atual anexada ao seu servidor.

```
aws transfer describe-server --server-id your-server-id
```

Esse `describe-server` comando retorna todos os detalhes do seu servidor, incluindo a seguinte linha:

```
"SecurityPolicyName": "TransferSecurityPolicy-2018-11"
```

Nesse caso, a política de segurança do servidor é `TransferSecurityPolicy-2018-11`.

2. Certifique-se de fornecer o nome exato da política de segurança ao comando.
Por exemplo, execute o comando a seguir para atualizar o servidor para `TransferSecurityPolicy-2023-05`.

```
aws transfer update-server --server-id your-server-id --security-policy-name  
"TransferSecurityPolicy-2023-05"
```

Note

Os nomes das políticas de segurança disponíveis estão listados em [Políticas de segurança para AWS Transfer Family servidores](#).

Se for bem-sucedido, o comando retornará o código a seguir e atualizará a política de segurança do seu servidor.

```
{  
  "ServerId": "your-server-id"
```

}

Altere o fluxo de trabalho gerenciado do seu servidor

No AWS Transfer Family console, você pode alterar o fluxo de trabalho gerenciado associado ao servidor.

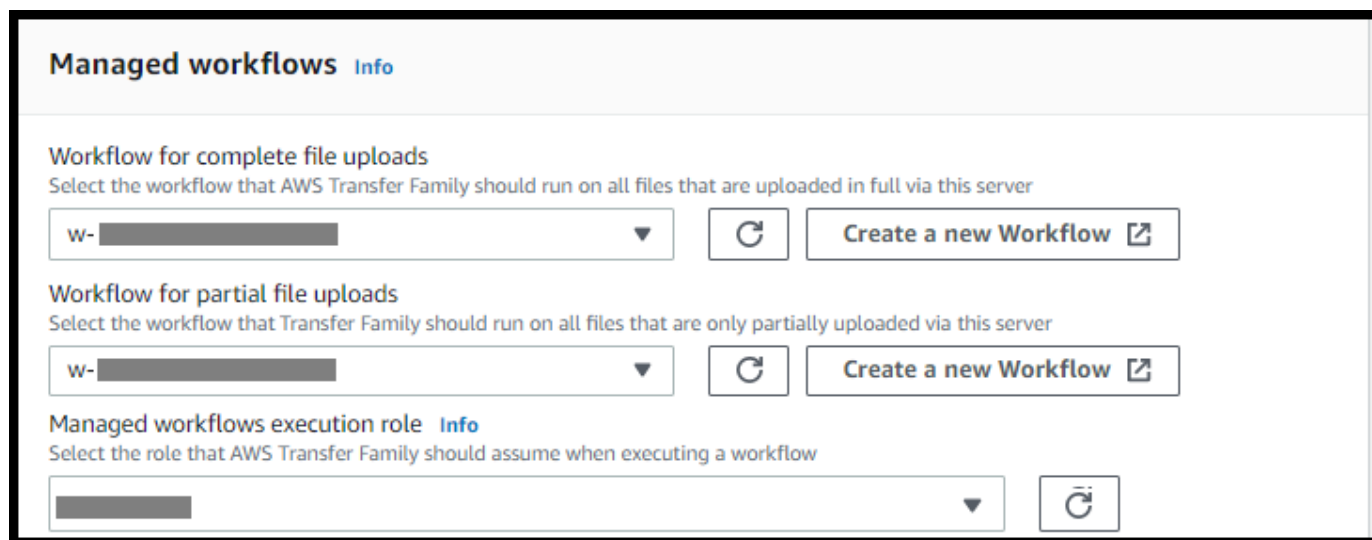
Para alterar o fluxo de trabalho gerenciado

1. Na página Detalhes do servidor, escolha Editar ao lado de Detalhes adicionais.
2. Na página Editar detalhes adicionais, na seção Fluxos de trabalho gerenciados, selecione um fluxo de trabalho a ser executado em todos os carregamentos.

Note

Se você ainda não tiver um fluxo de trabalho, escolha Criar um novo fluxo de trabalho para criar um.

- a. Selecione a ID do fluxo de trabalho a ser usada.
- b. Escolha uma função de execução. Esta é a função que o Transfer Family assume ao executar as etapas do fluxo de trabalho. Para obter mais informações, consulte [Políticas do IAM para fluxos de trabalho](#). Escolha Salvar.



Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- ▼  [Create a new Workflow](#) 

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- ▼  [Create a new Workflow](#) 

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

▼ 

3. Escolha Salvar. Você retorna à página Detalhes do servidor.

Altere os banners de exibição do seu servidor

No AWS Transfer Family console, você pode alterar os banners de exibição associados ao servidor.

Para alterar os banners de exibição

1. Na página Detalhes do servidor, escolha Editar ao lado de Detalhes adicionais.
2. Na página Editar detalhes adicionais, na seção Exibir banners, insira o texto dos banners de exibição disponíveis.
3. Escolha Salvar. Você retorna à página Detalhes do servidor.

Coloque seu servidor online ou offline

No AWS Transfer Family console, você pode colocar seu servidor online ou offline.

Para colocar seu servidor online

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores.
3. Marque a caixa de seleção do servidor que está offline.
4. Em Ações, escolha Iniciar.

Pode levar alguns minutos para um servidor mudar de offline para online.

Note

Quando você interrompe um servidor, deixando-o offline, você ainda está acumulando cobranças de serviço para esse servidor. Para eliminar cobranças adicionais com base em servidor, exclua esse servidor.

Para colocar seu servidor offline

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação, selecione Servidores.

3. Marque a caixa de seleção do servidor que está online.
4. Em Ações, escolha Interromper.

Enquanto um servidor está sendo iniciado ou desligado, os servidores ficam indisponíveis para operações de arquivo. O console não mostra os estados iniciar e interromper.

Se você encontrar a condição de erro `START_FAILED` ou `STOP_FAILED` entre em contato AWS Support para ajudar a resolver seus problemas.

Editar a configuração do provedor de identidade

Você pode alterar o tipo de provedor de identidade do seu servidor de qualquer tipo para qualquer outro tipo. Os tipos de provedores de identidade disponíveis são:

- Serviço gerenciado — Armazene as credenciais do usuário dentro do serviço
- AWS Directory Service — Use o Microsoft AD AWS gerenciado ou o AWS Directory Service para serviços de domínio Entra ID
- Personalizado — Use a função Lambda ou o Amazon API Gateway para integrar-se ao seu provedor de identidade existente

Ao alterar os tipos de provedores de identidade, você precisa fornecer informações específicas, dependendo da transição que você está fazendo. As seções a seguir descrevem as informações necessárias para cada tipo de alteração.

Important

Considerações ao alterar os provedores de identidade:

- Migração de usuários — Ao alterar os tipos de provedores de identidade, as configurações de usuário existentes não são migradas automaticamente. Você precisará configurar usuários no novo sistema do provedor de identidade.
- Teste — Teste minuciosamente a configuração do novo provedor de identidade antes de fazer a alteração nos ambientes de produção.
- Permissões — Certifique-se de que o novo provedor de identidade tenha as permissões e funções necessárias do IAM configuradas antes de fazer a alteração.

Mudando para provedor de identidade gerenciado por serviços

Ao mudar de qualquer outro tipo de provedor de identidade para gerenciado por serviços, você precisa:

- Selecione Serviço gerenciado como o tipo de provedor de identidade
- Crie novos usuários diretamente AWS Transfer Family após a conclusão da alteração, pois as configurações de usuário existentes de outros provedores de identidade não serão transferidas

Exemplo: se você estiver mudando de um provedor de identidade personalizado para um serviço gerenciado, precisará recriar todas as contas de usuário e suas permissões associadas no serviço.
AWS Transfer Family

Mudando para AWS Directory Service

Ao mudar de qualquer outro tipo de provedor de identidade para o AWS Directory Service, você precisa fornecer:

- Diretório — Selecione um Microsoft AD AWS gerenciado existente ou AWS Directory Service para o diretório Entra ID Domain Services
- Acesso — Escolha se deseja restringir o acesso a um grupo específico ou permitir o acesso a todos os usuários no diretório
- Função de acesso — Uma função do IAM que AWS Transfer Family permite acessar seu diretório

Exemplo: se você estiver mudando de gerenciado por serviço para AWS Directory Service, selecione seu d-1234567890 diretório existente, opte por restringir o acesso ao TransferUsers grupo e especifique a TransferDirectoryAccessRole função do IAM.

Mudando para um provedor de identidade personalizado

Ao mudar de qualquer outro tipo de provedor de identidade para um provedor de identidade personalizado, você precisa escolher entre a função Lambda ou o Amazon API Gateway e fornecer a configuração necessária:

Usando a função Lambda

Para a integração da função Lambda, forneça:

- Função — Selecione uma função Lambda existente que gerencia a autenticação
- Método de autenticação (para protocolo SFTP) — Escolha senha, chave pública ou ambas

Exemplo: se você estiver mudando de AWS Directory Service para um provedor de identidade Lambda personalizado, você selecionaria sua `TransferCustomAuth` função e escolheria Password como método de autenticação.

Transfer Family > Servers > s-[redacted] > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ Service managed
Create and manage users within the service

☐ AWS Directory Service [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)
Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

[redacted] ▼



Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

 Either a valid password or valid private key will be required during user authentication

Cancel

Save

Usando o Amazon API Gateway

Para a integração com o Amazon API Gateway, forneça:

- URL do API Gateway — O URL de invocação do seu endpoint do API Gateway

- Função de invocação — Uma função do IAM que permite AWS Transfer Family invocar seu API Gateway
- Método de autenticação (para protocolo SFTP) — Escolha senha, chave pública ou ambas

Exemplo: se você estiver mudando do serviço gerenciado para o API Gateway, forneça a URL `https://abcdef123.execute-api.us-east-1.amazonaws.com/prod`, especifique a função `TransferApiGatewayInvocationRole` do IAM e escolha a chave pública como método de autenticação.

Transfer Family > Servers > s-[redacted] > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

☐ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☒ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

Provide an Amazon API Gateway URL

Invocation role
IAM role for the service to invoke your Amazon API Gateway URL

Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ **Password OR public key**
☐ Password ONLY
☐ Public Key ONLY
☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel Save

Mudança do Amazon API Gateway para a função Lambda

Uma transição comum é mudar do Amazon API Gateway para a função Lambda para integração personalizada com provedores de identidade. Essa alteração permite que você simplifique sua arquitetura enquanto mantém a mesma lógica de autenticação.

Principais considerações para essa transição:

- Mesma função, permissões diferentes — Você pode usar a mesma função do Lambda tanto para o API Gateway quanto para a integração direta com o Lambda, mas a política de recursos deve ser atualizada.
- Requisitos da política de recursos — Ao mudar para a integração direta com o Lambda, a política de recursos da função deve conceder `transfer.amazonaws.com` com permissão para invocar a função, além de `apigateway.amazonaws.com`

Para fazer essa alteração

1. Atualize a política de recursos da sua função Lambda para permitir `transfer.amazonaws.com` a invocação da função.
2. No AWS Transfer Family console, altere o provedor de identidade do API Gateway para a função Lambda.
3. Selecione sua função Lambda existente.
4. Teste a configuração para garantir que a autenticação funcione corretamente.

Exemplo de política de recursos para integração direta com o Lambda:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "transfer.amazonaws.com",
        "apigateway.amazonaws.com"
      ]
    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:function-name"
  }]
}
```

Preservação do usuário durante as transições do provedor de identidade

Ao alternar entre os tipos de provedores de identidade, as configurações de usuário existentes são preservadas em cenários específicos para permitir uma reversão eficiente em caso de problemas:

- Service-managed para provedor de identidade personalizado e vice-versa — Se você mudar de provedor de identidade gerenciado por serviço para provedor de identidade personalizado e depois voltar para gerenciado por serviço, todos os usuários serão preservados em sua última configuração conhecida.
- AWS Directory Service para o provedor de identidade personalizado e vice-versa — Se você mudar AWS Directory Service para um provedor de identidade personalizado e depois voltar para AWS Directory Service, todas as definições dos grupos de Acesso Delegado serão mantidas em sua última configuração conhecida.

Esse comportamento de preservação permite que você teste com segurança as configurações personalizadas do provedor de identidade e volte para a configuração anterior sem perder as configurações de acesso do usuário.

Considerações importantes ao alterar os provedores de identidade

- Migração de usuários — Ao alterar os tipos de provedores de identidade, as configurações de usuário existentes não são migradas automaticamente. Você precisará configurar usuários no novo sistema do provedor de identidade.
- Teste — Teste minuciosamente a configuração do novo provedor de identidade antes de fazer a alteração nos ambientes de produção.
- Permissões — Certifique-se de que o novo provedor de identidade tenha as permissões e funções necessárias do IAM configuradas antes de fazer a alteração.

Gerencie as chaves de host SFTP-enabled do seu servidor

As chaves de host do servidor são chaves privadas usadas pelo servidor Transfer Family para fornecer uma identidade exclusiva ao chamador e garantir que ele seja o servidor correto. Essa garantia é aplicada pela presença da chave pública correta no arquivo do chamador. `known_hosts` (O `known_hosts` arquivo é um recurso padrão usado pela maioria dos clientes SSH para armazenar as chaves públicas dos servidores aos quais você se conectou.) Você pode recuperar a chave pública que corresponde à chave do host do servidor executando `ssh-keyscan` para o seu servidor.

 Important

A alteração acidental de uma chave de host do servidor pode causar interrupções. Dependendo de como seu cliente SFTP está configurado, ele pode falhar imediatamente, com a mensagem de que não existe uma chave de host confiável ou apresentar avisos ameaçadores. Se houver scripts para automatizar conexões, eles provavelmente também falharão.

Por padrão, AWS Transfer Family gera chaves de host para seu SFTP-enabled servidor. Você pode importar chaves do host do servidor para preservar a identidade do host e evitar a atualização dos repositórios confiáveis do cliente. [Quando importar chaves de host](#) lista alguns motivos pelos quais você pode querer fazer isso. Se você não fornecer chaves de host, novas chaves serão geradas para você.

AWS Transfer Family oferece suporte a várias chaves de host de diferentes tipos (RSA, ECDSA e ED25519) para fornecer compatibilidade com uma variedade mais ampla de algoritmos de assinatura de host cliente. Diferentes tipos de chaves permitem algoritmos específicos: as chaves RSA ativam os algoritmos rsa-*, as chaves ECDSA habilitam os algoritmos ecdsa-* e as chaves ED25519 habilitam os algoritmos ed25519. Planeje seus tipos de chave no momento da criação do servidor, pois a introdução de tipos de chaves adicionais depois que os clientes começarem a interagir com o servidor pode causar interrupções para alguns clientes e pode ser tão problemática quanto substituir as chaves de host existentes.

Para evitar que seus usuários sejam solicitados a verificar a autenticidade do seu SFTP-enabled servidor novamente, importe a chave do host do seu servidor local para o servidor. SFTP-enabled Isso também impede que os usuários recebam um aviso sobre um possível ataque man-in-the-middle.

Você também pode alternar as chaves do host periodicamente, como medida de segurança adicional. Para obter detalhes, consulte [Altere as chaves do host do servidor](#).

 Note

As chaves de host do servidor são usadas por servidores que oferecem suporte ao protocolo SFTP.

Quando importar chaves de host

Embora AWS Transfer Family possa gerar chaves de host automaticamente, há vários cenários em que importar suas próprias chaves de host oferece benefícios operacionais:

- Migração de servidor - Você está migrando de um servidor existente para clientes existentes AWS Transfer Family e deseja evitar a atualização de armazenamentos confiáveis (known_hosts arquivos) de clientes existentes.
- Recuperação de desastres e failover - Você tem vários AWS Transfer Family servidores (por exemplo, um no Leste dos EUA (Ohio) e outro no Oeste dos EUA (Oregon)) que compartilham o mesmo nome DNS público. O uso das mesmas chaves de host nos dois servidores garante um failover contínuo sem falhas na autenticação do cliente.
- Continuidade operacional - Você deseja que o material da chave do host esteja disponível para uso com outros servidores (AWS Transfer Family ou não) no futuro para manter a identidade consistente do servidor em toda a sua infraestrutura.
- Controle de algoritmo - Você deseja maior compatibilidade com o cliente fornecendo mais algoritmos de chave de host ou deseja controlar quais algoritmos os clientes podem usar oferecendo apenas chaves compatíveis com algoritmos específicos.

Os tópicos a seguir fornecem procedimentos detalhados para gerenciar as chaves do host do servidor:

- [Adicionar uma chave de host do servidor adicional](#)- Adicione chaves de host adicionais ao seu servidor
- [Excluir uma chave de host do servidor](#)- Remova as chaves do host do seu servidor
- [Altere as chaves do host do servidor](#)- Gire as chaves do host para aumentar a segurança
- [Informações adicionais sobre a chave do host do servidor](#)- Visualize e gerencie os detalhes da chave do host

Adicionar uma chave de host do servidor adicional

No AWS Transfer Family console, você pode adicionar mais chaves de host do servidor. Adicionar chaves de host adicionais de formatos diferentes pode ser útil para identificar um servidor quando os clientes se conectam a ele, além de melhorar seu perfil de segurança. Por exemplo, se sua chave original for uma chave RSA, você poderá adicionar uma chave ECDSA adicional.

Note

O cliente SFTP se conectará usando a chave mais antiga na configuração que corresponda ao algoritmo da chave. A chave mais antiga para cada tipo de chave (RSA, ECDSA ou ED25519) é a chave ativa do servidor desse tipo.

Nota de segurança quando um servidor Transfer Family tem vários tipos de chaves de host

Se um servidor tiver vários tipos de chaves de host, o cliente SFTP poderá atribuir uma preferência por tipo. Portanto, quando existem chaves de host RSA, ECDSA e ED25519 para o servidor, a escolha é orientada pela preferência por tipo.

Clientes SFTP modernos preferem as chaves de host ECDSA e ED25519 quando elas existem. Isso se torna importante se você quiser adicionar uma chave ECDSA ou ED25519 quando o servidor anteriormente tinha apenas chaves RSA. A adição da nova chave ECDSA ou ED25519 se manifestaria potencialmente como um aviso de segurança para um cliente.

Para o cliente, a chave aparecerá como tendo sido alterada, quando na verdade não foi alterada: a nova chave foi adicionada além da chave RSA existente. Lembre-se disso se você decidir adicionar novos tipos de chaves de host do servidor.

Para adicionar uma chave de host do servidor adicional

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, selecione Servidores e, em seguida, escolha um servidor que use o protocolo SFTP.
3. Na página de detalhes do servidor, role para baixo até a seção Chaves do host do servidor.

Server host keys (2)							Actions	Add host key
Find resources							< 1 >	
☐	Name	Host key ID	Fingerprint	Description	Key type	Date imported		
☐	Default host key	hostkey- 	SHA256: 	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey- 	SHA256: 	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

4. Escolha Adicionar chave do host.

A página Adicionar chave de host do servidor é exibida.

5. Na seção Chave do host do servidor, insira uma chave privada RSA, ECDSA ou ED25519 usada para identificar seu servidor quando os clientes se conectam a ele pelo servidor. SFTP-enabled

 Note

Ao criar uma chave de host do servidor, certifique-se de especificar `-N ""` (sem senha). Consulte [Criação de chaves SSH no macOS, Linux ou Unix](#) para obter detalhes sobre como gerar pares de chaves.

6. (Opcional) Adicione uma descrição para diferenciar entre várias chaves de host de servidor. Você também pode adicionar tags à sua chave.
7. Escolha Adicionar chave. Você retorna à página Detalhes do servidor.

Para adicionar uma chave de host usando o AWS Command Line Interface (AWS CLI), use a operação de [ImportHostKey](#) API e forneça a nova chave de host. Se você criar um novo SFTP-enabled servidor, fornecerá sua chave de host como parâmetro na operação da [CreateServer](#) API. Você também pode usar o AWS CLI para atualizar a descrição de uma chave de host existente.

O `import-host-key` AWS CLI comando de exemplo a seguir importa uma chave de host para o SFTP-enabled servidor especificado.

```
aws transfer import-host-key --description key-description --server-id your-server-id --host-key-body file://my-host-key
```

Excluir uma chave de host do servidor

No AWS Transfer Family console, você pode excluir uma chave de host do servidor.

Para excluir uma chave de host do servidor

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. No painel de navegação esquerdo, selecione Servidores e, em seguida, escolha um servidor que use o protocolo SFTP.
3. Na página de detalhes do servidor, role para baixo até a seção Chaves do host do servidor.

Server host keys (2)

Actions

Add host key

☐	Name 	Host key ID 	Fingerprint Info	Description 	Key type 	Date imported 
☐	Default host key	hostkey- 	SHA256: 	Default	ssh-rsa	2023-06-30
☐	ecdsa-521	hostkey- 	SHA256: 	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13

4. Na seção Chaves do host do servidor, selecione uma chave e, em Ações, escolha Excluir.
5. Na caixa de diálogo de confirmação exibida, insira a palavra **delete** e, em seguida, escolha Excluir para confirmar que deseja excluir a chave do host.

A chave do host é excluída da página Servidores.

Para excluir a chave do host usando o AWS CLI, use a operação da [DeleteHostKey](#) API e forneça o ID do servidor e o ID da chave do host.

O `delete-host-key` AWS CLI comando de exemplo a seguir exclui uma chave de host para o SFTP-enabled servidor especificado.

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

Altere as chaves do host do servidor

Periodicamente, você pode alternar a chave do host do servidor. Este tópico descreve como o servidor escolhe qual chave aplicar e o procedimento para girar essas chaves.

Como o cliente escolhe uma chave de host do servidor

A forma como a Transfer Family escolhe qual chave de servidor aplicar depende das condições do cliente SFTP, conforme explicado aqui. A suposição é que há uma chave mais antiga e uma chave mais nova.

- Um cliente SFTP não tem uma chave de host pública anterior para o servidor. Na primeira vez que o cliente se conecta ao servidor, ocorre uma das seguintes situações:
 - O cliente falha na conexão, se estiver configurado para isso.
 - Ou o cliente escolhe a primeira chave que corresponde aos possíveis algoritmos disponíveis e pergunta ao usuário se essa chave é confiável. Nesse caso, o cliente atualiza automaticamente o `known_hosts` arquivo (ou qualquer arquivo ou recurso de configuração local que o cliente use para registrar decisões de confiança) e insere essa chave.
- Um cliente SFTP tem uma chave antiga em seu `known_hosts` arquivo. O cliente prefere usar essa chave, mesmo que exista uma chave mais nova, seja para o algoritmo dessa chave ou para outro algoritmo. Isso ocorre porque o cliente tem um nível mais alto de confiança na chave que está em seu `known_hosts` arquivo.

- Um cliente SFTP tem a nova chave (em qualquer um dos algoritmos disponíveis) em seu arquivo de `known_hosts` chaves. O cliente ignora as chaves mais antigas porque elas não são confiáveis e usa a nova chave.
- Um cliente SFTP tem as duas chaves em seu `known_hosts` arquivo. O cliente escolhe a primeira chave por índice que corresponde à lista de chaves disponíveis oferecida pelo servidor.

O Transfer Family prefere que o cliente SFTP tenha todas as chaves em seu `known_hosts` arquivo, pois isso permite maior flexibilidade ao se conectar a um servidor Transfer Family. A rotação de chaves é baseada no fato de que várias entradas podem existir no `known_hosts` arquivo para o mesmo servidor Transfer Family.

Procedimento de rotação da chave do host do servidor

Como exemplo, suponha que você tenha adicionado o seguinte conjunto de chaves de host do servidor ao seu servidor Transfer Family.

Chaves do host do servidor

Tipo de chave do host	Data adicionada ao servidor
RSA	1 de abril de 2020
ECDSA	1 de fevereiro de 2020
ED25519	1.º de dezembro de 2019
RSA	1 de outubro de 2019
ECDSA	1.º de junho de 2019
ED25519	1 de março de 2019

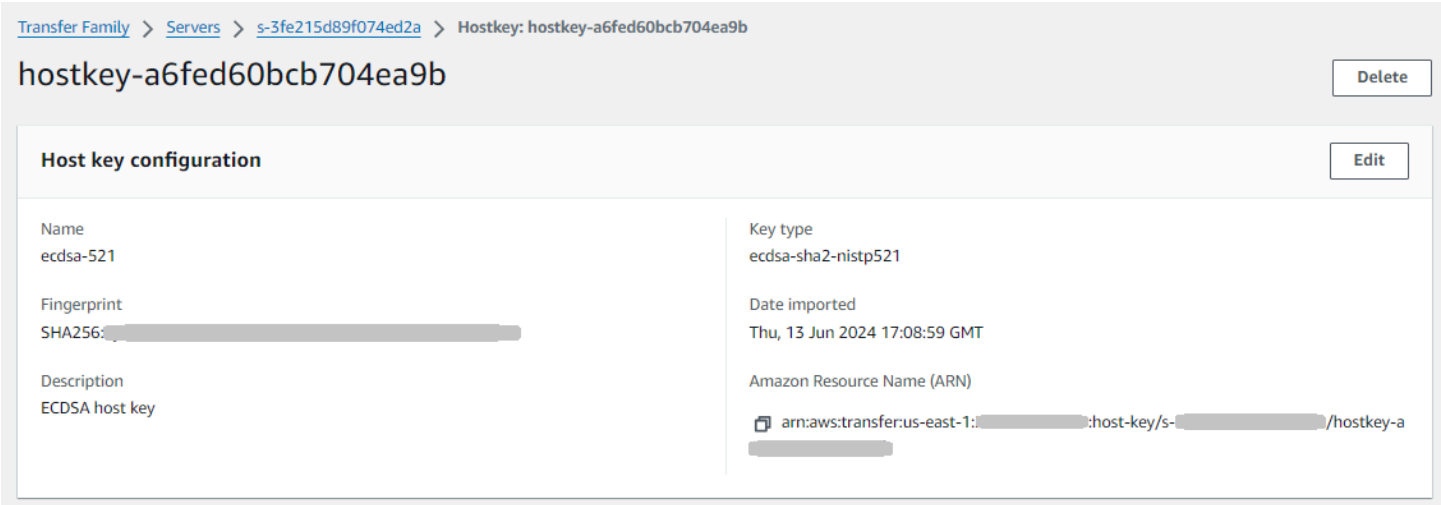
Para alternar as chaves do host do servidor

1. Adicione uma nova chave do host do servidor. Este procedimento está descrito em [Adicionar uma chave de host do servidor adicional](#).
2. Exclua uma ou mais chaves de host do mesmo tipo que você adicionou anteriormente. Este procedimento está descrito em [Excluir uma chave de host do servidor](#).

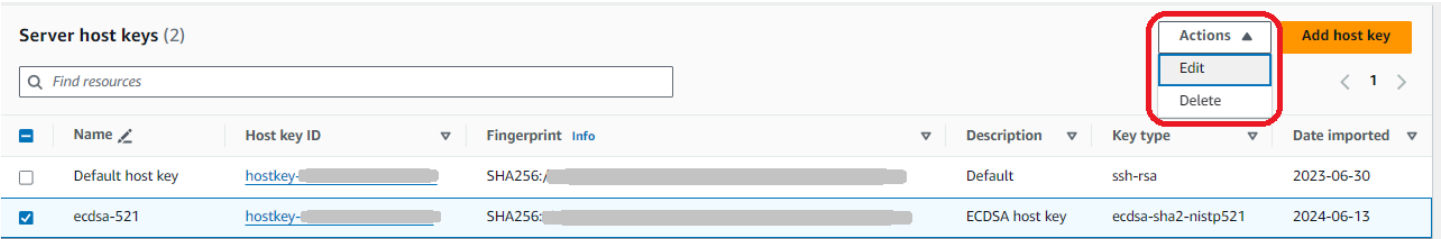
3. Todas as teclas estão visíveis e podem estar ativas, de acordo com o comportamento descrito anteriormente em [Como o cliente escolhe uma chave de host do servidor](#).

Informações adicionais sobre a chave do host do servidor

Você pode selecionar uma chave do host para exibir os detalhes dessa chave.



Você pode excluir uma chave de host ou editar sua descrição no menu Ações na tela de detalhes do servidor. Selecione a chave do host e, em seguida, escolha a ação apropriada no menu.



Monitoramento do uso no console

Você pode obter informações sobre as métricas do seu servidor na página Detalhes do servidor. Isso fornece um único local para monitorar suas workloads de transferências de arquivos. Você pode acompanhar quantos arquivos você trocou com seus parceiros e acompanhar de perto o uso deles usando um painel centralizado. Para obter detalhes, consulte [Exibir detalhes do servidor SFTP, FTPS e FTP](#). A tabela a seguir descreve as métricas disponíveis para Transfer Family.

Namespace	Métrica	Description
AWS/Transfer	BytesIn	O número total de bytes transferidos para o servidor. Critérios de relatório: • Para SFTP/FTP/FTPS: emitido a cada 5 minutos enquanto uma conexão é estabelecida com o servidor Transfer Family. Se nenhum arquivo ou byte for transferido no período, "0" será emitido. • Para AS2: quando o cliente recebe uma mensagem em seu servidor AS2 e é emitida assim que a mensagem de entrada termina de ser processada Unidades: contagem Período: 5 minutos
	BytesOut	O número total de bytes transferidos do servidor. Critérios de relatório: • Para SFTP/FTP/FTPS: emitido a cada 5 minutos enquanto uma conexão é estabelecida com o servidor Transfer Family. Se nenhum arquivo ou byte for transferido no período, "0" será emitido. • Para AS2: quando o cliente liga <code>StartFile Transfer</code> de seu conector AS2 e emite assim que a mensagem de saída termina de ser processada. Unidades: contagem Período: 5 minutos
	FilesIn	O número total de arquivos transferidos para o servidor. Para servidores que usam o protocolo AS2, essa métrica representa o número de mensagens recebidas.

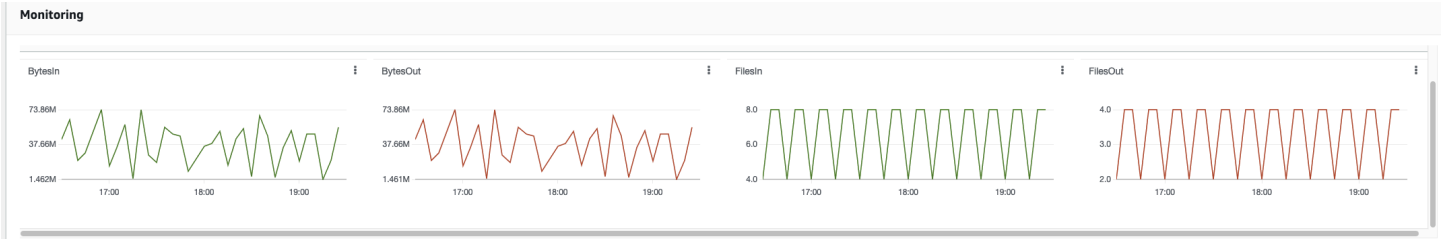
Namespace	Métrica	Description
		Critérios de relatório: • Para SFTP/FTP/FTPS: emitido a cada 5 minutos enquanto uma conexão é estabelecida com o servidor Transfer Family. Se nenhum arquivo ou byte for transferido no período, "0" será emitido. • Para AS2: quando o cliente recebe uma mensagem em seu servidor AS2 e é emitida assim que a mensagem de entrada termina de ser processada. Unidades: contagem Período: 5 minutos
	FilesOut	O número total de arquivos transferidos do servidor. Critérios de relatório: • Para SFTP/FTP/FTPS: emitido a cada 5 minutos enquanto uma conexão é estabelecida com o servidor Transfer Family. Se nenhum arquivo ou byte for transferido no período, "0" será emitido. • Para AS2: quando o cliente liga <code>StartFile Transfer</code> de seu conector AS2 e emite assim que a mensagem de saída termina de ser processada. Unidades: contagem Período: 5 minutos

Namespace	Métrica	Description
	InboundMessage	O número total de mensagens AS2 recebidas com êxito de um parceiro comercial. Critérios de emissão de relatórios: quando o cliente recebe uma mensagem em seu servidor AS2 e é emitida assim que o processamento da mensagem de entrada é concluído com êxito Unidades: contagem Período: 5 minutos
	InboundFailedMessage	O número total de mensagens AS2 que não foram recebidas com êxito de um parceiro comercial. Ou seja, um parceiro comercial enviou uma mensagem, mas o servidor Transfer Family não conseguiu processá-la com êxito. Critérios de emissão de relatórios: quando o cliente recebe uma mensagem em seu servidor AS2 e é emitida assim que o processamento da mensagem de entrada é concluído sem sucesso Unidades: contagem Período: 5 minutos
	OnUploadExecutionsStarted	O número total de execuções de fluxo de trabalho iniciadas no servidor. Critérios de emissão de relatórios: acionados sempre que uma execução é iniciada Unidades: contagem Período: 1 minuto

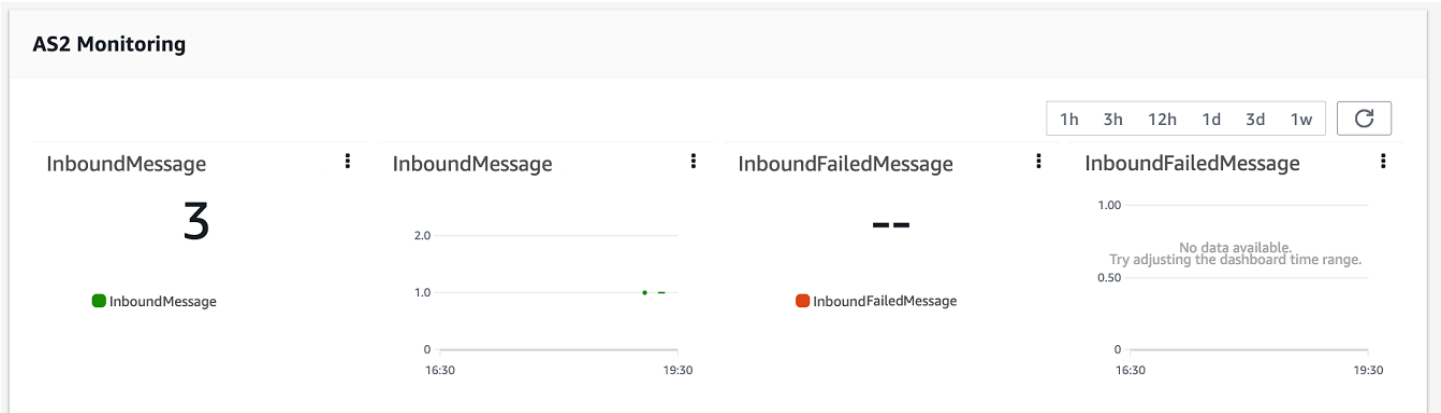
Namespace	Métrica	Description
	OnUploadExecutionsSuccess	O número total de execuções de fluxo de trabalho bem-sucedidas no servidor. Critérios de emissão de relatórios: acionados sempre que uma execução é concluída com sucesso Unidades: contagem Período: 1 minuto
	OnUploadExecutionsFailed	O número total de execuções de fluxo de trabalho malsucedidas no servidor. Critérios de emissão de relatórios: acionados sempre que uma execução não é concluída com êxito Unidades: contagem Período: 1 minuto
	OutboundMessage	O número total de mensagens AS2 enviadas com sucesso a um parceiro comercial. Critérios de emissão de relatórios: quando o cliente liga <code>StartFileTransfer</code> de seu conector AS2 e emite assim que o processamento da mensagem de saída é concluído com êxito Unidades: contagem Período: 5 minutos

Namespace	Métrica	Description
	OutboundFailedMessage	O número total de mensagens AS2 que foram enviadas sem sucesso a um parceiro comercial. Critérios de emissão de relatórios: quando o cliente liga <code>StartFileTransfer</code> de seu conector AS2 e é emitida assim que o processamento da mensagem de saída é concluído sem sucesso Unidades: contagem Período: 5 minutos

A seção Monitoramento contém quatro gráficos individuais. Esses gráficos mostram os bytes de entrada, bytes de saída, arquivos de entrada e arquivos de saída.



Para servidores que têm o protocolo AS2 ativado, há uma seção Monitoramento AS2 abaixo das informações de monitoramento. Esta seção contém detalhes sobre o número de mensagens recebidas, tanto bem-sucedidas quanto malsucedidas.



Para abrir o gráfico selecionado em sua própria janela, escolha o ícone de expansão ().

Você também pode clicar no ícone de elipse vertical de um gráfico



)

para abrir um menu suspenso com os seguintes itens:

- Ampliar – abre o gráfico selecionado em sua própria janela.
- Atualizar – recarrega o gráfico com os dados mais recentes.
- Exibir nas métricas — Abre os detalhes das métricas correspondentes na Amazon CloudWatch.
- Exibir registros — Abre o grupo de registros correspondente em CloudWatch.

Gerenciar controles de acesso

Você pode controlar o acesso de um usuário aos AWS Transfer Family recursos usando uma política AWS Identity and Access Management (IAM). Uma política do IAM é uma instrução, normalmente no formato JSON, que permite determinado nível de acesso a um recurso. Use uma política do IAM para definir quais operações de arquivo você deseja permitir ou não que os seus usuários executem. Você também pode usar uma política do IAM para definir o bucket ou buckets do Amazon S3 aos quais você deseja conceder acesso aos seus usuários. Para especificar essas políticas para os usuários, você cria uma função do IAM AWS Transfer Family que tenha a política do IAM e a relação de confiança associada a ela.

Cada usuário SFTP é atribuído um perfil do IAM. O tipo de função do IAM que AWS Transfer Family usa é chamado de função de serviço. Quando um usuário faz login no seu servidor, AWS Transfer Family assume a função do IAM mapeada para o usuário. Para saber mais sobre a criação de uma função do IAM que fornece ao usuário acesso a um bucket do Amazon S3, consulte [Criação de uma função para delegar permissões a um AWS serviço](#) no Guia do usuário do IAM.

Você pode conceder acesso somente de gravação aos objetos do Amazon S3 usando determinadas permissões dentro de uma política do IAM. Para obter detalhes, consulte [Conceder a capacidade de somente gravar e listar arquivos](#).

O blog AWS de armazenamento contém uma postagem detalhando como configurar o acesso com privilégios mínimos. Para obter detalhes, consulte [Implementação do acesso com privilégios mínimos em um AWS Transfer Family fluxo de trabalho](#).

Note

Se seu bucket do Amazon S3 for criptografado usando AWS Key Management Service (AWS KMS), você deverá especificar permissões adicionais em sua política. Para obter detalhes, consulte [Proteção e criptografia de dados](#). Além disso, é possível ver mais informações sobre [políticas de sessão](#) no Guia do usuário do IAM.

Tópicos

- [Permitir acesso de leitura e gravação a um bucket do Amazon S3](#)
- [Criar uma política de sessão de um bucket do Amazon S3](#)

- [Abordagens dinâmicas de gerenciamento de permissões](#)

Permitir acesso de leitura e gravação a um bucket do Amazon S3

Esta seção descreve como criar uma política do IAM que permite acesso de leitura e gravação a um bucket específico do Amazon S3. A atribuição de uma função do IAM que tenha essa política do IAM ao seu usuário dá a esse usuário read/write acesso ao bucket do Amazon S3 especificado.

A política a seguir fornece acesso de leitura e gravação programático a um bucket do Amazon S3. As declarações de `GetObjectACL` e `PutObjectACL` só são necessárias se você precisar habilitar o acesso entre contas. Ou seja, seu servidor Transfer Family precisa acessar um bucket em uma conta diferente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteS3",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/*"]
    }
  ]
}
```

```
}
```

A ação `ListBucket` requer permissão para o bucket propriamente dito. As ações `PUT`, `GET` e `DELETE` exigem permissões de objeto. Como esses recursos são diferentes, elas são especificadas com o uso de diferentes nomes do recurso da Amazon (ARNs).

Para restringir ainda mais o acesso dos usuários somente ao prefixo home do bucket do Amazon S3 especificado, consulte [Criar uma política de sessão de um bucket do Amazon S3](#).

Criar uma política de sessão de um bucket do Amazon S3

Uma política de sessão é uma política AWS Identity and Access Management (IAM) que restringe os usuários a determinadas partes de um bucket do Amazon S3. Ela faz isso avaliando o acesso em tempo real.

Note

As políticas de sessão são usadas somente com o Amazon S3. Para o Amazon EFS, você usa permissões de arquivo POSIX para limitar o acesso.

Use uma política de sessão quando você precisar fornecer o mesmo acesso a determinada parte do seu bucket do Amazon S3 a um grupo de usuários. Por exemplo, um grupo de usuários pode precisar acessar somente o diretório home. Esse grupo de usuários compartilha o mesmo perfil do IAM.

Note

O tamanho máximo de uma política de sessão é 2.048 caracteres. Para obter mais detalhes, consulte o [parâmetro de solicitação de política](#) para a `CreateUser` ação na referência da API.

Para criar uma política de sessão, use as seguintes variáveis de política na sua política do IAM:

- `${transfer:HomeBucket}`
- `${transfer:HomeDirectory}`

- `${transfer:HomeFolder}`
- `${transfer:UserName}`

Important

Você não pode usar as variáveis anteriores em políticas gerenciadas. Você também não pode usá-las como variáveis de política em uma definição de perfil do IAM. Crie essas variáveis em uma política do IAM e as forneça diretamente ao configurar o seu usuário. Além disso, você não pode usar a variável `${aws:Username}` nesta política de sessão. Essa variável refere-se a um nome de usuário do IAM, e não ao nome de usuário exigido pelo AWS Transfer Family.

Exemplo de política de sessão

O código a seguir mostra um exemplo de política de sessão.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::${transfer:HomeBucket}"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "${transfer:HomeFolder}/*",
            "${transfer:HomeFolder}"
          ]
        }
      }
    }
  ],
}
```



```
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
  ]
}
```

Note

O exemplo de política anterior pressupõe que os usuários tenham seus diretórios pessoais configurados para incluir uma barra final, para indicar que é um diretório. Se, por outro lado, você definir um HomeDirectory de usuário sem a barra final, então deve incluí-lo como parte de sua política.

No exemplo anterior da política, observe o uso dos parâmetros de política `transfer:HomeFolder`, `transfer:HomeBucket`, e `transfer:HomeDirectory`. Esses parâmetros são definidos para o HomeDirectory que está configurado para o usuário, conforme descrito em [HomeDirectoryImplementar seu método do API Gateway](#). Esses parâmetros têm as seguintes definições:

- O parâmetro `transfer:HomeBucket` é substituído pelo primeiro componente do HomeDirectory.
- O parâmetro `transfer:HomeFolder` é substituído pelas partes restantes do parâmetro HomeDirectory.
- O parâmetro `transfer:HomeDirectory` tem a barra inicial (/) removida para que possa ser usado como parte do nome do recurso da Amazon (ARN) do S3 em uma instrução Resource.

Note

Se você estiver usando diretórios lógicos, ou seja, o `homeDirectoryType` do usuário é `LOGICAL`, esses parâmetros de política (`HomeBucket`, `HomeDirectory`, e `HomeFolder`) não serão compatíveis.

Por exemplo, suponha que o parâmetro `HomeDirectory` configurado para o usuário do Transfer Family seja `/home/bob/amazon/stuff/`.

- `transfer:HomeBucket` está definido como `/home`.
- `transfer:HomeFolder` está definido como `/bob/amazon/stuff/`.
- `transfer:HomeDirectory` se torna `home/bob/amazon/stuff/`.

O primeiro "Sid" permite que o usuário liste todos os diretórios a partir de `/home/bob/amazon/stuff/`.

O segundo "Sid" limita o acesso `put` e `get` do usuário ao mesmo caminho, `/home/bob/amazon/stuff/`.

Com a política anterior vigente, ao fazer login, o usuário poderá acessar somente objetos em seu diretório inicial. No momento da conexão, AWS Transfer Family substitui essas variáveis pelos valores apropriados para o usuário. Isso facilita a aplicação das mesmas políticas para vários usuários. Essa abordagem reduz a sobrecarga de gerenciamento de perfil e política do IAM para gerenciar o acesso dos usuários ao seu bucket do Amazon S3.

Você também pode usar uma política de sessão para personalizar o acesso de cada um dos usuários com base em suas necessidades comerciais. Para obter mais informações, consulte [Permissões para AssumeRole AssumeRoleWithSAML, e AssumeRoleWithWebIdentity](#) no Guia do usuário do IAM.

Note

AWS Transfer Family armazena o JSON da política, em vez do Amazon Resource Name (ARN) da política. Portanto, ao alterar a política no console do IAM, você precisa retornar ao AWS Transfer Family console e atualizar seus usuários com o conteúdo mais recente da política. É possível atualizar o usuário na guia Informações da política na seção de Configuração do usuário.

Se você estiver usando o AWS CLI, você pode usar o comando a seguir para atualizar a política.

```
aws transfer update-user --server-id server --user-name user --policy \  
    "$ (aws iam get-policy-version --policy-arn policy --version-id version --  
    output json)"
```

Substituições aninhadas para políticas de sessão

As substituições aninhadas não são realizadas nas políticas de sessão do Transfer Family. As políticas de sessão podem usar variáveis aninhadas, como `${transfer:HomeDirectory}`. Quando a política é processada, a variável externa (por exemplo, `${transfer:HomeDirectory}`) pode ser substituída por um valor que contém outra variável (por exemplo, `{amzn-s3-demo-bucket:/${transfer:UserName}}`). No entanto, a variável aninhada não é posteriormente substituída pelo nome de usuário real (por exemplo, `johndoe`).

Isso significa que, ao criar políticas de sessão para o Transfer Family, você precisa considerar esse comportamento e garantir que a estrutura da política e o uso de variáveis sejam projetados adequadamente. As variáveis aninhadas podem não ser resolvidas conforme o esperado e a política pode não conceder as permissões pretendidas. É importante testar e validar minuciosamente as políticas da sessão para garantir que funcionem conforme o esperado. Esse comportamento é uma consideração importante ao implementar controle de acesso e permissões para seu ambiente Transfer Family.

Uma solução para esse problema é usar o nome real do bucket Amazon S3 em sua política de sessão. Então, por exemplo, em vez de especificar `${transfer:HomeDirectory}` em sua política de sessão, use o seguinte, onde `amzn-s3-demo-bucket` é seu bucket real: `${amzn-s3-demo-bucket/transfer:UserName}`

Abordagens dinâmicas de gerenciamento de permissões

Entendendo a arquitetura de permissão do Transfer Family

AWS Transfer Family oferece suporte ao gerenciamento dinâmico de permissões por meio de políticas de sessão, que permitem restringir as permissões efetivas das funções do IAM em tempo de execução. Essa abordagem funciona tanto para usuários gerenciados por serviços quanto para

usuários de provedores de identidade personalizados, mas só é suportada na transferência de arquivos de ou para o Amazon S3 (não para o Amazon EFS).

Cada AWS Transfer Family usuário opera com um modelo de permissão que consiste em:

1. Função básica do IAM - Define as permissões básicas para o usuário
2. Política de sessão opcional - restringe (reduz o escopo) as permissões básicas em tempo de execução

As permissões efetivas são a interseção das permissões da função básica e das permissões da política de sessão. As políticas de sessão só podem restringir as permissões; elas não podem conceder permissões adicionais além do permitido pela função básica.

Essa arquitetura se aplica aos dois tipos de usuário:

- Service-managed usuários - as políticas de sessão podem ser configuradas diretamente nas configurações do usuário
- Usuários de provedores de identidade personalizados - as políticas de sessão podem ser retornadas como parte da resposta de autenticação ou armazenadas em AWS Secrets Manager

Duas abordagens para o gerenciamento de permissões

Ao criar permissões para usuários do Transfer Family que precisam de padrões de acesso exclusivos, você pode escolher entre duas abordagens principais:

Uma função por usuário

Crie uma função do IAM separada para cada usuário do Transfer Family com permissões específicas adaptadas às necessidades desse usuário. Use essa abordagem quando:

- Cada usuário requer permissões muito diferentes
- A administração de permissões é feita por diferentes pessoas em sua organização
- Você precisa de um controle refinado sobre o acesso individual do usuário

Função compartilhada com políticas de sessão

Use uma única função do IAM com amplas permissões (como acesso a um bucket inteiro do Amazon S3 contendo vários diretórios iniciais de usuários) e aplique políticas de sessão para restringir cada usuário à sua área específica. Essa abordagem reduz significativamente a

sobrecarga administrativa em comparação com o gerenciamento de funções separadas para cada usuário. Use essa abordagem quando:

- Os usuários precisam de tipos de acesso semelhantes, mas a recursos diferentes (por exemplo, todos os usuários precisam read/write acessar, mas cada um somente à sua própria pasta)
- Você quer simplificar o gerenciamento de funções e evitar a criação de dezenas ou centenas de funções individuais
- Os usuários só devem acessar seus diretórios iniciais designados em um bucket compartilhado
- A administração de permissões é centralizada em sua organização

Por exemplo, em vez de criar funções separadas para os usuários “alice”, “bob” e “charlie”, você pode criar uma função com acesso a todo o `s3://company-transfers/` bucket e, em seguida, usar políticas de sessão para restringir aliceto `s3://company-transfers/alice/`, bob to `s3://company-transfers/bob/` e assim por diante.

Implementando políticas de sessão

As políticas de sessão funcionam restringindo as permissões efetivas da função básica do IAM atribuída a um usuário. As permissões finais são a interseção das permissões da função e das permissões da política de sessão.

Você pode implementar políticas de sessão dinâmicas de duas maneiras:

Substituição de variáveis

Use variáveis de política do Transfer Family `${transfer:Username}`, como `${transfer:HomeDirectory}`, e `${transfer:HomeBucket}` em suas políticas de sessão. Essas variáveis são substituídas automaticamente pelos valores reais em tempo de execução. Para obter mais informações sobre essas variáveis, consulte [Criar uma política de sessão de um bucket do Amazon S3](#).

Geração dinâmica

Para provedores de identidade personalizados, gere políticas de sessão em tempo real como parte da resposta de autenticação da sua função Lambda ou método do API Gateway. Essa abordagem permite criar políticas altamente personalizadas com base em atributos do usuário, associações a grupos ou fontes de dados externas no momento da autenticação.

Você também pode armazenar políticas de sessão AWS Secrets Manager pré-geradas incluindo uma chave nomeada `Policy` com o JSON da política de sessão como valor. Isso permite que você use a mesma função ampla do IAM em vários usuários, mantendo os controles de acesso específicos do usuário.

 Note

As políticas de sessão são suportadas somente para transferências de arquivos de e para o Amazon S3. Eles não se aplicam aos sistemas de arquivos do Amazon EFS. Para o Amazon EFS, as permissões são governadas UID/GID e os bits de permissão aplicados dentro do próprio sistema de arquivos.

Implementação por tipo de usuário

Service-managed usuários

Para usuários gerenciados por serviços, você pode especificar políticas de sessão diretamente na configuração do usuário por meio do AWS Transfer Family console, da API ou da CLI. Para obter mais informações, consulte [Trabalhar com usuários gerenciados por serviços](#).

Usuários de provedores de identidade personalizados

Para usuários de provedores de identidade personalizados, você pode fornecer políticas de sessão de duas maneiras:

- AWS Secrets Manager Incluindo uma chave nomeada `Policy` com a política de sessão como valor
- Diretamente na resposta da função Lambda ou na resposta do API Gateway como parte do resultado da autenticação

Para obter mais informações, consulte [Solução personalizada de provedor de identidade](#).

Exemplo: simplificação do gerenciamento de funções com políticas de sessão

Este exemplo demonstra como o gerenciamento dinâmico de permissões pode reduzir significativamente a sobrecarga administrativa e, ao mesmo tempo, manter a segurança.

Cenário

Sua organização tem 50 usuários que precisam de acesso SFTP para transferir arquivos. Cada usuário só deve acessar sua própria pasta dentro de um bucket compartilhado do Amazon S3 chamado `company-transfers`. Sem as políticas de sessão, você precisaria criar 50 funções diferentes do IAM.

Abordagem tradicional (sem políticas de sessão)

- Crie 50 funções do IAM: `TransferRole-Alice`, `TransferRole-Bob`, `TransferRole-Charlie`, etc.
- Cada função tem permissões específicas somente para a pasta desse usuário
- O gerenciamento de permissões requer a atualização de funções individuais
- Adicionar novos usuários requer a criação de novas funções

Abordagem dinâmica (com políticas de sessão)

- Crie 1 função do IAM: `TransferRole-Shared` com amplas permissões para todo o bucket
- Use políticas de sessão para restringir cada usuário à sua pasta específica em tempo de execução
- O gerenciamento de permissões requer a atualização de uma função ou modelo de política de sessão
- Adicionar novos usuários não requer novas funções, apenas configuração do usuário

Implementação

Veja como você implementaria a abordagem dinâmica (usando o `company-transfers` bucket como exemplo para ser substituído pelo seu bucket real do Amazon S3):

Para implementar o gerenciamento dinâmico de permissões

1. Crie uma função compartilhada do IAM com amplas permissões do Amazon S3:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```

        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
    ],
    "Resource": "arn:aws:s3:::company-transfers/*"
},
{
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::company-transfers"
}
]
}

```

2. Crie um modelo de política de sessão que restrinja o acesso à pasta do usuário:

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::company-transfers/${transfer:Username}/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::company-transfers",
            "Condition": {
                "StringLike": {
                    "s3:prefix": "${transfer:Username}*"
                }
            }
        }
    ]
}

```

3. Configure cada usuário com:

- A função compartilhada do IAM
- A política de sessão foi aplicada da seguinte forma:
 - Service-managed usuários: use a API ou a CLI para aplicar o JSON por meio do parâmetro Policy ao criar ou modificar usuários (o console oferece apenas opções de política predefinidas)
 - Usuários de provedores de identidade personalizados: retorne-a como parte da resposta da função Lambda durante a autenticação ou armazene-a AWS Secrets Manager como uma chave chamada “Política” junto com as credenciais do usuário
- Diretório inicial: `/company-transfers/${transfer:Username}/`

AWS CloudTrail registrando para AWS Transfer Family

AWS Transfer Family integra-se com ambos AWS CloudTrail e com a Amazon CloudWatch. CloudTrail e CloudWatch servem propósitos diferentes, mas complementares.

- Este tópico aborda a integração com CloudTrail, um AWS serviço que cria um registro das ações realizadas em sua Conta da AWS. Ele monitora e registra continuamente as operações da API para atividades como logins, AWS Command Line Interface comandos e SDK/API operações do console. Isso permite que você mantenha um registro de quem realizou qual ação, quando e de onde. CloudTrail ajuda na auditoria, no gerenciamento de acesso e na conformidade regulatória, fornecendo um histórico de todas as atividades em seu AWS ambiente. Para obter detalhes, consulte o [Guia AWS CloudTrail do usuário](#).
- [CloudWatch Registro na Amazon para AWS Transfer Family servidores](#) abrange a integração com CloudWatch, um serviço de monitoramento de AWS recursos e aplicativos. Ele coleta métricas e registros para fornecer visibilidade sobre a utilização de recursos, o desempenho do aplicativo e a integridade geral do sistema. CloudWatch ajuda nas tarefas operacionais, como solução de problemas, configuração de alarmes e escalonamento automático. Para obter detalhes, consulte o [Guia CloudWatch do usuário da Amazon](#).

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

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos para AWS Transfer Family, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para 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 eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- [Visão geral da criação de uma trilha](#)
- [CloudTrail serviços e integrações suportados](#)

- [Configurando notificações do Amazon SNS para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#) e [Recebendo arquivos de CloudTrail log de várias contas](#)

Todas AWS Transfer Family as ações são registradas CloudTrail e documentadas no [ActionsAPI reference](#). Por exemplo, chamadas para o `CreateServer` `ListUsers` e `StopServer` as ações geram entradas nos arquivos de CloudTrail log.

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 de AWS Identity and Access Management usuário.
- 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 AWS serviço.

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para AWS Transfer Family. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos.

Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AWS Transfer Family, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

Tópicos

- [Ativar AWS CloudTrail registro](#)
- [Exemplo de entrada de registro para criar um servidor](#)
- [Exemplos de registros de acesso a dados](#)

Ativar AWS CloudTrail registro

Você pode monitorar as operações AWS Transfer Family da API usando AWS CloudTrail o. Ao monitorar as operações da API, você pode obter informações operacionais e de segurança úteis. Se você tiver o [registro em log no nível de objeto do Amazon S3 ativado](#), RoleSessionName está contido no campo Solicitante como [AWS:Role Unique Identifier]/username.sessionid@server-id. Para obter mais informações sobre identificadores exclusivos de funções AWS Identity and Access Management (IAM), consulte [Identificadores exclusivos](#) no Guia do AWS Identity and Access Management usuário.

Important

O tamanho máximo do RoleSessionName é 64 caracteres. Se o RoleSessionName for mais longo, server-id ficará truncado.

Habilitando eventos de dados do Amazon S3

Para rastrear operações de arquivos realizadas AWS Transfer Family em seus buckets do Amazon S3, você precisa habilitar eventos de dados para esses buckets. Os eventos de dados fornecem atividade de API em nível de objeto e são particularmente úteis para rastrear uploads, downloads e outras operações realizadas pelos usuários. AWS Transfer Family

Para habilitar eventos de dados do Amazon S3 para seu AWS Transfer Family servidor:

1. Abra o CloudTrail console em <https://console.aws.amazon.com/cloudtrail/>.
2. No painel de navegação, escolha Trilhas e, em seguida, selecione uma trilha existente ou crie uma nova.
3. Em Eventos de dados, escolha Editar.
4. Em Tipo de evento de dados, selecione S3.
5. Escolha os buckets do Amazon S3 para registrar eventos de dados. Você pode registrar eventos de dados para todos os buckets ou especificar buckets individuais.
6. Escolha se deseja registrar eventos de leitura, eventos de gravação ou ambos.
7. Escolha Salvar alterações.

Depois de habilitar os eventos de dados, você pode acessar esses logs no bucket do Amazon S3 configurado para sua CloudTrail trilha. Os registros incluem detalhes como o usuário que realizou a ação, o registro de data e hora da ação, o objeto específico afetado e o `onBehalfOf` campo que ajuda a rastrear `userId` as ações realizadas. AWS Transfer Family

Exemplo de entrada de registro para criar um servidor

O exemplo a seguir mostra uma entrada de CloudTrail registro (no formato JSON) que demonstra a `CreateServer` ação.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAA4FFF5HHHHH6NNWWW:user1",
    "arn": "arn:aws:sts::123456789102:assumed-role/Admin/user1",
    "accountId": "123456789102",
    "accessKeyId": "AAAA52C2WWWWW3BB4Z",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-12-18T20:03:57Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAAA4FFF5HHHHH6NNWWW",
        "arn": "arn:aws:iam::123456789102:role/Admin",
        "accountId": "123456789102",
        "userName": "Admin"
      }
    }
  },
  "eventTime": "2024-02-05T19:18:53Z",
  "eventSource": "transfer.amazonaws.com",
  "eventName": "CreateServer",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "11.22.1.2",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36",
  "requestParameters": {
    "domain": "S3",
    "hostKey": "HIDDEN_DUE_TO_SECURITY_REASONS",
```

```

    "protocols": [
      "SFTP"
    ],
    "protocolDetails": {
      "passiveIp": "AUTO",
      "tlsSessionResumptionMode": "ENFORCED",
      "setStatOption": "DEFAULT"
    },
    "securityPolicyName": "TransferSecurityPolicy-2020-06",
    "s3StorageOptions": {
      "directoryListingOptimization": "ENABLED"
    }
  },
  "responseElements": {
    "serverId": "s-1234abcd5678efghi"
  },
  "requestID": "6fe7e9b1-72fc-45b0-a7f9-5840268aeadf",
  "eventID": "4781364f-7c1e-464e-9598-52d06aa9e63a",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789102",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "transfer.us-east-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
}

```

Exemplos de registros de acesso a dados

Ao habilitar eventos de dados do Amazon S3 para sua CloudTrail trilha, você pode rastrear as operações de arquivos realizadas por meio de AWS Transfer Family. Esses registros ajudam você a monitorar quem acessou quais dados, quando e como.

Exemplo de entrada de registro para acesso bem-sucedido aos dados

O exemplo a seguir mostra uma entrada de CloudTrail registro de uma operação bem-sucedida de download de arquivos por meio de AWS Transfer Family.

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:TransferSessionUser",
    "arn": "arn:aws:sts::123456789012:assumed-role/TransferS3AccessRole/TransferSessionUser",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/TransferS3AccessRole",
        "accountId": "123456789012",
        "userName": "TransferS3AccessRole"
      },
      "attributes": {
        "creationDate": "2025-07-15T16:12:05Z",
        "mfaAuthenticated": "true"
      }
    },
    "invokedBy": "transfer.amazonaws.com"
  },
  "eventTime": "2025-07-15T16:15:22Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "bucketName": "my-transfer-bucket",
    "key": "users/john.doe/reports/quarterly-report-2025-Q2.pdf",
    "Host": "my-transfer-bucket.s3.amazonaws.com",
    "x-amz-request-payer": "requester"
  },
  "responseElements": null,
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2458732,
  }
}

```

```

    "x-amz-id-2":
      "EXAMPLE123456789+abcdefghijklmnopqrstuvxyzABCDEFGHIJKLMNOPQRSTUVWXYZ="
    },
    "requestID": "EXAMPLE123456789",
    "eventID": "example12-3456-7890-abcd-ef1234567890",
    "readOnly": true,
    "resources": [
      {
        "type": "AWS::S3::Object",
        "ARN": "arn:aws:s3:::my-transfer-bucket/users/john.doe/reports/quarterly-report-2025-Q2.pdf"
      },
      {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::my-transfer-bucket"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "requestParameters": {
      "x-amz-onBehalfOf": "john.doe.sessionid@s-abcd1234efgh5678"
    }
  }
}

```

Neste exemplo, observe os seguintes campos importantes:

- `eventName`: indica a operação da API S3 que foi executada (GetObject para o download de um arquivo).
- `requestParameters.bucketName` e `requestParameters.key`: Mostre qual objeto do S3 foi acessado.
- `additionalEventData.bytesTransferredOut`: mostra o tamanho do arquivo baixado em bytes.
- `requestParameters.x-amz-onBehalfOf`: contém o AWS Transfer Family nome de usuário e o ID da sessão, permitindo rastrear qual AWS Transfer Family usuário executou a ação.

O `x-amz-onBehalfOf` campo é particularmente importante, pois vincula a chamada da API S3 ao AWS Transfer Family usuário específico que iniciou a ação. Esse campo segue o formato `username.sessionid@server-id`, em que:

- `username` é o AWS Transfer Family nome de usuário.
- `sessionid` é um identificador exclusivo para a sessão do usuário.
- `server-id` é o ID do AWS Transfer Family servidor.

Operações comuns de acesso a dados

Ao monitorar o acesso aos dados AWS Transfer Family, você normalmente verá as seguintes operações da API S3 em seus CloudTrail registros:

Operações comuns do S3 em registros AWS Transfer Family

Operação da API S3	AWS Transfer Family Ação	Description
GetObject	Download do arquivo	O usuário baixou um arquivo do servidor
PutObject	Upload de arquivo	O usuário enviou um arquivo para o servidor
DeleteObject	Exclusão de arquivo	O usuário excluiu um arquivo do servidor
ListObjects ou ListObjects V2	Listagem de diretórios	Arquivos listados pelo usuário em um diretório
CopyObject	Cópia do arquivo	O usuário copiou um arquivo dentro do servidor

Ao monitorar essas operações em seus CloudTrail registros, você pode rastrear todas as atividades de arquivos realizadas por meio de seu AWS Transfer Family servidor, ajudando você a atender aos requisitos de conformidade e detectar acesso não autorizado.

CloudWatch Registro na Amazon para AWS Transfer Family servidores

CloudWatch A Amazon é um poderoso serviço de monitoramento e observabilidade que fornece visibilidade abrangente de seus AWS recursos, inclusive AWS Transfer Family.

- **Real-time monitoramento:** CloudWatch monitora os recursos e aplicativos da Transfer Family em tempo real, permitindo que você acompanhe e analise seu desempenho.
- **Coleção de métricas:** CloudWatch coleta e rastreia várias métricas para seus recursos e aplicativos, que são variáveis que você pode medir e usar para análise.
- **CloudWatch página inicial:** a página CloudWatch inicial exibe automaticamente métricas sobre o Transfer Family e outros AWS serviços que você usa, fornecendo uma visão centralizada dos seus dados de monitoramento.
- **Painéis personalizados:** você pode criar painéis personalizados CloudWatch para exibir métricas específicas para seus aplicativos personalizados e os recursos que você escolhe monitorar.
- **Alarmes e notificações:** CloudWatch permite criar alarmes que monitoram suas métricas e acionam notificações ou ações automatizadas quando determinados limites são violados. Isso pode ser útil para monitorar a atividade de transferência de arquivos nos servidores do Transfer Family e dimensionar os recursos adequadamente.
- **Otimização de custos:** você pode usar os dados coletados por CloudWatch para identificar recursos subutilizados e tomar medidas, como interromper ou excluir instâncias, para otimizar seus custos.

No geral, os recursos abrangentes de monitoramento o CloudWatch tornam uma ferramenta valiosa para gerenciar e otimizar sua infraestrutura da Transfer Family e os aplicativos executados nela.

Os detalhes de CloudWatch registro dos aplicativos web Transfer Family estão disponíveis em [CloudTrail registro para aplicativos web Transfer Family](#).

Tipos de CloudWatch registro para Transfer Family

O Transfer Family fornece duas maneiras de registrar eventos em CloudWatch:

- Registro de log estruturado em JSON
- Registro por meio de uma função de registro

Para servidores Transfer Family, você pode escolher o mecanismo de registro de sua preferência. Para conectores e fluxos de trabalho, somente funções de registro são suportadas.

Registro estruturado em JSON

Para registrar eventos do servidor, recomendamos usar o registro estruturado JSON. Isso fornece um formato de registro mais abrangente que permite a consulta de CloudWatch registros. Para esse tipo de registro, a política do IAM para o usuário que cria o servidor (ou edita a configuração de registro do servidor) deve conter as seguintes permissões:

- logs:CreateLogDelivery
- logs>DeleteLogDelivery
- logs:DescribeLogGroups
- logs:DescribeResourcePolicies
- logs:GetLogDelivery
- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

Veja abaixo um exemplo de política .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

```
]
}
```

Para obter detalhes sobre como configurar o registro estruturado JSON, consulte [Criação, atualização e visualização de registros para servidores](#).

Função de registro

Para registrar eventos para um fluxo de trabalho gerenciado conectado a um servidor, bem como para conectores, você precisa especificar uma função de registro. Para definir o acesso, crie uma política do IAM com base em recursos e um perfil do IAM que forneça as informações daquele acesso. Veja a seguir um exemplo de política para uma Conta da AWS que pode registrar eventos do servidor.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

Para obter detalhes sobre como configurar uma função de registro para registrar eventos do fluxo de trabalho, consulte [Gerenciando registros para fluxos de trabalho](#).

Criação, atualização e visualização de registros para servidores

Para todos os AWS Transfer Family servidores, fornecemos registros estruturados. Recomendamos que você use o registro estruturado para todos os servidores Transfer Family novos e existentes. Os benefícios de usar o registro estruturado incluem o seguinte:

- Receba logs em um formato JSON estruturado.

- Consulte seus registros com o Amazon CloudWatch Logs Insights, que descobre automaticamente campos formatados em JSON.
- O compartilhamento de grupos de registros entre AWS Transfer Family recursos permite combinar fluxos de registros de vários servidores em um único grupo de registros, facilitando o gerenciamento das configurações de monitoramento e retenção de registros.
- Crie métricas e visualizações agregadas que podem ser adicionadas aos CloudWatch painéis.
- Monitore dados de uso e desempenho usando grupos de logs para criar métricas, visualizações e painéis de logs consolidados.

Para habilitar o registro em fluxos de trabalho conectados aos servidores, você deve usar uma função de registro.

 Note

Quando você adiciona uma função de registro, o grupo de registro está sempre `/aws/transfer/your-serverID` e não pode ser alterado. Isso significa que, a menos que você esteja enviando seus registros estruturados do servidor para o mesmo grupo, você estará se conectando a dois grupos de registro separados.

Se você sabe que vai associar um fluxo de trabalho ao seu servidor e, portanto, precisa adicionar uma função de registro, você pode configurar o registro estruturado para registrar no grupo de registros padrão de `/aws/transfer/your-serverID`.

Para modificar seu grupo de registro, consulte [StructuredLogDestinations](#) na Referência AWS Transfer Family da API.

Se você criar um novo servidor usando o console do Transfer Family, o registro em log é habilitado por padrão. Depois de criar o servidor, você pode usar a operação da `UpdateServer` API para alterar sua configuração de registro. Para obter detalhes, consulte [StructuredLogDestinations](#).

Atualmente, para fluxos de trabalho, se quiser o registro em log habilitado, você deve especificar uma função de registro em log:

- Se você associar um fluxo de trabalho a um servidor, usando a operação `CreateServer` ou a `UpdateServer` API, o sistema não criará automaticamente uma função de registro. Se quiser registrar em log seus eventos de fluxo de trabalho, você precisa anexar explicitamente uma função de registro em log ao servidor.

- Se você criar um servidor usando o console do Transfer Family e anexar um fluxo de trabalho, os registros em logs serão enviados para um grupo de registros de logs que contém a ID do servidor no nome. O formato é `/aws/transfer/server-id`, por exemplo, `/aws/transfer/s-1111aaaa2222bbbb3`. Os registros em logs do servidor podem ser enviados para esse mesmo grupo de logs ou para um diferente.

Considerações sobre registro em logs para criar e editar servidores no console

- Os novos servidores criados por meio do console oferecem suporte apenas ao registro em log JSON estruturado, a menos que um fluxo de trabalho esteja anexado ao servidor.
- Nenhum log não é uma opção para novos servidores que você cria no console.
- Os servidores existentes podem habilitar registro em log JSON estruturado por meio do console em qualquer período.
- Habilitar registro em log JSON estruturado por meio do console desabilita o método de registro em logs existente para não cobrar duas vezes dos clientes. A exceção será se um fluxo de trabalho for anexado ao servidor.
- Se você habilitar registro em log JSON estruturado, não poderá desabilitá-lo posteriormente por meio do console.
- Se você habilitar registro em log JSON estruturado, poderá alterar o destino do grupo de logs por meio do console em qualquer período.
- Se você habilitar registro em log JSON estruturado, não poderá editar a função de registro em log por meio do console se tiver habilitado os dois tipos de log por meio da API. A exceção será se seu servidor tiver um fluxo de trabalho anexado. No entanto, a função de log continua aparecendo em Detalhes adicionais.

Considerações sobre registros em logs para criar e editar servidores usando API ou SDK

- Se você criar um novo servidor por meio da API, poderá configurar um ou os dois tipos de log ou optar por nenhum log.
- Para servidores existentes, habilite e desabilite o registro em log JSON estruturado em qualquer período.
- Você pode alterar o grupo de logs por meio da API em qualquer período.
- Você pode alterar a função de registro em log por meio da API em qualquer período.

Para habilitar o registro em log estruturado, você deve estar conectado a uma conta com as seguintes permissões

- `logs:CreateLogDelivery`
- `logs>DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

Um exemplo de política está disponível na seção [Configurar função de CloudWatch registro](#).

Tópicos

- [Criação de registros para servidores](#)
- [Atualizando registro em logs de um servidor](#)
- [Como visualizar a configuração do servidor](#)

Criação de registros para servidores

Ao criar um novo servidor, na página Configurar detalhes adicionais, você pode especificar um grupo de logs existente ou criar um novo.

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

Note Logging role is only required when selecting a workflow in the Managed workflows section below.

Se você escolher Criar grupo de registros, o CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) abrirá a página Criar grupo de registros. Para obter detalhes, consulte [Criar um grupo de CloudWatch registros em Registros](#).

Atualizando registro em logs de um servidor

Os detalhes dos registros em logs dependem do cenário da sua atualização.

Note

Quando você opta pelo registro em log JSON estruturado, pode haver um atraso, em casos raros, em que o Transfer Family para o registro no formato antigo, mas leva algum tempo para iniciar o registro em log no novo formato JSON. Isso pode resultar em eventos que não são registrados. Não haverá qualquer interrupções no serviço, mas você deve ter cuidado ao transferir arquivos durante a primeira hora após a alteração do método de registro em logs, pois os logs podem ser descartados.

Se você estiver editando um servidor existente, suas opções dependerão do estado do servidor.

- O servidor já tem uma função de registro em log habilitada, mas não tem o registro em log JSON estruturado habilitado.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/scooter ▼



Create log group [↗](#)

Enabling the structured JSON log format will override your existing logging configuration. Potential changes include new log format and log group.

Logging Role [Info](#)

Select an existing role from your account

AWSTransferLoggingAccess ▼



Workflows events will be delivered to a log group labelled with the server ID.

- O servidor não tem nenhum registro em log habilitado.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☐ Enable structured JSON logging

Choose an existing log group ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- O servidor já tem um registro em log JSON estruturado habilitada, mas não tem uma função de registro em log especificada.

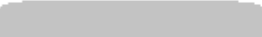
Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/  ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- O servidor já tem um Registro em log JSON estruturado habilitado, e tem uma função de registro em log especificada.

Edit additional details

Logging [Info](#)

Log group [Info](#)
Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

▼

Logging Role [Info](#)
Select an existing role from your account

▼

 Workflows events will be delivered to a log group labelled with the server ID.

Como visualizar a configuração do servidor

Os detalhes da página de configuração do servidor dependem do seu cenário:

Dependendo do seu cenário, a página de configuração do servidor pode ter a aparência de um dos exemplos a seguir:

- Nenhum log está habilitado.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [REDACTED]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role -	Passive IP -

- O registro em log JSON estruturado está habilitado.

Additional details
Edit

Log group /aws/transfer/s[REDACTED]	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [REDACTED]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role -	Passive IP -

- A função de registro em log está habilitada, mas o registro em log JSON estruturado não está habilitado.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:lx39/	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role execution-role	Passive IP -

- Ambos os tipos de registro em log (função de registro em log e registro em log JSON estruturado) estão habilitados.

Additional details
Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows	Passive IP -

Gerenciando registros para fluxos de trabalho

CloudWatch fornece auditoria e registro consolidados para o progresso e os resultados do fluxo de trabalho. Além disso, AWS Transfer Family fornece várias métricas para fluxos de trabalho. Você pode visualizar métricas de quantas execuções de fluxos de trabalho foram iniciadas, concluídas com êxito e falharam no minuto anterior. Todas as CloudWatch métricas do Transfer Family estão descritas em [Usando CloudWatch métricas para servidores Transfer Family](#).

Veja os CloudWatch registros da Amazon para fluxos de trabalho

1. Abra o CloudWatch console da Amazon em <https://console.aws.amazon.com/cloudwatch/>.

2. No painel de navegação à esquerda, escolha Logs e, em seguida, escolha Grupos de logs.
3. Na página Grupos de registros, na barra de navegação, escolha a região correta para seu AWS Transfer Family servidor.
4. Escolha o grupo de logs que corresponde ao seu servidor.

Por exemplo, se o ID do seu servidor for `s-1234567890abcdef0`, seu grupo de logs será `/aws/transfer/s-1234567890abcdef0`.

5. Na página de detalhes do grupo de logs do seu servidor, os fluxos de log mais recentes são exibidos. Há dois fluxos de log para o usuário que você está explorando:
 - Um para cada sessão do File Transfer Protocol (SFTP) da Secure Shell (SSH).
 - Um para o fluxo de trabalho que está sendo executado no seu servidor. O formato do fluxo de logs do fluxo de trabalho é `username.workflowID.uniqueStreamSuffix`.

Por exemplo, se o seu usuário é `mary-major`, você terá os seguintes fluxos de logs:

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

 Note

Os identificadores alfanuméricos de 16 dígitos listados neste exemplo são fictícios. Os valores que você vê na Amazon CloudWatch são diferentes.

A página Eventos de log para o `mary-major-usa-east.1234567890abcdef0` exibe os detalhes de cada sessão do usuário, e o fluxo de logs para o `mary.w-abcdef01234567890.021345abcdef6789` contém os detalhes do fluxo de trabalho.

Veja a seguir um exemplo de fluxo de logs para o `mary.w-abcdef01234567890.021345abcdef6789`, com base em um fluxo de trabalho (`w-abcdef01234567890`) que contém uma etapa de cópia.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
```

```

        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
    }
}
},
"workflowId": "w-abcdef01234567890",
"executionId": "execution-id",
"transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
}
},
{
    "type": "StepStarted",
    "details": {
        "input": {
            "fileLocation": {
                "backingStore": "S3",
                "bucket": "amzn-s3-demo-bucket",
                "key": "mary/workflowSteps2.json",
                "versionId": "version-id",
                "etag": "etag-id"
            }
        },
        "stepType": "COPY",
        "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
        "serverId": "s-server-id",
        "username": "mary",
        "sessionId": "session-id"
    }
},
{
    "type": "StepCompleted",
    "details": {
        "output": {},
        "stepType": "COPY",
        "stepName": "copyToShared"
    }
}

```

```

    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "ExecutionCompleted",
    "details": {},
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  }
}

```

Configurar função de CloudWatch registro

Para definir o acesso, crie uma política do IAM com base em recursos e um perfil do IAM que forneça as informações daquele acesso.

Para habilitar o CloudWatch registro na Amazon, você começa criando uma política do IAM que permite o CloudWatch registro. Crie um perfil do IAM e anexe a política a ele. É possível fazer isso quando estiver [criando um servidor](#) ou [editando um servidor existente](#). Para obter mais informações sobre CloudWatch, consulte [O que é a Amazon CloudWatch?](#) e [O que são CloudWatch registros da Amazon?](#) no Guia do CloudWatch usuário da Amazon.

Use o exemplo de políticas do IAM a seguir para permitir o CloudWatch registro.

Use a logging role

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",

```



```

    "Effect": "Allow",
    "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
  }
]
}

```

Use structured logging

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs>ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}

```

No exemplo anterior de política, para o **Resource**, substitua o *region-id* e *Conta da AWS* por seus valores. Por exemplo, **"Resource": "arn:aws::logs:us-east-1:111122223333:log-group:/aws/transfer/*"**.

Em seguida, você cria uma função e anexa a política de CloudWatch registros que você criou.

Para criar um perfil do IAM e anexar uma política

1. No painel de navegação, escolha Perfis e Criar perfil.

Na página Criar função, certifique-se de que AWS Serviço foi escolhido.

2. Selecione Transferir na lista de serviço, e Próximo: Permissões. Isso estabelece uma relação de confiança entre AWS Transfer Family e a função do IAM. Além disso, adicione as chaves de condição `aws:SourceAccount` e `aws:SourceArn` para se proteger contra o problema de "confused deputy". Para obter mais detalhes, consulte a documentação a seguir:

- Procedimento para estabelecer uma relação de confiança com AWS Transfer Family:
[Estabelecer um relacionamento de confiança](#)
- Descrição do problema de "confused deputy": [o problema do "confused deputy"](#)

3. Na seção Anexar políticas de permissões, localize e escolha a política de CloudWatch registros que você acabou de criar e escolha Avançar: Tags.
4. (Opcional) Insira uma chave e um valor para a tag e selecione Próximo: análise.
5. Na página Análise, insira um nome e uma descrição para a sua nova função, e escolha Criar função.
6. Para visualizar os logs, escolha o ID do servidor para abrir a página de configuração do servidor e selecione Visualizar logs. Você é redirecionado para o CloudWatch console, onde pode ver seus fluxos de log.

Na CloudWatch página do seu servidor, você pode ver registros de autenticação do usuário (sucesso e falha), uploads de dados (PUToperações) e downloads de dados (GEToperações).

Visualizando fluxos de registros do Transfer Family

Para ver os logs do servidor Transfer Family

1. Navegar até a página de detalhes de um servidor.
2. Selecione Exibir logs. Isso abre a Amazon CloudWatch.
3. O grupo de logs do servidor selecionado é exibido.

CloudWatch X

CloudWatch > Log groups > /aws/transfer/s-

/aws/transfer/s- Actions View in Logs Insights Search log group

Log group details

ARN arn:aws:logs:us-east-2:5:log-group:/aws/transfer/s-:*	Metric filters 0 Subscription filters 0 Contributor Insights rules -	Data protection - new Inactive Sensitive data found - new - KMS key ID -

Creation time
2 years ago

Retention
Never expire

Stored bytes
39.39 MB

Log streams Metric filters Subscription filters Contributor Insights Tags Data protection - new

Log streams (10) [Refresh] [Delete] [Create log stream] [Search all log streams]

Q Filter log streams or try prefix search ☐ Exact match ☐ Show expired Info < 1 > [Settings]

☐ Log stream	Last event
☐ ERRORS	2023-
☐ scooterstack4-	2023-
☐ scooterstack4-	2023-
☐ scooterstack4-	2023-

4. É possível selecionar um fluxo de logs para exibir detalhes e entradas individuais do fluxo.
- Se houver uma lista de ERROS, é possível escolhê-la para ver os detalhes dos erros mais recentes do servidor.

CloudWatch > Log groups > /aws/transfer/s- > ERRORS

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

↻

Actions ▾

Create metric filter

🔍 Filter events

Clear 1m 30m 1h 12h Custom

📅

Display ▾

⚙️

▶	Timestamp	Message	
There are older events to load. Load more.			
▶	2023-03-23T16:08:29.281-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:30.979-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:32.647-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:34.306-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:36.010-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:37.659-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:12:33.307-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
▼	2023-03-23T16:12:34.943-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
		ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" SourceIP=	Copy
▼	2023-03-23T16:12:56.857-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
▼	2023-03-23T16:12:58.430-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
▶	2023-03-23T16:13:00.106-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	

- Escolha qualquer outra entrada para ver um exemplo de fluxo de logs.

CloudWatch > Log groups > /aws/transfer/s- > scooterstack4.

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

↻

Actions ▾

Create metric filter

🔍 Filter events

Clear 1m 30m 1h 12h Custom

📅

Display ▾

⚙️

▶	Timestamp	Message	
No older events at this moment. Retry			
▼	2023-03-23T16:19:43.747-04:00	scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- Client=SSH-2.0- OpenSSH_7.4 Role=arn:aws:iam:: :role/ Kex=	Copy
▼	2023-03-23T16:19:47.030-04:00	scooterstack4. DISCONNECTED scooterstack4. DISCONNECTED	Copy
No newer events at this moment. Auto retry paused. Resume			

Visualizando fluxos de registros do Transfer Family

600

- Se seu servidor tiver um fluxo de trabalho gerenciado associado a ele, é possível visualizar os logs das execuções do fluxo de trabalho.

Note

O formato do fluxo de logs do fluxo de trabalho é `username.workflowId.uniqueStreamSuffix`. Por exemplo, `decrypt-user.w-a1111222233334444.aaaa1111bbbb2222` pode ser o nome de um fluxo de logs para usuário **decrypt-user** e fluxo de trabalho **w-a1111222233334444**.

CloudWatch > Log groups > /aws/transfer/s- > decrypt-user.w-

Log events
You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions Create metric filter

Filter events Clear 1m 30m 1h 12h Custom Display

Timestamp	Message
2023-03-21T13:37:57.795-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-user/test.json.gpg", "versionId": "...", "etag": "..." } } } }
2023-03-21T14:12:02.850-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-user/test.json.gpg", "versionId": "...", "etag": "..." } } } }
2023-03-21T14:12:03.464-04:00	{ "type": "StepCompleted", "details": { "output": { } }, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-" }

Note

Para qualquer entrada de log expandida, é possível copiar a entrada para a área de transferência escolhendo Copiar. Para obter mais detalhes sobre CloudWatch registros, consulte [Visualização de dados de registro](#).

Criação de CloudWatch alarmes na Amazon

O exemplo a seguir mostra como criar CloudWatch alarmes da Amazon usando a AWS Transfer Family métrica,FilesIn.

CDK

```
new cloudwatch.Metric({
  namespace: "AWS/Transfer",
  metricName: "FilesIn",
  dimensionsMap: { ServerId: "s-000000000000000000" },
  statistic: "Average",
  period: cdk.Duration.minutes(1),
}).createAlarm(this, "AWS/Transfer FilesIn", {
  threshold: 1000,
  evaluationPeriods: 10,
  datapointsToAlarm: 5,
  comparisonOperator:
    cloudwatch.ComparisonOperator.GREATER_THAN_OR_EQUAL_TO_THRESHOLD,
});
```

CloudFormation

```
Type: AWS::CloudWatch::Alarm
Properties:
  Namespace: AWS/Transfer
  MetricName: FilesIn
  Dimensions:
    - Name: ServerId
      Value: s-000000000000000000
  Statistic: Average
  Period: 60
  Threshold: 1000
  EvaluationPeriods: 10
  DatapointsToAlarm: 5
  ComparisonOperator: GreaterThanOrEqualToThreshold
```

Registrando as operações da API do Amazon S3 nos logs de acesso do S3

Note

Esta seção não se aplica aos aplicativos web Transfer Family.

Se você estiver [usando os logs de acesso do Amazon S3 para identificar solicitações de S3](#) feitas em nome de seus usuários de transferência de arquivos, RoleSessionName é usado para exibir qual perfil do IAM foi assumido para atender às transferências de arquivos. Ele também exibe informações adicionais, como nome de usuário, ID da sessão e ID do servidor usados para as transferências. O formato é [AWS:Role Unique Identifier]/username.sessionid@server-id e está contido no campo Solicitante. Por exemplo, a seguir está o conteúdo de um campo de exemplo de Solicitante de um log de acesso do S3 para um arquivo que foi copiado para o bucket do S3.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/  
username.sessionid@server-id
```

No campo Solicitante acima, ele mostra o perfil do IAM chamado IamRoleName. Para obter mais informações sobre identificadores exclusivos do perfil do IAM, consulte [Identificadores exclusivos](#) no Guia do usuário do AWS Identity and Access Management .

Exemplos para limitar o problema de "confused deputy"

O problema "confused deputy" é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executar a ação. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. Consulte mais detalhes em [Cross-service prevenção delegada confusa](#).

Note

Nos exemplos a seguir, substitua cada um *user input placeholder* por suas próprias informações.

Nesses exemplos, você pode remover os detalhes do ARN de um fluxo de trabalho se o servidor não tiver nenhum fluxo de trabalho vinculado a ele.

O exemplo de logging/invoke política a seguir permite que qualquer servidor (e fluxo de trabalho) na conta assumam a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

O exemplo de logging/invoke política a seguir permite que um servidor específico (e fluxo de trabalho) assumam a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificServerWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
    }
  ]
}
```



```

    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:transfer:us-west-2:111122223333:server/server-id",
          "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-
id"
        ]
      }
    }
  }
]
}

```

CloudWatch estrutura de log para Transfer Family

Este tópico descreve os campos que são preenchidos nos registros do Transfer Family: tanto para entradas de registro estruturadas JSON quanto para entradas de registro legadas.

Tópicos

- [Registros estruturados JSON para Transfer Family](#)
- [Registros legados para Transfer Family](#)

Registros estruturados JSON para Transfer Family

A tabela a seguir contém detalhes dos campos de entrada de registro para SFTP/FTP/FTPS ações do Transfer Family, no novo formato de log estruturado JSON.

Campo	Description	Exemplo de entrada
tipo de atividade	A ação do usuário	Os tipos de atividades disponíveis são os seguintes: AUTH_FAILURE CONNECTED ,DISCONNECTED ,ERROR,EXIT_REAS

Campo	Description	Exemplo de entrada
		ON ,CLOSE,CREATE_SY MLINK ,DELETE,MKDIR,OPEN,PARTIA LOSE ,RENAME,RMDIR,SETSTAT,TLS_ E_FAILURE .
bytes-in	Número de bytes enviados pelo usuário	29238420042
saída de bytes	Número de bytes baixados pelo usuário	23094032490328
ciphers	Especifica a cifra SSH negociada para a conexão (as cifras disponíveis estão listadas em) Algoritmos criptográficos	aes256-gcm@openssh.com
client	O software cliente do usuário	SSH-2.0-OpenSSH_7,4
diretório inicial	O diretório em que o usuário final acessa quando se conecta ao endpoint, se o tipo de diretório inicial for PATH: se ele tiver um diretório inicial lógico, esse valor será sempre /	/página inicial do usuário-- bucket/test
kex	Especifica a troca de chaves SSH (KEX) negociada para a conexão (as KEX disponíveis estão listadas em) Algoritmos criptográficos	diffie-hellman-group14-sha256
message	Fornece mais informações relacionadas ao erro	<string>
method	O método de autenticação	publickey

Campo	Description	Exemplo de entrada
modo	Especifica como um cliente abre um arquivo	CRIAR TRUNCAR ESCREVER
operação	A operação do cliente em um arquivo	ABRIR FECHAR
caminho	Caminho real do arquivo afetado	bucket/test/amzn-s3-demo- - file-1.pdf
chave pública ssh	O corpo da chave pública para o usuário que está se conectando	AAAAC3NzaC1lZDI1NT E5AAAAIA9OY0qV6XYV HaaOiWAcj2spDJVbgj rqDPY4pxd6GnHl
impressão digital de chave pública ssh-	A impressão digital da chave pública, conforme mostrada no console para usuários gerenciados pelo serviço ao listar suas chaves de usuário.	SHA256:BY3gNMHwTfj d4n2VuT4pTyLOk82zW Zj4KEYEu7y4r/0

 Note

No console, a impressão digital é exibida com os caracteres de preenchimento (se houver): de 0 a 3 sinais iguais (=) no final. Na entrada de registro, esse preenchimento é retirado da saída.

Campo	Description	Exemplo de entrada
tipo de chave pública ssh	Tipo de chave pública: o Transfer Family suporta RSA, ECDSA e chaves ED25519-formatted	ssh-ed25519
ganho de recursos	Um identificador exclusivo atribuído pelo sistema para um recurso específico (por exemplo, um servidor)	arn: aws: transferência: ap-nordeste-1:12346789012:-1234567890akeu2js2 server/s
perfil	A função do IAM do usuário	arn: aws: iam: 0293883675: -role role/testuser
session-id	Um identificador exclusivo atribuído pelo sistema para uma única sessão	9ca9a0e1cec6ad9d
ip de origem	Endereço IP do cliente	18.323.0.129
usuário	O nome de usuário do usuário final	meu nome 192
política de usuário	As permissões especificadas para o usuário final: esse campo será preenchido se a política do usuário for uma política de sessão.	O código JSON para a política de sessão que está sendo usada

Registros legados para Transfer Family

A tabela a seguir contém detalhes das entradas de registro de várias ações do Transfer Family.

Note

Essas entradas não estão no novo formato de log estruturado JSON.

A tabela a seguir contém detalhes das entradas de registro para várias ações do Transfer Family, no novo formato de log estruturado JSON.

Ação	Registros correspondentes no Amazon CloudWatch Logs
Falhas de autenticação	ERROS AUTH_FAILURE METHOD=publicKey user=Ihr message="RSA +b7 +a+hxg0c711jiz0" sourceIP=3.8.172.211 SHA256:Lfz3R2nmLY4raK Rb1rSvUIbAE
COPY/TAG/DELETE/DECRYPT fluxo de trabalho	<pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "BackingStore": "EFS", "fileSystemId": "fs-12345678", "path": "/Ihr/regex.py" }, "stepType": "TAG", "stepName": "successful_tag_step", "workflowName": "successful_tag_step", "workflowId": "w-11aaaa2222bbbb3", "ExecutionId": "81234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverId": "s-1234abcd5678efghi", "nome de usuário": "Ihr", "sessionId": "1234abcd5678efghi", "nome de usuário": "Ihr", "sessionId": "1234abcd5678efghi", "nome de usuário": "Ihr", "sessionId": "1234abcd5678efghi", "nome de usuário": "Ihr", "sessionId": "1234abcd567890abcdef0" } } } }</pre>
Fluxo de trabalho personalizado das etapas	<pre>{ "type": "CustomStepInvoked", "details": { "output": { "token": "", "stepType": "CUSTOM", "stepName": "efs-s3_copy_2", "workflowId": "w-9283e49d33297c3f7", "ExecutionId": "1234abcd-123gh-ef-123gh-ef7-5678-ijklmnopqr90", "TransferDetails": { "serverId": "s-zzzz1111aaaa22223", "nome de usuário": "Ihr", "sessionId": "1234567890abcdef" } } } }</pre>

Ação	Registros correspondentes no Amazon CloudWatch Logs
	0"}} MzM4Mjg5YWUtYTEzMy00YjZlLWI3OGMtYzU4OGI2ZjQyMzE5
Exclui	lhr.33a8fb495ffb383b EXCLUIR CAMINHO =/ /123.jpg bucket/user
Downloads	lhr.33a8fb495ffb383b ABRIR CAMINHO=/ /123.jpg MODE=LER bucket/user llhr.33a8fb495ffb383b FECHAR CAMINHO =/ /123.jpg =3618546 bucket/user BytesOut
Logins/Logouts	user.914984e553bcddb6 FONTE CONECTADA IP=1.22.111.222 usuário=L HR =Cliente LÓGICO= _7.4 role=arn: aws: :iam: :123456789012: -s3-access HomeDir SSH-2.0-OpenSSH role/sftp user.914984e553bcddb6 DISCONNECTED
Renomeia	lhr.33a8fb495ffb383b RENOMEAR CAMINHO=/ /lambo.png =/ /ferrari.png bucket/ user NewPath bucket/user
Exemplo de log de erros do fluxo de trabalho	{"type": "StepErrored", "details": {"errorType": "BAD_REQUEST", "errorMessage": "Não é possível marcar o arquivo Efs", "stepType": "TAG", "stepName": "successful_tag_step"}, "workflowID": "w-1234abcd5678efghi", "executionId": "81234abcd-1234-efgh-5678-ijklmnopqr90", "TransferDetails": {"serverID": "s-1234abcd5678efghi", "nome de usuário": "lhr", "SessionID": "1234567890abcdef0"}}

Ação	Registros correspondentes no Amazon CloudWatch Logs
Symlinks	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK =/fs- /pqr.jpg =abc.jpg LinkPath 12345678/lhr TargetPath
Uploads	lhr.33a8fb495ffb383b ABRIR CAMINHO=/ /123.jpg mode=Create truncate Write bucket/user lhr.33a8fb495ffb383b FECHAR CAMINHO =/ /123.jpg =3618546 bucket/user BytesIn
Fluxos de trabalho	<pre>{ "type": "ExecutionStarted", "details": { "input": { "initial FileLocation": { "BackingStore": "EFS", "fileSystemID": "fs-12345678", "path": "/lhr/regex.py" }, "WorkflowId": "w-11aaaa2222bbbb3", "ExecutionId": "1234abcB3", "d-1234-efgh-5678-ijklmnopqr90", "TransferDetails": { "serverID": "s-zzzz11aaaa22223", "nome de usuário": "lhr", "sessionID": "1234567890abcdef0" } } } }</pre> <pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "BackingStore": "EFS", "fileSystemID": "fs-12345678", "path": "/lhr/regex.py" }, "stepType": "CUSTOM", "stepName": "efs-s3_copy_2", "WorkflowId": "w-9283e49d33297c3f7", "executionId": "1234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverID": "s-18ca49dce5d842e0b", "nome de usuário": "lhr", "sID da sessão": "1234567890abcdef0" } } } }</pre>

Exemplo de entradas CloudWatch de registro

Este tópico apresenta exemplos de entradas de registro.

Tópicos

- [Exemplo de entradas de registro de sessões de transferência](#)
- [Exemplo de entradas de registro para conectores SFTP](#)
- [Exemplo de entradas de registro para conectores VPC Lattice](#)
- [Exemplo de entradas de registro para falhas no algoritmo de troca de chaves](#)

Exemplo de entradas de registro de sessões de transferência

Neste exemplo, um usuário do SFTP se conecta a um servidor Transfer Family, carrega um arquivo e depois se desconecta da sessão.

A entrada de registro a seguir reflete um usuário SFTP se conectando a um servidor Transfer Family.

```
{
  "role": "arn:aws:iam::500655546075:role/transfer-s3",
  "activity-type": "CONNECTED",
  "ciphers": "chacha20-poly1305@openssh.com,chacha20-poly1305@openssh.com",
  "client": "SSH-2.0-OpenSSH_7.4",
  "source-ip": "52.94.133.133",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "home-dir": "/test/log-me",
  "ssh-public-key":
"AAAAC3NzaC1lZDI1NTE5AAAAIA90Y0qV6XYVHaa0iWAcj2spDJVbgjrQDPY4pxd6GnH1",
  "ssh-public-key-fingerprint": "SHA256:BY3gNMHwTfjd4n2VuT4pTyL0k82zWZj4KEYEu7y4r/0",
  "ssh-public-key-type": "ssh-ed25519",
  "user": "log-me",
  "kex": "ecdh-sha2-nistp256",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

A entrada de registro a seguir reflete o usuário do SFTP fazendo o upload de um arquivo em seu bucket do Amazon S3.

```
{
  "mode": "CREATE|TRUNCATE|WRITE",
  "path": "/test/log-me/config-file",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
}
```



```
{
  "session-id": "9ca9a0e1cec6ad9d"
}
```

As entradas de registro a seguir refletem o usuário do SFTP se desconectando da sessão do SFTP. Primeiro, o cliente fecha a conexão com o bucket e, em seguida, desconecta a sessão SFTP.

```
{
  "path": "/test/log-me/config-file",
  "activity-type": "CLOSE",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "bytes-in": "121",
  "session-id": "9ca9a0e1cec6ad9d"
}

{
  "activity-type": "DISCONNECTED",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

Note

Os tipos de atividades disponíveis são os seguintes:

AUTH_FAILURE, RECONNECTED, DISCONNECTED, ERROR, EXIT_REASON, CLOSE, CREATE_SYMLINK, DELETE

Exemplo de entradas de registro para conectores SFTP

Esta seção contém registros de exemplo de uma transferência bem-sucedida e malsucedida. Os registros são gerados em um grupo de registros chamado `/aws/transfer/connector-id`, onde *connector-id* está o identificador do seu conector SFTP. As entradas de registro para conectores SFTP são geradas quando você executa um comando `StartFileTransfer` ou `StartDirectoryListing`.

Essa entrada de registro é para uma transferência que foi concluída com êxito.

```
{
  "operation": "RETRIEVE",
```

```

    "timestamp": "2023-10-25T16:33:27.373720Z",
    "connector-id": "connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://192.0.2.0",
    "file-path": "/remotebucket/remotefilepath",
    "status-code": "COMPLETED",
    "start-time": "2023-10-25T16:33:26.945481Z",
    "end-time": "2023-10-25T16:33:27.159823Z",
    "account-id": "480351544584",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "local-directory-path": "/connectors-localbucket",
    "bytes": 514,
    "egress-type": "SERVICE_MANAGED"
  }

```

Essa entrada de registro é para uma transferência que atingiu o tempo limite e, portanto, não foi concluída com êxito.

```

{
  "operation": "RETRIEVE",
  "timestamp": "2023-10-25T22:33:47.625703Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://192.0.2.0",
  "file-path": "/remotebucket/remotefilepath",
  "status-code": "FAILED",
  "failure-code": "TIMEOUT_ERROR",
  "failure-message": "Transfer request timeout.",
  "account-id": "480351544584",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
  "local-directory-path": "/connectors-localbucket",
  "egress-type": "SERVICE_MANAGED"
}

```

Essa entrada de registro é para uma operação SEND bem-sucedida.

```

{
  "operation": "SEND",
  "timestamp": "2024-04-24T18:16:12.513207284Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",

```

```

    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/amzn-s3-demo-bucket/my-test-folder/connector-metrics-us-east-1-2024-01-02.csv",
    "status-code": "COMPLETED",
    "start-time": "2024-04-24T18:16:12.295235884Z",
    "end-time": "2024-04-24T18:16:12.461840732Z",
    "account-id": "255443218509",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "bytes": 275,
    "egress-type": "SERVICE_MANAGED"
  }

```

Descrições de alguns campos-chave nos exemplos de registro anteriores.

- `timestamp` representa quando o registro é adicionado CloudWatch a. `start-time` e `end-time` correspondem a quando o conector realmente inicia e termina uma transferência.
- `transfer-id` é um identificador exclusivo atribuído a cada `start-file-transfer` solicitação. Se o usuário passar vários caminhos de arquivo em uma única operação de `start-file-transfer` API, todos os arquivos compartilharão o mesmo `transfer-id`.
- `file-transfer-id` é um valor exclusivo gerado para cada arquivo transferido. Observe que a parte inicial do `file-transfer-id` é a mesma que `transfer-id`.

Exemplo de entradas de registro para conectores VPC Lattice

Esta seção contém registros de exemplo para conectores VPC Lattice. Para conectores VPC Lattice, os registros incluem campos adicionais que fornecem informações sobre a configuração do conector e a configuração da rede.

Essa entrada de registro é para uma operação SEND do conector VPC Lattice que foi concluída com êxito.

```

{
  "operation": "SEND",
  "timestamp": "2025-09-05T14:20:19.577192454Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "file-path": ""/amzn-s3-demo-bucket/my-test-folder/connector-vpc-lattice-us-east-1-2025-03-22.csv"",

```

```

"status-code": "COMPLETED",
"start-time": "2025-09-05T14:20:19.434072509Z",
"end-time": "2025-09-05T14:20:19.481453346Z",
"account-id": "account-id",
"connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
"remote-directory-path": "/test-bucket/test-folder/",
"bytes": 262,
"egress-type": "VPC_LATTICE",
"vpc-lattice-resource-configuration-arn": "arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/resource-configuration-arn-id",
"vpc-lattice-port-number": 22
}

```

Os registros do conector VPC Lattice incluem os seguintes campos adicionais:

- `egress-type`- Tipo de configuração de saída para o conector
- `vpc-lattice-resource-configuration-arn`- ARN da configuração de recursos de rede VPC que define a localização do servidor SFTP de destino
- `vpc-lattice-port-number`- Número da porta para conexão com o servidor SFTP por meio do VPC Lattice

Exemplo de entradas de registro para falhas no algoritmo de troca de chaves

Esta seção contém exemplos de registros em que o algoritmo de troca de chaves (KEX) falhou. Esses são exemplos do fluxo de registros ERRORS para registros estruturados.

Essa entrada de registro é um exemplo em que há um erro de tipo de chave de host.

```

{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-999999999999999999",
  "message": "no matching host key type found",
  "kex": "ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519,ssh-rsa,ssh-dss"
}

```

Essa entrada de registro é um exemplo em que há uma incompatibilidade de KEX.

```
{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-99999999999999999999",
  "message": "no matching key exchange method found",
  "kex": "diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group14-sha256"
}
```

Usando CloudWatch métricas para servidores Transfer Family

Note

Você também pode obter métricas para o Transfer Family no próprio console do Transfer Family. Para obter detalhes, consulte [Monitoramento do uso no console](#)

Você pode obter informações sobre seu servidor usando CloudWatch métricas. Uma métrica representa um conjunto ordenado por tempo de pontos de dados publicados em. CloudWatch Ao usar métricas, você deve especificar o namespace do Transfer Family, o nome da métrica e a [dimensão](#). Para obter mais informações sobre métricas, consulte [Métricas](#) no Guia CloudWatch do usuário da Amazon.

A tabela a seguir descreve as CloudWatch métricas do Transfer Family.

Namespace	Métrica	Description
AWS/Transfer	BytesIn	O número total de bytes transferidos para o servidor. Critérios de relatório: Para SFTP/FTP/FTPS: emitido a cada 5 minutos enquanto uma conexão é estabelecida com o servidor Transfer Family. Se nenhum arquivo ou byte for transferido no período, "0" será emitido.

Namespace	Métrica	Description
		Para AS2: quando o cliente recebe uma mensagem em seu servidor AS2 e é emitida assim que a mensagem de entrada termina de ser processada Unidades: contagem Período: 5 minutos
	BytesOut	O número total de bytes transferidos do servidor. Critérios de relatório: - Para SFTP/FTP/FTPS: emitido a cada 5 minutos enquanto uma conexão é estabelecida com o servidor Transfer Family. Se nenhum arquivo ou byte for transferido no período, "0" será emitido. - Para AS2: quando o cliente liga <code>StartFile Transfer</code> de seu conector AS2 e emite assim que a mensagem de saída termina de ser processada. Unidades: contagem Período: 5 minutos

Namespace	Métrica	Description
	FilesIn	O número total de arquivos transferidos para o servidor. Para servidores que usam o protocolo AS2, essa métrica representa o número de mensagens recebidas. Critérios de relatório: • Para SFTP/FTP/FTPS: emitido a cada 5 minutos enquanto uma conexão é estabelecida com o servidor Transfer Family. Se nenhum arquivo ou byte for transferido no período, "0" será emitido. • Para AS2: quando o cliente recebe uma mensagem em seu servidor AS2 e é emitida assim que a mensagem de entrada termina de ser processada. Unidades: contagem Período: 5 minutos
	FilesOut	O número total de arquivos transferidos do servidor. Critérios de relatório: • Para SFTP/FTP/FTPS: emitido a cada 5 minutos enquanto uma conexão é estabelecida com o servidor Transfer Family. Se nenhum arquivo ou byte for transferido no período, "0" será emitido. • Para AS2: quando o cliente liga <code>StartFile Transfer</code> de seu conector AS2 e emite assim que a mensagem de saída termina de ser processada. Unidades: contagem Período: 5 minutos

Namespace	Métrica	Description
	InboundMessage	O número total de mensagens AS2 recebidas com êxito de um parceiro comercial. Critérios de emissão de relatórios: quando o cliente recebe uma mensagem em seu servidor AS2 e é emitida assim que o processamento da mensagem de entrada é concluído com êxito Unidades: contagem Período: 5 minutos
	InboundFailedMessage	O número total de mensagens AS2 que não foram recebidas com êxito de um parceiro comercial. Ou seja, um parceiro comercial enviou uma mensagem, mas o servidor Transfer Family não conseguiu processá-la com êxito. Critérios de emissão de relatórios: quando o cliente recebe uma mensagem em seu servidor AS2 e é emitida assim que o processamento da mensagem de entrada é concluído sem sucesso Unidades: contagem Período: 5 minutos
	OnUploadExecutionsStarted	O número total de execuções de fluxo de trabalho iniciadas no servidor. Critérios de emissão de relatórios: acionados sempre que uma execução é iniciada Unidades: contagem Período: 1 minuto

Namespace	Métrica	Description
	OnUploadExecutionsSuccess	O número total de execuções de fluxo de trabalho bem-sucedidas no servidor. Critérios de emissão de relatórios: acionados sempre que uma execução é concluída com sucesso Unidades: contagem Período: 1 minuto
	OnUploadExecutionsFailed	O número total de execuções de fluxo de trabalho malsucedidas no servidor. Critérios de emissão de relatórios: acionados sempre que uma execução não é concluída com êxito Unidades: contagem Período: 1 minuto
	OutboundMessage	O número total de mensagens AS2 enviadas com sucesso a um parceiro comercial. Critérios de emissão de relatórios: quando o cliente liga <code>StartFileTransfer</code> de seu conector AS2 e emite assim que o processamento da mensagem de saída é concluído com êxito Unidades: contagem Período: 5 minutos

Namespace	Métrica	Description
	OutboundFailedMessage	O número total de mensagens AS2 que foram enviadas sem sucesso a um parceiro comercial. Critérios de emissão de relatórios: quando o cliente liga <code>StartFileTransfer</code> de seu conector AS2 e é emitida assim que o processamento da mensagem de saída é concluído sem sucesso Unidades: contagem Período: 5 minutos

Dimensões do Transfer Family

Uma dimensão é um name/value par que faz parte da identidade de uma métrica. Para obter mais informações sobre dimensões, consulte [Dimensões](#) no Guia do CloudWatch usuário da Amazon.

A tabela a seguir descreve as CloudWatch dimensões do Transfer Family.

Dimensão	Description
ServerId	O ID exclusivo do usuário.
ConnectorId	O ID exclusivo do conector. Usado para AS2, para OutboundMessage e OutboundFailedMessage

Usando Notificações de Usuários da AWS com AWS Transfer Family

Para ser notificado sobre AWS Transfer Family eventos, você pode usar [Notificações de Usuários da AWS](#) para configurar vários canais de entrega. Você recebe uma notificação quando um evento corresponde a uma regra especificada por você.

É possível receber notificações para eventos por meio de diversos canais, incluindo o e-mail, o [Amazon Q Developer em aplicações de chat](#), notificações por chat ou notificações push do [AWS](#)

[Console Mobile Application](#). Você também pode ver as notificações na [Central de Notificações do Console](#). Notificações de Usuários suporta agregação, o que pode reduzir o número de notificações que você recebe durante eventos específicos.

Para obter mais informações, consulte a postagem do blog [Personalizar notificações de entrega de arquivos usando fluxos de trabalho AWS Transfer Family gerenciados](#) e [O que é Notificações de Usuários da AWS?](#) no Guia do Notificações de Usuários da AWS usuário.

Usando consultas para filtrar entradas de registro

Você pode usar CloudWatch consultas para filtrar e identificar entradas de registro do Transfer Family. Esta seção contém alguns exemplos.

1. Faça login no Console de gerenciamento da AWS e abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. Você pode criar consultas ou regras.
 - Para criar uma consulta do Logs Insights, escolha Logs Insights no painel de navegação esquerdo e insira os detalhes da sua consulta.
 - Para criar uma regra do Contributor Insights, escolha Insights > Contributor Insights no painel de navegação esquerdo e, em seguida, insira os detalhes da sua regra.
3. Execute a consulta ou regra que você criou.

Veja os principais contribuidores de falhas de autenticação

Em seus registros estruturados, uma entrada de registro de falha de autenticação é semelhante à seguinte:

```
{
  "method": "password",
  "activity-type": "AUTH_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "message": "Invalid user name or password",
  "user": "exampleUser"
}
```

Execute a consulta a seguir para ver os principais contribuintes para falhas de autenticação.

```
filter @logStream = 'ERRORS'
| filter `activity-type` = 'AUTH_FAILURE'
| stats count() as AuthFailures by user, method
| sort by AuthFailures desc
| limit 10
```

Em vez de usar o CloudWatch Logs Insights, você pode criar uma regra do CloudWatch Contributors Insights para visualizar as falhas de autenticação. Crie uma regra semelhante à seguinte.

```
{
  "AggregateOn": "Count",
  "Contribution": {
    "Filters": [
      {
        "Match": "$.activity-type",
        "In": [
          "AUTH_FAILURE"
        ]
      }
    ],
    "Keys": [
      "$.user"
    ]
  },
  "LogFormat": "JSON",
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "LogGroupARNs": [
    "arn:aws:logs:us-east-1:999999999999:log-group:/customer/structured_logs"
  ]
}
```

Exibir entradas de registro em que um arquivo foi aberto

Em seus registros estruturados, uma entrada de registro de leitura de arquivo é semelhante à seguinte:

```
{
  "mode": "READ",
  "path": "/fs-0df669c89d9bf7f45/avtester/example",
```

```
"activity-type":"OPEN",  
"resource-arn":"arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",  
"session-id":"0049cd844c7536c06a89"  
}
```

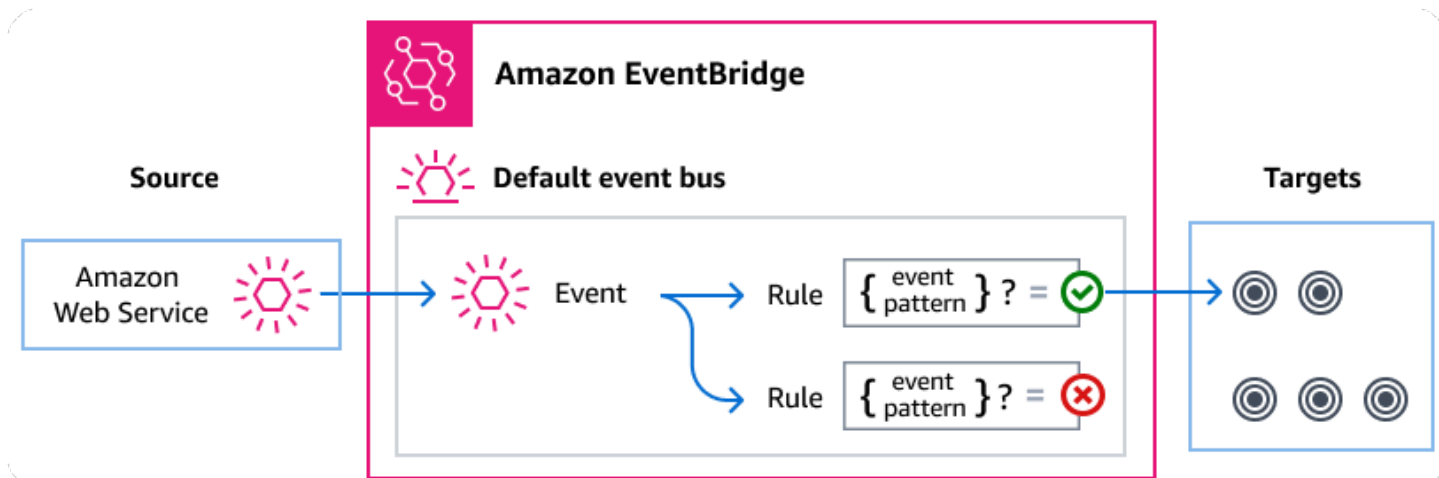
Execute a consulta a seguir para visualizar as entradas de registro que indicam que um arquivo foi aberto.

```
filter `activity-type` = 'OPEN'  
| display @timestamp, @logStream, `session-id`, mode, path
```

Gerenciamento Transfer Family eventos usando Amazon EventBridge

Amazon EventBridge é um serviço sem servidor que usa eventos para conectar componentes do aplicativo, o que pode facilitar a criação de aplicativos escaláveis orientados por eventos. Event-driven arquitetura é um estilo de construir sistemas de software fracamente acoplados que trabalham juntos emitindo e respondendo a eventos. Os eventos representam uma mudança em um recurso ou ambiente.

Como acontece com muitos AWS serviços, Transfer Family gera e envia eventos para o barramento de eventos EventBridge padrão. Observe que o barramento de eventos padrão é provisionado automaticamente em todas as AWS contas. Um barramento de eventos é um roteador que recebe eventos e os entrega a zero ou mais destinos, ou alvos. Você especifica regras para o barramento de eventos que avalia os eventos à medida que eles chegam. Cada regra verifica se um evento corresponde ao padrão do evento. Se o evento corresponder, o barramento de eventos enviará o evento para um ou mais destinos especificados.



Tópicos

- [Transfer Family eventos](#)
- [Enviando Transfer Family eventos usando EventBridge regras](#)
- [Amazon EventBridge permissões](#)
- [Adicional EventBridge recursos](#)
- [Transfer Family referência de detalhes de eventos](#)

Transfer Family eventos

Transfer Family envia eventos automaticamente para o barramento de EventBridge eventos padrão. Você pode criar regras no barramento de eventos em que cada regra inclui um padrão de evento e um ou mais alvos.

Os eventos que correspondem ao padrão de eventos de uma regra são entregues às metas especificadas com o melhor esforço possível ou de forma duradoura (observe que alguns eventos podem ser entregues fora de ordem). Esses níveis de entrega são descritos em [Nível de entrega para eventos AWS de serviço](#) na Amazon EventBridge Events Reference.

- Server-level os eventos para servidores SFTP, FTPS e FTP são entregues com base no melhor esforço.
- Os eventos do conector SFTP são fornecidos de forma durável.
- Os eventos AS2 são realizados de forma durável.

Os eventos a seguir são gerados por Transfer Family. Para obter mais informações, consulte [Eventos do EventBridge](#), no Guia do usuário do Amazon EventBridge .

Eventos de servidor SFTP, FTPS e FTP

As tabelas a seguir listam os eventos dos servidores SFTP, FTPS e FTP, organizados por tipo de evento.

Eventos de upload e download de arquivos

Tipo de detalhe de evento	Description
Download do arquivo do servidor FTP concluído	Um arquivo foi baixado com sucesso para o protocolo FTP.
Falha no download do arquivo do servidor FTP	Houve falha na tentativa de baixar um arquivo para o protocolo FTP.
Carregamento do arquivo do servidor FTP concluído	Um arquivo foi carregado com sucesso para o protocolo FTP.

Tipo de detalhe de evento	Description
Falha no upload do arquivo do servidor FTP	Houve falha na tentativa de carregar um arquivo para o protocolo FTP.
Download do arquivo do servidor FTPS concluído	Um arquivo foi baixado com sucesso para o protocolo FTPS.
Falha no download do arquivo do servidor FTPS	Houve falha na tentativa de baixar um arquivo para o protocolo FTPS.
Carregamento do arquivo do servidor FTPS concluído	Um arquivo foi carregado com sucesso para o protocolo FTPS.
Falha no upload do arquivo do servidor FTPS	Houve falha na tentativa de carregar um arquivo para o protocolo FTPS.
Download do arquivo do servidor SFTP concluído	Um arquivo foi baixado com sucesso para o protocolo SFTP.
Falha no download do arquivo do servidor SFTP	Houve falha na tentativa de baixar um arquivo para o protocolo SFTP.
Carregamento do arquivo do servidor SFTP concluído	Um arquivo foi carregado com sucesso para o protocolo SFTP.
Falha no carregamento do arquivo do servidor SFTP	Houve falha na tentativa de carregar um arquivo para o protocolo SFTP.

Outros eventos de operações de arquivo

Tipo de detalhe de evento	Description
Criação do diretório do servidor FTP concluída	Um diretório foi criado com sucesso para o protocolo FTP.
Falha na criação do diretório do servidor FTP	Houve falha na tentativa de criar um diretório para o protocolo FTP.

Tipo de detalhe de evento	Description
<u>Exclusão do diretório do servidor FTP concluída</u>	Um diretório foi excluído com sucesso para o protocolo FTP.
<u>Falha na exclusão do diretório do servidor FTP</u>	Houve falha na tentativa de excluir um diretório para o protocolo FTP.
<u>A exclusão do arquivo do servidor FTP foi concluída</u>	Um arquivo foi excluído com sucesso para o protocolo FTP.
<u>Falha na exclusão do arquivo do servidor FTP</u>	Houve falha na tentativa de excluir um arquivo para o protocolo FTP.
<u>Renomeação do arquivo do servidor FTP concluída</u>	Um arquivo foi renomeado com sucesso para o protocolo FTP.
<u>Falha na renomeação do arquivo do servidor FTP</u>	Houve falha na tentativa de renomear um arquivo para o protocolo FTP.
<u>Criação do diretório do servidor FTPS concluída</u>	Um diretório foi criado com sucesso para o protocolo FTPS.
<u>Falha na criação do diretório do servidor FTPS</u>	Houve falha na tentativa de criar um diretório para o protocolo FTPS.
<u>Exclusão do diretório do servidor FTPS concluída</u>	Um diretório foi excluído com sucesso para o protocolo FTPS.
<u>Falha na exclusão do diretório do servidor FTPS</u>	Houve falha na tentativa de excluir um diretório para o protocolo FTPS.
<u>A exclusão do arquivo do servidor FTPS foi concluída</u>	Um arquivo foi excluído com sucesso para o protocolo FTPS.
<u>Falha na exclusão do arquivo do servidor FTPS</u>	Houve falha na tentativa de excluir um arquivo no protocolo FTPS.
<u>Renomeação do arquivo do servidor FTPS concluída</u>	Um arquivo foi renomeado com sucesso para o protocolo FTPS.

Tipo de detalhe de evento	Description
Falha na renomeação do arquivo do servidor FTPS	Houve falha na tentativa de renomear um arquivo para o protocolo FTPS.
Criação do diretório do servidor SFTP concluída	Um diretório foi criado com sucesso para o protocolo SFTP.
Falha na criação do diretório do servidor SFTP	Houve falha na tentativa de criar um diretório para o protocolo SFTP.
Exclusão do diretório do servidor SFTP concluída	Um diretório foi excluído com sucesso para o protocolo SFTP.
Falha na exclusão do diretório do servidor SFTP	Houve falha na tentativa de excluir um diretório para o protocolo SFTP.
A exclusão do arquivo do servidor SFTP foi concluída	Um arquivo foi excluído com sucesso para o protocolo SFTP.
Falha na exclusão do arquivo do servidor SFTP	Houve falha na tentativa de excluir um arquivo para o protocolo SFTP.
Renomeação do arquivo do servidor SFTP concluída	Um arquivo foi renomeado com sucesso para o protocolo SFTP.
Falha na renomeação do arquivo do servidor SFTP	Houve falha na tentativa de renomear um arquivo para o protocolo SFTP.

Eventos do conector SFTP

Note

Esses eventos são entregues EventBridge em um nível durável, conforme descrito em [Nível de entrega para eventos AWS de serviço](#) na Referência de EventBridge Eventos da Amazon.

Tipo de detalhe de evento	Description
Envio do arquivo do conector SFTP concluído	A transferência de arquivo de um conector para um servidor SFTP remoto foi concluída com êxito.
Falha no envio do arquivo do conector SFTP	Uma transferência de arquivo de um conector para um servidor SFTP remoto falhou.
Recuperação do arquivo do conector SFTP concluída	Uma transferência de arquivo de um servidor SFTP remoto para um conector foi concluída com êxito.
Falha na recuperação do arquivo do conector SFTP	Uma transferência de arquivo de um servidor SFTP remoto para um conector falhou.
Lista de diretórios de conectores SFTP concluída	Uma chamada de listagem do diretório de arquivos inicial que foi concluída com êxito.
Falha na listagem do diretório do conector SFTP	Uma listagem do diretório do arquivo inicial que falhou.
Movimentação remota do conector SFTP concluída	Os arquivos ou diretórios foram movidos ou renomeados com êxito no servidor remoto.
Falha na movimentação remota do conector SFTP	Não foi possível mover ou renomear arquivos ou diretórios no servidor remoto.
Exclusão remota do conector SFTP concluída	Os arquivos ou diretórios foram excluídos com sucesso no servidor remoto.
Falha na exclusão remota do conector SFTP	Não foi possível excluir arquivos ou diretórios no servidor remoto.

Eventos AS2

Note

Esses eventos são entregues EventBridge em um nível durável, conforme descrito em [Nível de entrega para eventos AWS de serviço](#) na Referência de EventBridge Eventos da Amazon.

Tipo de detalhe de evento	Description
Recebimento do AS2 Payload concluído	A carga útil de uma mensagem AS2 foi recebida.
Falha no recebimento da carga útil do AS2	A carga útil de uma mensagem AS2 não foi recebida.
Envio do AS2 Payload concluído	A carga útil de uma mensagem AS2 foi enviada com sucesso.
Falha no envio da carga útil do AS2	Falha no envio da carga útil de uma mensagem AS2.
Recebimento AS2 MDN concluído	A notificação de disposição da mensagem para uma mensagem AS2 foi recebida.
Falha na recepção do AS2 MDN	A notificação de disposição da mensagem para uma mensagem AS2 não foi recebida.
Envio AS2 MDN concluído	A notificação de disposição da mensagem para uma mensagem AS2 foi enviada com sucesso.
Falha no envio do AS2 MDN	A notificação de disposição da mensagem para uma mensagem AS2 falhou no envio.

Enviando Transfer Family eventos usando EventBridge regras

Se você quiser que o barramento de eventos EventBridge padrão envie Transfer Family eventos para um destino, você deve criar uma regra que contenha um padrão de evento que corresponda aos dados dos Transfer Family eventos desejados.

Para capturar AWS Transfer Family eventos na Amazon EventBridge

1. Faça login no Console de gerenciamento da AWS e abra o EventBridge console da Amazon em <https://console.aws.amazon.com/events/>.
2. No painel de navegação, escolha Regras e, em seguida, escolha Criar regra.
3. Insira um nome descritivo para a regra e, opcionalmente, insira uma descrição.

4. Em Tipo de regra, selecione Regra com um padrão de evento e escolha Avançar.
5. Na seção Origem do evento, selecione AWS eventos ou eventos de EventBridge parceiros.
6. Na seção Método de criação, escolha Usar formulário padrão.
7. Na seção Padrão de eventos, forneça as seguintes informações.
 - a. Em Fonte do evento, selecione Serviços da AWS .
 - b. Para o AWS serviço, escolha Transferir.
 - c. Em Tipo de evento, escolha o tipo de evento Transfer Family que você deseja acionar sua regra.

Dependendo da seleção do tipo de evento, você pode receber uma seção Especificação 1 do tipo de evento.

- d. Se você ver a seção Especificação do tipo de evento 1, selecione os eventos específicos que deseja capturar (ou selecione Qualquer evento para capturar todos os eventos do tipo de evento selecionado).
 - e. (Opcional) Use o editor de padrões de eventos para especificar filtros para detalhes do evento.
 - f. Escolha Próximo.
8. Escolha um alvo entre as opções disponíveis em Selecionar alvos. Escolha entre os seguintes alvos disponíveis.
 - AWS serviço. As opções mais populares são funções Lambda para computação sem servidor, filas do Amazon SQS para processamento de mensagens, tópicos do Amazon SNS para notificações e para orquestrar fluxos de trabalho. AWS Step Functions
 - EventBridge Destino da API. Se você quiser enviar eventos para um endpoint HTTP externo AWS, você pode usar um destino de API como seu destino.
 - EventBridge ônibus de eventos. Você pode enviar eventos para outro ônibus de eventos, na mesma conta e região ou em uma conta ou região diferente.

Para obter instruções abrangentes sobre a criação de regras de barramento de eventos, consulte [Criação de regras que reagem a eventos](#) no Guia EventBridge do usuário da Amazon.

Para obter ajuda na seleção de um alvo, consulte [Selecionar alvos](#) no Guia EventBridge do usuário da Amazon.

9. Configure todas as opções adicionais para seu alvo e escolha Avançar.
10. (Opcional) Adicione tags à sua regra e escolha Avançar.
11. Na tela Revisar e criar, se tudo estiver correto, escolha Criar regra.

Criação de padrões de eventos para Transfer Family eventos

Ao Transfer Family entregar um evento ao barramento de eventos padrão, EventBridge usa o padrão de evento definido para cada regra para determinar se o evento deve ser entregue aos destinos da regra. Um padrão de evento corresponde aos dados nos eventos do Transfer Family desejados. Cada padrão de evento é um objeto JSON que contém o seguinte:

- Um atributo `source` que identifica o serviço que envia o evento. Para Transfer Family eventos, a fonte é `aws.transfer`.
- (Opcional) Um `detail-type` atributo que contém uma matriz dos tipos de eventos a serem correspondentes.
- (Opcional) Um `detail` atributo contendo quaisquer outros dados de eventos aos quais corresponder.

Por exemplo, o padrão de eventos a seguir corresponde a todos os eventos de Transfer Family:

```
{
  "source": ["aws.transfer"]
}
```

O exemplo de padrão de evento a seguir corresponde a todos os eventos do conector SFTP:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Connector File Send Completed", "SFTP Connector File Retrieve Completed",
                  "SFTP Connector File Retrieve Failed", "SFTP Connector File Send Failed"]
}
```

O exemplo de padrão de evento a seguir corresponde a todos os eventos com falha do Transfer Family:

```
{
```

```
"source": ["aws.transfer"],
"detail-type": [{"wildcard", "*Failed"}]
}
```

O exemplo de padrão de evento a seguir corresponde a downloads de SFTP bem-sucedidos para o usuário *username*:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Server File Download Completed"],
  "detail": {
    "username": [username]
  }
}
```

Para obter mais informações sobre como escrever padrões de eventos, consulte [Padrões de eventos](#) no Guia do usuário do EventBridge .

Testando padrões de eventos para Transfer Family eventos em EventBridge

Você pode usar o EventBridge Sandbox para definir e testar rapidamente um padrão de evento, sem precisar concluir o processo mais amplo de criação ou edição de uma regra. Usando o Sandbox, você pode definir um padrão de evento e usar um evento de amostra para confirmar se o padrão corresponde aos eventos desejados. EventBridge oferece a opção de criar uma nova regra usando esse padrão de evento diretamente da sandbox.

Para obter mais informações, consulte [Testando um padrão de evento usando o EventBridge Sandbox](#) no Guia do EventBridge usuário.

Amazon EventBridge permissões

Transfer Family não exige nenhuma permissão adicional para realizar eventos Amazon EventBridge.

Os alvos que você especificar podem exigir permissões ou configurações específicas. Para obter mais detalhes sobre o uso de serviços específicos para destinos, consulte [Destinos do Amazon EventBridge](#) no Guia do usuário do Amazon EventBridge .

Adicional EventBridge recursos

Consulte os tópicos a seguir no [Guia do Amazon EventBridge usuário](#) para obter mais informações sobre como usar EventBridge para processar e gerenciar eventos.

- Para obter informações detalhadas sobre como os barramentos de eventos funcionam, consulte [Barramento de eventos do Amazon EventBridge](#).
- Para obter informações sobre a estrutura de eventos, consulte [Eventos](#)
- Para obter informações sobre a construção de padrões de eventos EventBridge para uso ao comparar eventos com regras, consulte [Padrões de eventos](#).
- Para obter informações sobre a criação de regras para especificar quais eventos são processados pelo EventBridge , consulte [Regras](#).
- Para obter informações sobre como especificar quais serviços ou outros destinos EventBridge enviam eventos correspondentes, consulte [Metas](#).

Transfer Family referência de detalhes de eventos

Todos os eventos dos AWS serviços têm um conjunto comum de campos contendo metadados sobre o evento. Esses metadados podem incluir o AWS serviço que é a origem do evento, a hora em que o evento foi gerado, a conta e a região em que o evento ocorreu, entre outros. Para obter as definições desses campos gerais, consulte [Referência da estrutura de eventos](#) no Guia do usuário do Amazon EventBridge .

Além disso, cada evento tem um campo de `detail` que contém dados específicos desse determinado evento. A referência a seguir define os campos de detalhes dos vários Transfer Family eventos.

Ao usar EventBridge para selecionar e gerenciar Transfer Family eventos, considere o seguinte:

- O `source` campo para todos os eventos de Transfer Family está definido como `aws.transfer`.
- O campo do `detail-type` especifica o tipo de evento.

Por exemplo, `.FTP Server File Download Completed`

- O campo de `detail` contém os dados específicos desse determinado evento.

Para obter mais informações sobre a criação de padrões de eventos que habilitam regras para corresponder a eventos do Transfer Family , consulte [Padrões de eventos](#) no Guia do usuário do Amazon EventBridge .

Para obter mais informações sobre eventos e como EventBridge os processa, consulte [Amazon EventBridge eventos](#) no Guia Amazon EventBridge do usuário.

Tópicos

- [Eventos de servidor SFTP, FTPS e FTP](#)
- [Eventos do conector SFTP](#)
- [Eventos AS2](#)

Eventos de servidor SFTP, FTPS e FTP

A seguir estão os campos de detalhes dos eventos do servidor SFTP, FTPS e FTP:

- Criação do diretório do servidor FTP concluída
- Falha na criação do diretório do servidor FTP
- A exclusão do diretório do servidor FTP foi concluída
- Falha na exclusão do diretório do servidor FTP
- A exclusão do arquivo do servidor FTP foi concluída
- Falha na exclusão do arquivo do servidor FTP
- Download do arquivo do servidor FTP concluído
- Falha no download do arquivo do servidor FTP
- Renomeação do arquivo do servidor FTP concluída
- Falha na renomeação do arquivo do servidor FTP
- Carregamento do arquivo do servidor FTP concluído
- Falha no upload do arquivo do servidor FTP
- Criação do diretório do servidor FTPS concluída
- Falha na criação do diretório do servidor FTPS
- Exclusão do diretório do servidor FTPS concluída
- Falha na exclusão do diretório do servidor FTPS
- A exclusão do arquivo do servidor FTPS foi concluída

- Falha na exclusão do arquivo do servidor FTPS
- Download do arquivo do servidor FTPS concluído
- Falha no download do arquivo do servidor FTPS
- Renomeação do arquivo do servidor FTPS concluída
- Falha na renomeação do arquivo do servidor FTPS
- Carregamento do arquivo do servidor FTPS concluído
- Falha no upload do arquivo do servidor FTPS
- Criação do diretório do servidor SFTP concluída
- Falha na criação do diretório do servidor SFTP
- A exclusão do diretório do servidor SFTP foi concluída
- Falha na exclusão do diretório do servidor SFTP
- A exclusão do arquivo do servidor SFTP foi concluída
- Falha na exclusão do arquivo do servidor SFTP
- Download do arquivo do servidor SFTP concluído
- Falha no download do arquivo do servidor SFTP
- Renomeação do arquivo do servidor SFTP concluída
- Falha na renomeação do arquivo do servidor SFTP
- Carregamento do arquivo do servidor SFTP concluído
- Falha no carregamento do arquivo do servidor SFTP

Os `detail-type` campos `source` e estão incluídos abaixo porque contêm valores específicos para Transfer Family eventos. Para obter as definições dos outros campos de metadados incluídos em todos os eventos, consulte [Referência de estrutura de eventos](#) no Guia do Amazon EventBridge usuário.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "failure-code" : "string",
    "status-code" : "string",
```

```

    "protocol" : "string",
    "bytes" : "number",
    "client-ip" : "string",
    "failure-message" : "string",
    "end-timestamp" : "string",
    "etag" : "string",
    "file-path" : "string",
    "original-file-path" : "string",
    "renamed-file-path" : "string",
    "directory-path" : "string",
    "server-id" : "string",
    "username" : "string",
    "session-id" : "string",
    "start-timestamp" : "string"
  }
}

```

detail-type

Identifica o tipo de evento.

Para esse evento, o valor é um dos nomes de eventos do servidor SFTP, FTPS ou FTP listados anteriormente.

source

Identifica o serviço que gerou o evento. Para eventos do Transfer Family, esse valor é `aws.transfer`.

detail

Um objeto JSON contém informações sobre o evento. O serviço que gera o evento determina o conteúdo desse campo.

Para esse evento, os dados incluem o seguinte:

failure-code

Categoria do motivo pelo qual a transferência falhou. Valores: `PARTIAL_UPLOAD` | `PARTIAL_DOWNLOAD` | `UNKNOWN_ERROR`

status-code

Se a transferência foi bem-sucedida. Valores: `COMPLETED` | `FAILED`.

`protocol`

O protocolo usado para a transferência. Valores: SFTP | FTPS | FTP

`bytes`

O número de bytes transferidos.

`client-ip`

O endereço IP do cliente envolvido na transferência

`failure-message`

Para transferências malsucedidas, os detalhes do motivo pelo qual a transferência falhou.

`end-timestamp`

Para transferências bem-sucedidas, o timestamp de quando o arquivo termina de ser processado.

`etag`

A tag da entidade (usada somente para arquivos do Amazon S3).

`file-path`

O caminho para o arquivo que está sendo transferido, excluído ou operado de outra forma.

`original-file-path`

Para eventos de renomeação de arquivo, o caminho original do arquivo antes da renomeação.

`renamed-file-path`

Para eventos de renomeação de arquivo, o novo caminho do arquivo após a renomeação.

`directory-path`

Para eventos de criação e exclusão de diretórios, o caminho do diretório.

`server-id`

O ID exclusivo do servidor Transfer Family.

`username`

O usuário que está realizando a transferência.

`session-id`

O identificador exclusivo da sessão de transferência.

start-timestamp

Para transferências bem-sucedidas, a data e hora de início do processamento do arquivo.

Example Exemplo de evento de falha no download do arquivo do servidor SFTP

O exemplo a seguir mostra um evento em que um download falhou em um servidor SFTP (Amazon EFS é o armazenamento que está sendo usado).

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Download Failed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2024-01-29T17:20:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "failure-code": "PARTIAL_DOWNLOAD",
    "status-code": "FAILED",
    "protocol": "SFTP",
    "bytes": 4100,
    "client-ip": "IP-address",
    "failure-message": "File was partially downloaded.",
    "end-timestamp": "2024-01-29T17:20:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2024-01-29T17:20:16.706282454Z"
  }
}
```

Example Exemplo de evento concluído para upload de arquivo do servidor FTP

O exemplo a seguir mostra um evento em que um upload foi concluído com êxito em um servidor FTP (Amazon S3 é o armazenamento que está sendo usado).

```
{
```

```

    "version": "0",
    "id": "event-ID",
    "detail-type": "FTP Server File Upload Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2024-01-29T16:31:43Z",
    "region": "us-east-1",
    "resources": [
      "arn:aws:transfer:us-east-1:958412138249:server/s-1111aaaa2222bbbb3"
    ],
    "detail": {
      "status-code": "COMPLETED",
      "protocol": "FTP",
      "bytes": 1048576,
      "client-ip": "10.0.0.141",
      "end-timestamp": "2024-01-29T16:31:43.311866408Z",
      "etag": "b6d81b360a5672d80c27430f39153e2c",
      "file-path": "/amzn-s3-demo-bucket/test/1mb_file",
      "server-id": "s-1111aaaa2222bbbb3",
      "username": "test",
      "session-id": "event-ID",
      "start-timestamp": "2024-01-29T16:31:42.462088327Z"
    }
  }
}

```

Example Exemplo de evento concluído para exclusão de arquivo do servidor SFTP

O exemplo a seguir mostra um evento em que um arquivo foi excluído com êxito em um servidor SFTP.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Delete Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T14:30:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",

```

```

    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T14:30:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file-to-delete.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T14:30:26.706282454Z"
  }
}

```

Example Exemplo de evento concluído com renomeação de arquivo do servidor SFTP

O exemplo a seguir mostra um evento em que um arquivo foi renomeado com êxito em um servidor SFTP.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Rename Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T15:45:12Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T15:45:12.749749117Z",
    "original-file-path": "/fs-1234abcd5678efghi/user0/old-filename.txt",
    "renamed-file-path": "/fs-1234abcd5678efghi/user0/new-filename.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T15:45:11.706282454Z"
  }
}

```

Exemplo Evento de exemplo concluído do SFTP Server Directory Create

O exemplo a seguir mostra um evento em que um diretório foi criado com sucesso em um servidor SFTP.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server Directory Create Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T16:20:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T16:20:05.749749117Z",
    "directory-path": "/fs-1234abcd5678efghi/user0/new-directory",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T16:20:04.706282454Z"
  }
}
```

Eventos do conector SFTP

Note

Esses eventos são entregues EventBridge em um nível durável, conforme descrito em [Nível de entrega para eventos AWS de serviço](#) na Referência de EventBridge Eventos da Amazon.

A seguir estão os campos de detalhes dos eventos do conector SFTP:

- Envio do arquivo do conector SFTP concluído
- Falha no envio do arquivo do conector SFTP

- Recuperação do arquivo do conector SFTP concluída
- Falha na recuperação do arquivo do conector SFTP
- Lista de diretórios de conectores SFTP concluída
- Falha na listagem do diretório do conector SFTP
- Movimentação remota do conector SFTP concluída
- Falha na movimentação remota do conector SFTP
- Exclusão remota do conector SFTP concluída
- Falha na exclusão remota do conector SFTP

Os `detail-type` campos `source` e estão incluídos abaixo porque contêm valores específicos para Transfer Family eventos. Para obter as definições dos outros campos de metadados incluídos em todos os eventos, consulte [Referência de estrutura de eventos](#) no Guia do Amazon EventBridge usuário.

```
{
  . . .,
  "detail-type": "string",
  "source": "aws.transfer",
  . . .,
  "detail": {
    "operation" : "string",
    "max-items" : "number",
    "connector-id" : "string",
    "output-directory-path" : "string",
    "listing-id" : "string",
    "transfer-id" : "string",
    "file-transfer-id" : "string",
    "url" : "string",
    "file-path" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "local-directory-path" : "string",
    "remote-directory-path" : "string",
    "item-count" : "number",
    "truncated" : "boolean",
    "bytes" : "number",
```

```

    "egress-type" : "string",
    "vpc-lattice-resource-configuration-arn" : "string",
    "vpc-lattice-port-number" : "number",
    "local-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    },
    "output-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    }
  }
}

```

detail-type

Identifica o tipo de evento.

Para esse evento, o valor é um dos nomes de eventos do conector SFTP listados anteriormente.

source

Identifica o serviço que gerou o evento. Para Transfer Family eventos, esse valor é `aws.transfer`.

detail

Um objeto JSON contém informações sobre o evento. O serviço que gera o evento determina o conteúdo desse campo.

Para esse evento, os dados incluem o seguinte:

max-items

O número máximo de directory/file nomes a serem retornados.

operation

Se a `StartFileTransfer` solicitação está enviando ou recuperando um arquivo.

Valores: `SEND` | `RETRIEVE`.

connector-id

O identificador exclusivo do conector SFTP que está sendo usado.

output-directory-path

O caminho (bucket e prefixo) no Amazon S3 para armazenar os resultados da file/directory listagem.

listing-id

Um identificador exclusivo para a operação StartDirectoryListing da API. Esse identificador pode ser usado para verificar CloudWatch os registros e ver o status da solicitação de listagem.

transfer-id

O identificador exclusivo do evento de transferência (uma StartFileTransfer solicitação).

file-transfer-id

O identificador exclusivo do arquivo que está sendo transferido.

url

O URL do endpoint SFTP ou AS2 do parceiro.

file-path

O local e o arquivo que estão sendo enviados ou recuperados.

status-code

Se a transferência foi bem-sucedida. Valores: FAILED | COMPLETED.

failure-code

Para transferências com falha, o código do motivo pelo qual a transferência falhou. Valores: ASSUME_ROLE_ERROR | UNSUPPORTED_OPERATION_ERROR | CONNECTION_ERROR | READ_FILE_ERROR | WRITE_FILE_ERROR | TIMEOUT_ERROR | LIST_DIRECTORY_ERROR | SEND_FILE_NOT_FOUND | RETRIEVE_FILE_NOT_FOUND | DIRECTORY_NOT_FOUND | FILE_NOT_FOUND | PATH_NOT_FOUND | RENAME_ERROR | DELETE_ERROR | INTERNAL_ERROR | UNKNOWN_ERROR.

failure-message

Para transferências malsucedidas, os detalhes do motivo pelo qual a transferência falhou.

start-timestamp

Para transferências bem-sucedidas, a data e hora de início do processamento do arquivo.

end-timestamp

Para transferências bem-sucedidas, o registro de data e hora de conclusão do processamento do arquivo.

local-directory-path

Para RETRIEVE solicitações, o local no qual colocar o arquivo recuperado.

remote-directory-path

Para SEND solicitações, o diretório de arquivos no qual colocar o arquivo no servidor SFTP do parceiro. Esse é o valor do RemoteDirectoryPath que o usuário passou para a StartFileTransfer solicitação. Você pode especificar um diretório padrão no servidor SFTP do parceiro. Nesse caso, esse campo está vazio.

item-count

O número de itens (diretórios e arquivos) retornados para a solicitação de listagem.

truncated

Se a saída da lista contém todos os itens contidos no diretório remoto ou não.

bytes

O número de bytes que estão sendo transferidos. O valor é 0 para transferências malsucedidas.

egress-type

Tipo de configuração de saída para o conector. Valores: SERVICE_MANAGED ou VPC_LATTICE.

vpc-lattice-resource-configuration-arn

ARN da configuração de recursos VPC_LATTICE que define a localização do servidor SFTP de destino. Esse campo é nulo para conectores gerenciados por serviços.

vpc-lattice-port-number

Número da porta para conexão com o servidor SFTP por meio de VPC_LATTICE.

local-file-location

Esse parâmetro contém os detalhes da localização do arquivo AWS de armazenamento.

`domain`

O armazenamento que está sendo usado. Atualmente, o único valor é S3.

`bucket`

O contêiner do objeto no Amazon S3.

`key`

O nome atribuído ao objeto no Amazon S3.

`output-file-location`

Esse parâmetro contém os detalhes do local onde armazenar os resultados da listagem de diretórios no AWS armazenamento.

`domain`

O armazenamento que está sendo usado. Atualmente, o único valor é S3.

`bucket`

O contêiner do objeto no Amazon S3.

`key`

O nome atribuído ao objeto no Amazon S3.

Example Exemplo de evento de falha no envio do arquivo do conector SFTP

O exemplo a seguir mostra um evento em que um conector SFTP falhou ao tentar enviar um arquivo para um servidor SFTP remoto.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector File Send Failed",
  "source": "aws.transfer",
  "account": "123456789012",
  "time": "2024-01-24T19:30:45Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
  ],
  "detail": {
    "operation": "SEND",
```

```

    "connector-id": "c-f1111aaaa2222bbbb3",
    "transfer-id": "transfer-ID",
    "file-transfer-id": "file-transfer-ID",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/amzn-s3-demo-bucket/testfile.txt",
    "status-code": "FAILED",
    "failure-code": "CONNECTION_ERROR",
    "failure-message": "Unknown Host",
    "remote-directory-path": "",
    "bytes": 0,
    "start-timestamp": "2024-01-24T18:29:33.658729Z",
    "end-timestamp": "2024-01-24T18:29:33.993196Z",
    "local-file-location": {
      "domain": "S3",
      "bucket": "amzn-s3-demo-bucket",
      "key": "testfile.txt"
    }
  }
}

```

Example Exemplo de evento concluído do SFTP Connector File Retrieve

O exemplo a seguir mostra um evento em que um conector SFTP recuperou com êxito um arquivo enviado de um servidor SFTP remoto.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector File Retrieve Completed",
  "source": "aws.transfer",
  "account": "123456789012",
  "time": "2024-01-24T18:28:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
  ],
  "detail": {
    "operation": "RETRIEVE",
    "connector-id": "c-fc68000012345aa18",
    "transfer-id": "file-transfer-ID",
    "file-transfer-id": "file-transfer-ID",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
    "file-path": "testfile.txt",

```

```

    "status-code": "COMPLETED",
    "local-directory-path": "/amzn-s3-demo-bucket",
    "bytes": 63533,
    "start-timestamp": "2024-01-24T18:28:07.632388Z",
    "end-timestamp": "2024-01-24T18:28:07.774898Z",
    "local-file-location": {
      "domain": "S3",
      "bucket": "amzn-s3-demo-bucket",
      "key": "testfile.txt"
    }
  }
}

```

Example Exemplo concluído de listagem de diretórios de conectores SFTP

O exemplo a seguir mostra um evento em que uma chamada de listagem de diretórios inicial recuperou um arquivo de listagem de um servidor SFTP remoto.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector Directory Listing Completed",
  "source": "aws.transfer",
  "account": "123456789012",
  "time": "2024-01-24T18:28:08Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
  ],
  "detail": {
    "max-items": 10000,
    "connector-id": "c-fc68000012345aa18",
    "output-directory-path": "/amzn-s3-demo-bucket/example/file-listing-output",
    "listing-id": "123456-23aa-7980-abc1-1a2b3c4d5e",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",

    "status-code": "COMPLETED",
    "remote-directory-path": "/home",
    "item-count": 10000,
    "truncated": true,
    "start-timestamp": "2024-01-24T18:28:07.632388Z",
    "end-timestamp": "2024-01-24T18:28:07.774898Z",
    "output-file-location": {

```

```

        "domain": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
    }
}

```

Eventos AS2

Note

Esses eventos são entregues EventBridge em um nível durável, conforme descrito em [Nível de entrega para eventos AWS de serviço](#) na Referência de EventBridge Eventos da Amazon.

A seguir estão os campos de detalhes dos eventos AS2:

- Recebimento do AS2 Payload concluído
- Falha no recebimento da carga útil do AS2
- Envio do AS2 Payload concluído
- Falha no envio da carga útil do AS2
- Recebimento AS2 MDN concluído
- Falha na recepção do AS2 MDN
- Envio AS2 MDN concluído
- Falha no envio do AS2 MDN

Os `detail-type` campos `source` e estão incluídos abaixo porque contêm valores específicos para Transfer Family eventos. Para obter as definições dos outros campos de metadados incluídos em todos os eventos, consulte [Referência de estrutura de eventos](#) no Guia do Amazon EventBridge usuário.

```

{
    . . . ,
    "detail-type": "string",
    "source": "aws.transfer",
    . . . ,
    "detail": {

```



```

    "s3-attributes" : {
      "file-bucket" : "string",
      "file-key" : "string",
      "json-bucket" : "string",
      "json-key" : "string",
      "mdn-bucket" : "string",
      "mdn-key" : "string"
    }
    "mdn-subject" : "string",
    "mdn-message-id" : "string",
    "disposition" : "string",
    "bytes" : "number",
    "as2-from" : "string",
    "as2-message-id" : "string",
    "as2-to" : "string",
    "connector-id" : "string",
    "client-ip" : "string",
    "agreement-id" : "string",
    "server-id" : "string",
    "requester-file-name" : "string",
    "message-subject" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "transfer-id" : "string"
  }
}

```

detail-type

Identifica o tipo de evento.

Para esse evento, o valor é um dos eventos AS2 listados anteriormente.

source

Identifica o serviço que gerou o evento. Para Transfer Family eventos, esse valor é `aws.transfer`.

detail

Um objeto JSON contém informações sobre o evento. O serviço que gera o evento determina o conteúdo desse campo.

s3-attributes

Identifica o bucket e a chave do Amazon S3 para o arquivo que está sendo transferido. Para eventos MDN, ele também identifica o bucket e a chave do arquivo MDN.

file-bucket

O contêiner do objeto no Amazon S3.

file-key

O nome atribuído ao objeto no Amazon S3.

json-bucket

Para transferências CONCLUÍDAS ou COM FALHA, o contêiner do arquivo JSON.

json-key

Para transferências CONCLUÍDAS ou FALHADAS, o nome atribuído ao arquivo JSON no Amazon S3.

mdn-bucket

Para eventos MDN, o contêiner do arquivo MDN.

mdn-key

Para eventos MDN, o nome atribuído ao arquivo MDN no Amazon S3.

mdn-subject

Para eventos MDN, uma descrição em texto para a disposição da mensagem.

mdn-message-id

Para eventos do MDN, um ID exclusivo para a mensagem do MDN.

disposition

Para eventos da MDN, a categoria para a disposição.

bytes

O número de bytes na mensagem.

as2-from

O parceiro comercial da AS2 que está enviando a mensagem.

`as2-message-id`

Um identificador exclusivo para a mensagem AS2 que está sendo transferida.

`as2-to`

O parceiro comercial da AS2 que está recebendo a mensagem.

`connector-id`

Para mensagens AS2 enviadas de um servidor Transfer Family para um parceiro comercial, o identificador exclusivo do conector AS2 está sendo usado.

`client-ip`

Para eventos de servidor (transferências de um parceiro comercial para um servidor Transfer Family), o endereço IP do cliente envolvido na transferência.

`agreement-id`

Para eventos de servidor, o identificador exclusivo do contrato AS2.

`server-id`

Para eventos de servidor, uma ID exclusiva somente para o servidor Transfer Family.

`requester-file-name`

Para eventos de carga, o nome original do arquivo recebido durante a transferência.

`message-subject`

Uma descrição em texto para o assunto da mensagem.

`start-timestamp`

Para transferências bem-sucedidas, a data e hora de início do processamento do arquivo.

`end-timestamp`

Para transferências bem-sucedidas, o registro de data e hora de conclusão do processamento do arquivo.

`status-code`

O código que corresponde ao estado do processo de transferência de mensagens AS2.

Valores válidos: COMPLETED | FAILED | PROCESSING.

failure-code

Para transferências malsucedidas, a categoria do motivo pelo qual a transferência falhou.

failure-message

Para transferências malsucedidas, os detalhes do motivo pelo qual a transferência falhou.

transfer-id

O identificador exclusivo do evento de transferência.

Example Exemplo de evento concluído do AS2 Payload Receive

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 Payload Receive Completed",
  "source": "aws.transfer",
  "account": "076722215406",
  "time": "2024-02-07T06:47:05Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:connector/c-1111aaaa2222bbbb3"],
  "detail": {
    "s3-attributes": {
      "file-key": "/inbound/processed/testAs2Message.dat",
      "file-bucket": "amzn-s3-demo-bucket"
    },
    "client-ip": "client-IP-address",
    "requester-file-name": "testAs2MessageVerifyFile.dat",
    "end-timestamp": "2024-02-07T06:47:06.040031Z",
    "as2-from": "as2-from-ID",
    "as2-message-id": "as2-message-ID",
    "message-subject": "Message from AS2 tests",
    "start-timestamp": "2024-02-07T06:47:05.410Z",
    "status-code": "PROCESSING",
    "bytes": 63,
    "as2-to": "as2-to-ID",
    "agreement-id": "a-1111aaaa2222bbbb3",
    "server-id": "s-1234abcd5678efghi"
  }
}
```

Example Exemplo de evento de falha no recebimento do AS2 MDN

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 MDN Receive Failed",
  "source": "aws.transfer",
  "account": "889901007463",
  "time": "2024-02-06T22:05:09Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:server/s-1111aaaa2222bbbb3"],
  "detail": {
    "mdn-subject": "Your Requested MDN Response re: Test run from Id 123456789abcde
to partner ijklmnop987654",
    "s3-attributes": {
      "json-bucket": "amzn-s3-demo-bucket1",
      "file-key": "/as2Integ/TestOutboundWrongCert.dat",
      "file-bucket": "amzn-s3-demo-bucket2",
      "json-key": "/as2Integ/failed/TestOutboundWrongCert.dat.json"
    },
    "mdn-message-id": "MDN-message-ID",
    "end-timestamp": "2024-02-06T22:05:09.479878Z",
    "as2-from": "PartnerA",
    "as2-message-id": "as2-message-ID",
    "connector-id": "c-1234abcd5678efghj",
    "message-subject": "Test run from Id 123456789abcde to partner ijklmnop987654",
    "start-timestamp": "2024-02-06T22:05:03Z",
    "failure-code": "VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND",
    "status-code": "FAILED",
    "as2-to": "MyCompany",
    "failure-message": "No public certificate matching message signature could be
found in profile: p-1234abcd5678efghj",
    "transfer-id": "transfer-ID"
  }
}
```

Segurança em AWS Transfer Family

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isto como segurança da nuvem e segurança na nuvem.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade](#) [Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#) .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a [documentação AWS de segurança](#).

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Transfer Family. Os tópicos a seguir mostram como configurar para atender AWS Transfer Family aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS Transfer Family recursos.

Oferecemos um workshop que fornece orientação prescritiva e um laboratório prático sobre como você pode criar uma arquitetura de transferência de arquivos escalável e segura AWS sem precisar modificar os aplicativos existentes ou gerenciar a infraestrutura do servidor. É possível ver os detalhes desse workshop [aqui](#).

Tópicos

- [Benefícios da segurança da conectividade VPC](#)
- [Políticas de segurança para AWS Transfer Family servidores](#)
- [Políticas de segurança para AWS Transfer Family Conectores SFTP](#)

- [Usando a troca híbrida de chaves pós-quânticas com AWS Transfer Family](#)
- [Proteção e criptografia de dados](#)
- [Gerenciando chaves SSH e PGP no Transfer Family](#)
- [Gerenciamento de identidade e acesso para AWS Transfer Family](#)
- [Validação de conformidade AWS Transfer Family](#)
- [Resiliência em AWS Transfer Family](#)
- [Crie uma conexão privada entre uma VPC e AWS Transfer Family APIs](#)
- [Segurança da infraestrutura em AWS Transfer Family](#)
- [Adicione um firewall da aplicação web](#)
- [Cross-service prevenção delegada confusa](#)
- [AWS políticas gerenciadas para AWS Transfer Family](#)

Benefícios da segurança da conectividade VPC

Os conectores SFTP com tipo de saída VPC oferecem benefícios aprimorados de segurança por meio do acesso a recursos: Cross-VPC

- Isolamento de rede: todo o tráfego permanece em seu ambiente de VPC, fornecendo isolamento completo da rede da Internet pública para conexões de endpoint privadas.
- Controle de IP de origem: os servidores SFTP remotos só veem endereços IP do intervalo CIDR da VPC, oferecendo controle total sobre os endereços IP de origem usados nas conexões.
- Acesso privado ao endpoint: conecte-se diretamente aos servidores SFTP em sua VPC usando endereços IP privados, eliminando a exposição à Internet pública.
- Conectividade híbrida: acesse com segurança servidores SFTP locais por meio de conexões VPN ou Direct Connect estabelecidas sem exposição adicional à Internet.
- Controles de segurança da VPC: aproveite os grupos de segurança, NACLs e políticas de roteamento existentes da VPC para controlar e monitorar o tráfego do conector SFTP.

Modelo de segurança VPC Lattice

A conectividade VPC para conectores SFTP usa o AWS VPC Lattice com redes de serviços para fornecer acesso seguro para vários locatários:

- **Prevenção delegada confusa:** as verificações de autenticação e autorização garantem que os conectores só possam acessar os recursos específicos para os quais estão configurados, impedindo o acesso não autorizado entre inquilinos.
- **IPv6-only rede de serviços:** usa endereçamento IPv6 para evitar possíveis conflitos de endereços IP e aprimorar o isolamento de segurança.
- **Sessão de acesso direto (FAS):** o tratamento temporário de credenciais elimina a necessidade de armazenamento de credenciais de longo prazo ou compartilhamento manual de recursos.
- **Resource-level controle de acesso:** cada conector está associado a uma configuração de recursos específica, garantindo controle de acesso granular a servidores SFTP individuais.

Práticas recomendadas de segurança para conectividade VPC

Ao usar conectores do tipo de saída VPC, siga estas práticas recomendadas de segurança:

- **Grupos de segurança:** configure grupos de segurança para permitir o tráfego SFTP (porta 22) somente entre os recursos necessários. Restrinja os intervalos de IP de origem e destino ao mínimo necessário.
- **Posicionamento do Resource Gateways:** implante gateways de recursos em sub-redes privadas sempre que possível e garanta que eles abranjam pelo menos duas zonas de disponibilidade para alta disponibilidade.
- **Monitoramento de rede:** use o VPC Flow Logs e CloudWatch a Amazon para monitorar padrões de tráfego de rede e detectar atividades anômalas.
- **Registro de acesso:** habilite o registro de conectores para rastrear atividades de transferência de arquivos e manter trilhas de auditoria para requisitos de conformidade.
- **Gerenciamento de configuração de recursos:** revise e atualize regularmente as configurações de recursos para garantir que elas apontem para os servidores SFTP corretos e usem as configurações de rede apropriadas.

Políticas de segurança para AWS Transfer Family servidores

As políticas de segurança do servidor AWS Transfer Family permitem que você limite o conjunto de algoritmos criptográficos (códigos de autenticação de mensagens (MACs), trocas de chaves (KEXs), conjuntos de cifras, cifras de criptografia de conteúdo e algoritmos de hash) associados ao seu servidor.

AWS Transfer Family suporta políticas de segurança pós-quântica que usam algoritmos híbridos de troca de chaves, combinando métodos criptográficos tradicionais com algoritmos pós-quânticos para fornecer segurança aprimorada contra futuras ameaças da computação quântica. Para obter mais informações, consulte [Usando a troca híbrida de chaves pós-quânticas com AWS Transfer Family](#).

Para ver uma lista dos algoritmos de chave suportados, consulte [Algoritmos criptográficos](#). Para obter uma lista de algoritmos de chave compatíveis para uso com chaves de host de servidor e chaves de usuário gerenciadas por serviços, consulte [Gerenciando chaves SSH e PGP no Transfer Family](#).

 Note

A partir de 2025, todas as novas políticas AWS Transfer Family de segurança incluem suporte criptográfico pós-quântico usando algoritmos híbridos de troca de chaves. Para obter mais informações sobre segurança pós-quântica, consulte [Usando a troca híbrida de chaves pós-quânticas com AWS Transfer Family](#).

 Note

É altamente recomendável atualizar seus servidores de acordo com nossa política de segurança mais recente.

- `TransferSecurityPolicy-2024-01` é a política de segurança padrão anexada ao seu servidor ao criar um servidor usando o console, a API ou a CLI.
- Se você criar um servidor Transfer Family usando CloudFormation e aceitar a política de segurança padrão, o servidor será atribuído `TransferSecurityPolicy-2018-11`.

Se você estiver preocupado com a compatibilidade do cliente, indique afirmativamente qual política de segurança você deseja usar ao criar ou atualizar um servidor, em vez de usar a política padrão, que está sujeita a alterações. Para alterar a política de segurança de um servidor, consulte [Edite a política de segurança](#).

 Note

As políticas pós-quânticas anteriores (TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 e TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04) estão obsoletas. Em vez disso, recomendamos que você use as novas políticas.

Para obter mais informações sobre segurança no Transfer Family, consulte as seguintes postagens no blog:

- [Seis dicas para melhorar a segurança do seu AWS Transfer Family servidor](#)
- [Como a Transfer Family pode ajudar você a criar uma solução de transferência gerenciada de arquivos segura e compatível](#)

Tópicos

- [Algoritmos criptográficos](#)
- [Detalhes da política de segurança](#)

Algoritmos criptográficos

Para chaves de host, oferecemos suporte aos seguintes algoritmos:

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`
- `ssh-ed25519`

Além disso, as seguintes políticas de segurança permitem `ssh-rsa`:

- `TransferSecurityPolicy-2018-11`
- `TransferSecurityPolicy-2020-06`
- `TransferSecurityPolicy-FIPS-2020-06`

- TransferSecurityPolicy-FIPS-2023-05
- TransferSecurityPolicy-FIPS-2024-01

 Note

É importante entender a distinção entre o tipo de chave RSA, que é sempre, `ssh-rsa` e o algoritmo de chave de host RSA, que pode ser qualquer um dos algoritmos compatíveis.

Veja a seguir uma lista dos algoritmos criptográficos compatíveis com cada política de segurança.

 Note

Na tabela e nas políticas a seguir, observe o seguinte uso dos tipos de algoritmo.

- Os servidores SFTP usam apenas algoritmos nas `SshMac`seções `SshCiphers``SshKex`s, e.
- Os servidores FTPS usam apenas algoritmos na `TlsCipher`seção.
- Os servidores FTP, como não usam criptografia, não usam nenhum desses algoritmos.
- Os servidores AS2 usam apenas algoritmos nas `HashAlgorithms`seções `ContentEncryptionCipher`s. Essas seções definem algoritmos usados para criptografar e assinar o conteúdo do arquivo.
- As políticas FIPS-2024-01 de segurança FIPS-2024-05 e são idênticas, exceto que FIPS-2024-05 não suportam o `ssh-rsa` algoritmo.
- A Transfer Family introduziu novas políticas restritas que são muito paralelas às políticas existentes:
 - As políticas `TransferSecurityPolicy-2018-11` de segurança `TransferSecurityPolicy-Restricted-2018-11` e são idênticas, exceto que a política restrita não suporta a `chacha20-poly1305@openssh.com` cifra.
 - As políticas `TransferSecurityPolicy-2020-06` de segurança `TransferSecurityPolicy-Restricted-2020-06` e são idênticas, exceto que a política restrita não suporta a `chacha20-poly1305@openssh.com` cifra.

* Na tabela a seguir, a `chacha20-poly1305@openssh.com` cifra está incluída somente na política não restrita,

Política de segurança	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-03
		FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06	FIPS	-11
		-2025-03	ditCom	stricted		-2024-01/		-2023-05		and	-2020-06	and
			iant-2025-02	2025-07		TransferSecurityPolicy-2024-05				TransferSecurityPolicy-2020-06		TransferSecurityPolicy-2018-11
SshCiphers												
aes128-ctr	◆	◆	◆	◆	◆					◆	◆	◆
aes128-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes192-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
chacha20-poly1305@openssh.com										◆*		◆*

Política de segurança	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03	TransferSecurity-2025-03
	FIPS	SshA	AS2R	01	FIPS	05	FIPS	03	06	FIPS	11		
	-2025-08	ditCom	restricted		-2024-01/		-2023-05		and	-2020-06	and		
		iant-2025-02	2025-07		TransferS				TransferS		TransferS		
					ecurityPo				ecurityPo		ecurityPo		
					licy-				licy-		licy-		
					FIPS				Rest		Rest		
					-2024-05				stricted-20		stricted-20		
									20-06		18-11		

SshKexs

	mlkem768x	mlkem768n	mlkem1024	curve25519-sha256	curve25519-sha256@libssh.org
mlkem768x	◆	◆			
mlkem768n	◆	◆			
mlkem1024	◆	◆			
curve25519-sha256				◆	◆
curve25519-sha256@libssh.org				◆	◆

Política de segurança	TransferSecurity-2025-03	TransferSecurity-2025-08	TransferSecurity-2025-08	TransferSecurity-2025-07	TransferSecurity-2024-01	TransferSecurity-2024-05	TransferSecurity-2023-05	TransferSecurity-2023-03	TransferSecurity-2023-06	TransferSecurity-2020-06	TransferSecurity-2018-11	TransferSecurity-2018-11
		FIPS	SshA	AS2R		FIPS		FIPS			FIPS	
		-2025-08	ditComes	stricted		-2024-01/		-2023-05		-06	-2020-06	
			iant-2025-02	2025-07		TransferS				TransferS		TransferS
						ecurityPo				ecurityPo		ecurityPo
						licy-				licy-		licy-
						FIPS				Rest		Rest
						-2024-05				ricted-20		ricted-20
										20-06		18-11
diffie-he llman- gro up14- sha1												◆
diffie-he llman- gro up14- sha2 56									◆	◆	◆	
diffie-he llman- gro up16- sha5 12	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Política de segurança	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA-2025-08	TransferSecurityPolicy-AS2R-2025-07	TransferSecurityPolicy-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-05	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-03	TransferSecurityPolicy-06 and 20-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-11 and 18-11
diffie-he llman-gro up18-sha5 12	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
diffie-he llman-gro up-exchan ge-sha256	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆
ecdh-sha2 -nistp256	◆	◆		◆	◆	◆				◆	◆	◆

Política de segurança	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-2024-05	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2023-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Restricted-2025-07			TransferSecurityPolicy-FIPS-2024-05				TransferSecurityPolicy-FIPS-Restricted-2020-06		TransferSecurityPolicy-FIPS-Restricted-2018-11
ecdh-sha2-nistp384	◆	◆	◆	◆	◆					◆	◆	◆
ecdh-sha2-nistp521	◆	◆	◆	◆	◆					◆	◆	◆
SshMacs												
hmac-sha1												◆
hmac-sha1-etm@openssh.com												◆
hmac-sha2-256								◆	◆	◆	◆	◆

Política de segurança	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA-2025-08	TransferSecurityPolicy-AS2R-2025-07	TransferSecurityPolicy-01-2025-07	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-05-2024-01	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-03-2023-05	TransferSecurityPolicy-06-2020-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-11-2018-11
hmac-sha2-256-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
hmac-sha2-512									◆	◆	◆	◆
hmac-sha2-512-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
umac-128-etm@openssh.com										◆		◆
umac-128-etm@openssh.com										◆		◆

Política de segurança	TransferSecurity-2025-03	TransferSecurity-2025-08	TransferSecurity-2025-08	TransferSecurity-2025-07	TransferSecurity-2025-07	TransferSecurity-2024-01	TransferSecurity-2024-05	TransferSecurity-2023-05	TransferSecurity-2023-06	TransferSecurity-2020-06	TransferSecurity-2018-11
		FIPS	SshA	AS2R	-01	FIPS	-05	FIPS	-03	-06 and	FIPS -11 and
		-2025-08	ditComes	stricted		-2024-01/		-2023-05		TransferS	TransferS
			iant-2025-02	2025-07		TransferS				ecurityPo	ecurityPo
						ecurityPo				ecurityPo	ecurityPo
						licy-				licy-	licy-
						FIPS				Rest	Rest
						-2024-05				ricted-20	ricted-20
										20-06	18-11
umac-64-											◆
e											
tm@openss											
h.com											
umac-64@o											◆
penssh.co											
m											
ContentEncryptionCiphers											
aes256-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes192-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes128-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
3des-cbc	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆
HashAlgorithms											
sha256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Política de segurança	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01/FIPS	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2022-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Compliant-2025-07			TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
sha384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha512	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha1	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆
TlsCiphers											
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Política de segurança	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-11	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Compliant-2025-07			TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-11	
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Política de segurança	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-2025-09	TransferSecurityPolicy-2025-07	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2022-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
		FIPS	SshA	AS2R		FIPS	FIPS			FIPS	
		-2025-08	ditCom	stricted		-2024-01/	-2023-05		-06	-2020-06	
			iant-2025-02	2025-07		TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_RSA_WITH_AES_128_CBC_SHA256										◆	
TLS_RSA_WITH_AES_128_CBC_SHA256										◆	

Detalhes da política de segurança

As seções a seguir contêm a representação JSON de cada política de segurança.

TransferSecurityPolicy-2025-03

O seguinte mostra a política TransferSecurityPolicy-2025-03 de segurança.

```
{
  "SecurityPolicy": {
```

```
"Fips": false,
"SecurityPolicyName": "TransferSecurityPolicy-2025-03",
"SshCiphers": [
    "aes256-gcm@openssh.com",
    "aes128-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
],
"SshKexs": [
    "mlkem768x25519-sha256",
    "mlkem768nistp256-sha256",
    "mlkem1024nistp384-sha384",
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group-exchange-sha256"
],
"SshMacs": [
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com"
],
"ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
],
"HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
],
"TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
```

```

        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-FIPS-2025-03

O seguinte mostra a política TransferSecurityPolicy-FIPS-2025-03 de segurança.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2025-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr",
      "aes128-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [

```

```

        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}

```

TransferSecurityPolicy-AS2Restricted-2025-07

Essa política de segurança foi projetada para transferências de arquivos AS2 que exigem segurança aprimorada, excluindo algoritmos criptográficos legados. Ele oferece suporte a algoritmos de SHA-2 hash e criptografia AES modernos, ao mesmo tempo em que remove o suporte para algoritmos mais fracos, como 3DES e SHA-1

Note

Essa política de segurança é idêntica TransferSecurityPolicy-2025-03, exceto que ela não oferece suporte a 3DES (in ContentEncryptionCiphers) e não oferece suporte a SHA1 (in

HashAlgorithms). Inclui todos os algoritmos de 2025-03, incluindo algoritmos criptográficos pós-quânticos (mlkem* KEXs).

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-AS2Restricted-2025-07",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512"
    ],
    "TlsCiphers": [
```

```

        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-SshAuditCompliant-2025-02

O seguinte mostra a política TransferSecurityPolicy-SshAuditCompliant-2025-02 de segurança.

Note

Essa política de segurança foi projetada com base nas recomendações fornecidas pela ssh-audit ferramenta e é 100% compatível com essa ferramenta.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "Protocols": [
      "SFTP",
      "FTPS"
    ],
    "SecurityPolicyName": "TransferSecurityPolicy-SshAuditCompliant-2025-02",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
  },
}

```

```

    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER"
  }
}

```

TransferSecurityPolicy-2024-01

O seguinte mostra a política TransferSecurityPolicy-2024-01 de segurança.

```

{
  "SecurityPolicy": {

```

```
"Fips": false,
"SecurityPolicyName": "TransferSecurityPolicy-2024-01",
"SshCiphers": [
    "aes128-gcm@openssh.com",
    "aes256-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
],
"SshKexs": [
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group-exchange-sha256"
],
"SshMacs": [
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com"
],
"ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
],
"HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
],
"TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
```

```
    ]
  }
}
```

TransferSecurityPolicy-FIPS-2024-01/TransferSecurityPolicy-FIPS-2024-05

A seguir, mostramos as políticas TransferSecurityPolicy-FIPS-2024-05 de segurança TransferSecurityPolicy-FIPS-2024-01 e.

Note

O endpoint TransferSecurityPolicy-FIPS-2024-01 e as políticas de TransferSecurityPolicy-FIPS-2024-05 segurança do serviço FIPS estão disponíveis somente em algumas AWS regiões. Para obter mais informações, consulte [endpoints e cotas do AWS Transfer Family](#) na Referência geral da AWS.

A única diferença entre essas duas políticas de segurança é que elas oferecem TransferSecurityPolicy-FIPS-2024-01 suporte ao `ssh-rsa` algoritmo e TransferSecurityPolicy-FIPS-2024-05 não.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
```

```

        "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-2023-05

O seguinte mostra a política TransferSecurityPolicy-2023-05 de segurança.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2023-05",
    "SshCiphers": [
        "aes256-gcm@openssh.com",
        "aes128-gcm@openssh.com",
        "aes256-ctr",
        "aes192-ctr"
    ],
    "SshKexs": [
        "curve25519-sha256",

```

```

        "curve25519-sha256@libssh.org",
        "diffie-hellman-group16-sha512",
        "diffie-hellman-group18-sha512",
        "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
        "hmac-sha2-512-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-FIPS-2023-05

Os detalhes da certificação FIPS AWS Transfer Family podem ser encontrados em <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

O seguinte mostra a política TransferSecurityPolicy-FIPS-2023-05 de segurança.

 Note

O endpoint do serviço FIPS e a política TransferSecurityPolicy-FIPS-2023-05 de segurança só estão disponíveis em algumas AWS regiões. Para obter mais informações, consulte [endpoints e cotas do AWS Transfer Family](#) na Referência geral da AWS.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2023-05",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
```



```

        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}

```

TransferSecurityPolicy-2022-03

O seguinte mostra a política TransferSecurityPolicy-2022-03 de segurança.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2022-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [

```

```

    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-2020-06 and TransferSecurityPolicy-Restricted-2020-06

O seguinte mostra a política TransferSecurityPolicy-2020-06 de segurança.

Note

As políticas TransferSecurityPolicy-2020-06 de segurança TransferSecurityPolicy-Restricted-2020-06 e são idênticas, exceto que a política restrita não suporta a `chacha20-poly1305@openssh.com` cifra.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2020-06
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],

```

```
"SshKexs": [  
  "ecdh-sha2-nistp256",  
  "ecdh-sha2-nistp384",  
  "ecdh-sha2-nistp521",  
  "diffie-hellman-group-exchange-sha256",  
  "diffie-hellman-group16-sha512",  
  "diffie-hellman-group18-sha512",  
  "diffie-hellman-group14-sha256"  
],  
"SshMacs": [  
  "umac-128-etm@openssh.com",  
  "hmac-sha2-256-etm@openssh.com",  
  "hmac-sha2-512-etm@openssh.com",  
  "umac-128@openssh.com",  
  "hmac-sha2-256",  
  "hmac-sha2-512"  
],  
"ContentEncryptionCiphers": [  
  "aes256-cbc",  
  "aes192-cbc",  
  "aes128-cbc",  
  "3des-cbc"  
],  
"HashAlgorithms": [  
  "sha256",  
  "sha384",  
  "sha512",  
  "sha1"  
],  
"TlsCiphers": [  
  "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",  
  "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",  
  "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",  
  "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",  
  "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",  
  "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",  
  "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",  
  "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"  
]  
}  
}
```

TransferSecurityPolicy-FIPS-2020-06

Os detalhes da certificação FIPS AWS Transfer Family podem ser encontrados em <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

O seguinte mostra a política TransferSecurityPolicy-FIPS-2020-06 de segurança.

Note

O endpoint do serviço FIPS e a política TransferSecurityPolicy-FIPS-2020-06 de segurança só estão disponíveis em algumas AWS regiões. Para obter mais informações, consulte [endpoints e cotas do AWS Transfer Family](#) na Referência geral da AWS.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2020-06",
    "SshCiphers": [
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
```

```

    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-2018-11 and TransferSecurityPolicy-Restricted-2018-11

O seguinte mostra a política TransferSecurityPolicy-2018-11 de segurança.

Note

As políticas TransferSecurityPolicy-2018-11 de segurança TransferSecurityPolicy-Restricted-2018-11 e são idênticas, exceto que a política restrita não suporta a `chacha20-poly1305@openssh.com` cifra.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2018-11
      "aes128-ctr",

```

```
    "aes192-ctr",
    "aes256-ctr",
    "aes128-gcm@openssh.com",
    "aes256-gcm@openssh.com"
  ],
  "SshKexs": [
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "diffie-hellman-group-exchange-sha256",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group14-sha256",
    "diffie-hellman-group14-sha1"
  ],
  "SshMacs": [
    "umac-64-etm@openssh.com",
    "umac-128-etm@openssh.com",
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com",
    "hmac-sha1-etm@openssh.com",
    "umac-64@openssh.com",
    "umac-128@openssh.com",
    "hmac-sha2-256",
    "hmac-sha2-512",
    "hmac-sha1"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
```

```

    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
    "TLS_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_RSA_WITH_AES_256_CBC_SHA256"
  ]
}
}

```

Políticas de segurança para AWS Transfer Family Conectores SFTP

As políticas de segurança do conector SFTP AWS Transfer Family permitem que você limite o conjunto de algoritmos criptográficos (códigos de autenticação de mensagens (MACs), trocas de chaves (KEXs) e pacotes de criptografia) associados ao seu conector SFTP. A seguir está uma lista dos algoritmos criptográficos suportados para cada política de segurança do conector SFTP.

Note

`TransferSFTPConnectorSecurityPolicy-2024-03` é a política de segurança padrão aplicada aos conectores SFTP.

Você pode alterar a política de segurança do seu conector. Selecione Connectors no painel de navegação esquerdo do Transfer Family e selecione seu conector. Em seguida, selecione Editar na seção de configuração do Sftp. Na seção Opções de algoritmo criptográfico, escolha qualquer política de segurança disponível na lista suspensa no campo Política de segurança.

Algoritmos criptográficos

Para chaves de host, os conectores SFTP oferecem suporte a todos os algoritmos compatíveis com os servidores Transfer Family, exceto o ed25519:

- `rsa-sha2-256`
- `rsa-sha2-512`

- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

Além disso, oferecemos suporte para chaves de `hostssh-rsa`, mas somente para `TransferSFTPConnectorSecurityPolicy-2023-07`.

Para autenticação, os conectores SFTP oferecem suporte aos seguintes tipos de chave:

- `ssh-rsa`
- `ecdsa`

Detalhes da política de segurança do conector SFTP

A tabela a seguir mostra os algoritmos criptográficos específicos suportados por cada política de segurança do conector SFTP.

Política de segurança	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
Ciphers			
<code>aes128-ctr</code>			◆
<code>aes128-gcm@openssh.com</code>	◆	◆	◆
<code>aes192-ctr</code>		◆	◆
<code>aes256-ctr</code>		◆	◆
<code>aes256-gcm@openssh.com</code>	◆	◆	◆
Kexs			
<code>curve25519-sha256</code>		◆	◆

Política de segurança	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
curve25519-sha256@libssh.org		◆	◆
diffie-hellman-group14-sha1			◆
diffie-hellman-group16-sha512		◆	◆
diffie-hellman-group18-sha512		◆	◆
diffie-hellman-group-exchange-sha256		◆	◆
ecdh-sha2-nistp256	◆		
ecdh-sha2-nistp384	◆		
ecdh-sha2-nistp521	◆		
Macs			
hmac-sha2-512-etm@openssh.com		◆	◆
hmac-sha2-256-etm@openssh.com		◆	◆
hmac-sha2-512	◆	◆	◆
hmac-sha2-256	◆	◆	◆
hmac-sha1			◆
hmac-sha1-96			◆

Política de segurança	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
Host Key Algorithms			
rsa-sha2-256	◆	◆	◆
rsa-sha2-512	◆	◆	◆
ecdsa-sha2-nistp256	◆	◆	◆
ecdsa-sha2-nistp384		◆	◆
ecdsa-sha2-nistp521		◆	◆
ssh-rsa			◆

Usando a troca híbrida de chaves pós-quânticas com AWS Transfer Family

O Transfer Family suporta uma opção híbrida de estabelecimento de chave pós-quântica para o protocolo Secure Shell (SSH). Post-quantum o estabelecimento de chaves é necessário porque já é possível registrar o tráfego da rede e salvá-lo para ser descriptografado futuramente por um computador quântico, o que é chamado de ataque store-now-harvest-later.

Você pode usar essa opção ao se conectar ao Transfer Family para transferências seguras de arquivos para dentro e para fora do armazenamento do Amazon Simple Storage Service (Amazon S3) ou do Amazon Elastic File System (Amazon EFS). Post-quantum o estabelecimento de chaves híbridas em SSH introduz mecanismos de estabelecimento de chaves pós-quânticas, que ele usa em conjunto com algoritmos clássicos de troca de chaves. As chaves SSH criadas com pacotes de criptografia clássicos estão protegidas contra ataques de força bruta com a tecnologia atual. No entanto, não se espera que a criptografia clássica permaneça segura após o surgimento da computação quântica em grande escala no futuro.

Se sua organização depende da confidencialidade de longo prazo de dados passados por uma conexão Transfer Family, você deverá considerar um plano para migrar para criptografia pós-quântica antes que computadores quânticos de grande escala sejam disponibilizados para uso.

Para proteger os dados criptografados hoje contra possíveis ataques futuros, AWS está participando com a comunidade criptográfica no desenvolvimento de algoritmos quânticos resistentes ou pós-quânticos. Implementamos pacotes de criptografia de troca de chaves pós-quânticas híbridas no Transfer Family que combinam elementos clássicos e pós-quânticos.

Esses pacotes de criptografia híbrida estão disponíveis para uso em suas workloads de produção na maioria das Regiões AWS. No entanto, como as características de desempenho e os requisitos de largura de banda dos pacotes de criptografia híbrida são diferentes dos mecanismos clássicos de troca de chaves, recomendamos testá-los em suas conexões do Transfer Family.

Saiba mais sobre criptografia pós-quântica na postagem do blog de segurança sobre [Post-Quantumcriptografia](#).

Sumário

- [Sobre a troca de chaves híbrida pós-quântica híbrida no SSH](#)
- [Como funciona o estabelecimento de chaves híbrida pós-quântica no Transfer Family](#)
 - [Por quê? ML-KEM](#)
 - [Post-quantum troca de chaves SSH híbridas e requisitos criptográficos \(FIPS 140\)](#)
- [Testando a troca de chaves híbrida pós-quântica no Transfer Family](#)
 - [Habilite a troca de chaves híbrida pós-quântica em seu endpoint SFTP](#)
 - [Configure um cliente SFTP que ofereça suporte à troca de chaves híbrida pós-quântica](#)
 - [Confirme a troca de chaves híbrida pós-quântica no SFTP](#)

Sobre a troca de chaves híbrida pós-quântica híbrida no SSH

O Transfer Family suporta conjuntos de cifras de troca de chaves híbridas pós-quânticas, que usam o algoritmo clássico de troca de chaves [Elliptic Curve Diffie-Hellman \(ECDH\)](#) e ML-KEM. ML-KEM é um algoritmo pós-quântico de criptografia de chave pública e estabelecimento de chaves que o [Instituto Nacional de Padrões e Tecnologia \(NIST\)](#) designou como seu primeiro algoritmo padrão de acordo de chave pós-quântico.

O cliente e o servidor ainda fazem uma troca de chaves ECDH. Além disso, o servidor encapsula um segredo compartilhado pós-quântico na chave pública KEM pós-quântica do cliente, que é anunciada na mensagem de troca de chaves SSH do cliente. Essa estratégia combina a alta garantia de uma troca de chaves clássica com a segurança das trocas de chaves pós-quântica propostas, para ajudar

a garantir que os apertos de mão sejam protegidos, desde que o ECDH ou o segredo compartilhado pós-quântico não possam ser quebrados.

Como funciona o estabelecimento de chaves híbrida pós-quântica no Transfer Family

AWS anunciou recentemente o suporte para troca de chaves pós-quânticas em transferências de arquivos SFTP em. AWS Transfer Family O Transfer Family dimensiona com segurança as transferências de arquivos entre empresas para serviços de AWS armazenamento usando SFTP e outros protocolos. O SFTP é uma versão mais segura do Protocolo de Transferência de Arquivos (FTP) que é executado por SSH. O suporte a troca de chaves pós-quânticas do Transfer Family eleva o nível de segurança para transferências de dados por SFTP.

O suporte SFTP de troca de chaves híbridas pós-quânticas no Transfer Family inclui a combinação de algoritmos pós-quânticos e ML-KEM-768, com ECDH ML-KEM-1024, sobre curvas P256, P384 ou Curve25519. Os seguintes métodos de troca de chaves SSH correspondentes são especificados no rascunho de troca de [chaves SSH híbrida pós-quântica](#).

- mlkem768nistp256-sha256
- mlkem1024nistp384-sha384
- mlkem768x25519-sha256

Por quê? ML-KEM

AWS está comprometida em oferecer suporte a algoritmos padronizados e interoperáveis. ML-KEM é o único algoritmo de troca de chaves pós-quântica padronizado e aprovado pelo projeto [NIST Post-Quantum](#) Cryptography. Os órgãos de padronização já estão se ML-KEM integrando aos protocolos. AWS já é compatível com ML-KEM TLS em alguns endpoints AWS da API.

Como parte desse compromisso, AWS apresentou um rascunho de proposta ao IETF para criptografia pós-quântica que combina ML-KEM com NIST-approved curvas como P256 para SSH. Para ajudar a melhorar a segurança de nossos clientes, a AWS implementação da troca de chaves pós-quânticas em SFTP e SSH segue esse rascunho. Planejamos oferecer suporte a futuras atualizações até que nossa proposta seja adotada pelo IETF e se torne um padrão.

Os novos métodos de troca de chaves (listados na seção [Como funciona o estabelecimento de chaves híbrida pós-quântica no Transfer Family](#)) podem mudar à medida que o rascunho evolui em direção à padronização.

 Note

Post-quantum Atualmente, o suporte a algoritmos está disponível para troca de chaves híbridas pós-quânticas em TLS para AWS KMS (consulte [Usando TLS híbrido pós-quântico com AWS KMS](#)) e endpoints de API AWS Certificate Manager. AWS Secrets Manager

Post-quantum troca de chaves SSH híbridas e requisitos criptográficos (FIPS 140)

Para clientes que precisam de conformidade com FIPS, a Transfer Family fornece FIPS-approved criptografia em SSH usando a biblioteca criptográfica de código aberto com certificação AWS FIPS 140, -LC. AWS Os métodos de troca de chaves híbridas pós-quânticas suportados TransferSecurityPolicy-FIPS-2025-03 na Transfer Family são aprovados pelo FIPS de acordo com o [SP 800-56Cr2 do NIST](#) (seção 2). O Escritório Federal Alemão de Segurança da Informação ([BSI](#)) e a Agência Nacional de Segurança da Informação da França([ANSSI](#), Agence nationale de la sécurité des systèmes d'information) também recomendam esses métodos de troca de chaves híbrida pós-quântica.

Testando a troca de chaves híbrida pós-quântica no Transfer Family

Esta seção descreve as etapas que você segue para testar a troca de chaves híbrida pós-quântica.

1. [Habilite a troca de chaves híbrida pós-quântica em seu endpoint SFTP.](#)
2. Use um cliente SFTP (como [Configure um cliente SFTP que ofereça suporte à troca de chaves híbrida pós-quântica](#)) que ofereça suporte à troca de chaves híbrida pós-quântica seguindo as orientações na especificação preliminar mencionada acima.
3. Transfira um arquivo usando um servidor Transfer Family.
4. [Confirme a troca de chaves híbrida pós-quântica no SFTP.](#)

Habilite a troca de chaves híbrida pós-quântica em seu endpoint SFTP

É possível escolher a política SSH ao criar um novo endpoint de servidor SFTP no Transfer Family ou ao editar as opções do algoritmo criptográfico em um endpoint SFTP existente. O instantâneo a seguir mostra um exemplo de Console de gerenciamento da AWS onde você atualiza a política SSH.

Cryptographic algorithm options [Info](#)

Security Policy

Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 ▲

Find a security policy

TransferSecurityPolicy-2018-11
TransferSecurityPolicy-2020-06
TransferSecurityPolicy-2022-03
TransferSecurityPolicy-2023-05
TransferSecurityPolicy-2024-01
TransferSecurityPolicy-2025-03 ✓
TransferSecurityPolicy-Restricted-2018-11
TransferSecurityPolicy-Restricted-2020-06

to it. Additi

Os nomes das políticas SSH que suportam a troca de chaves pós-quânticas são e.

TransferSecurityPolicy-2025-03TransferSecurityPolicy-FIPS-2025-03 Para obter mais detalhes sobre as políticas do Transfer Family, consulte [Políticas de segurança para AWS Transfer Family servidores](#).

Configure um cliente SFTP que ofereça suporte à troca de chaves híbrida pós-quântica

Depois de selecionar a política SSH pós-quântica correta em seu endpoint do SFTP Transfer Family, é possível experimentar o SFTP pós-quântico no Transfer Family. Instale o cliente OpenSSH mais recente (como a versão 9.9) em seu sistema local para testar.

Note

Certifique-se de que seu cliente ofereça suporte a um ou mais dos ML-KEM algoritmos listados anteriormente. Você pode visualizar os algoritmos suportados para sua versão do OpenSSH executando este comando: `ssh -Q kex`

Você pode executar o cliente SFTP de exemplo para se conectar ao seu endpoint SFTP (por exemplo, `s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com`) usando os métodos de troca de chaves híbridas pós-quânticas, conforme mostrado no comando a seguir.

```
sftp -v -o \
  KexAlgorithms=mlkem768x25519-sha256 \
  -i username_private_key_PEM_file \
  username@server-id.server.transfer.region-id.amazonaws.com
```

No comando a seguir, substitua os seguintes itens por suas próprias informações:

- *username_private_key_PEM_file* Substitua pelo arquivo de chave PEM-encoded privada do usuário do SFTP
- *username* Substitua pelo nome de usuário do SFTP
- *server-id* Substitua pela ID do servidor Transfer Family
- *region-id* Substitua pela região real em que seu servidor Transfer Family está localizado

Confirme a troca de chaves híbrida pós-quântica no SFTP

Para confirmar se a troca de chaves híbrida pós-quântica foi usada durante uma conexão SSH do SFTP com o Transfer Family, verifique a saída do cliente. Opcionalmente, é possível usar um programa de captura de pacotes. Se você usa o cliente OpenSSH 9.9, a saída deve ser semelhante à seguinte (omitindo informações irrelevantes para resumir):

```
% sftp -o KexAlgorithms=mlkem768x25519-sha256 -v -o IdentitiesOnly=yes -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_9.9p2, OpenSSL 3.4.1 11 Feb 2025
debug1: Reading configuration data /Users/username/.ssh/config
debug1: /Users/username/.ssh/config line 146: Applying options for *
debug1: Reading configuration data /Users/username/.ssh/bastions-config
debug1: Reading configuration data /opt/homebrew/etc/ssh/ssh_config
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
[xxx.yyy.zzz.nnn] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_9.9
debug1: Remote protocol version 2.0, remote software version AWS_SFTP_1.1
debug1: compat_banner: no match: AWS_SFTP_1.1
```

```
debug1: Authenticating to s-1111aaaa2222bbbb3.server.transfer.us-  
west-2.amazonaws.com:22 as 'username'  
debug1: load_hostkeys: fopen /Users/username/.ssh/known_hosts2: No such file or  
directory  
[...]  
debug1: SSH2_MSG_KEXINIT sent  
debug1: SSH2_MSG_KEXINIT received  
debug1: kex: algorithm: mlkem768x25519-sha256  
debug1: kex: host key algorithm: ssh-ed25519  
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com  
compression: none  
debug1: kex: client->server cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com  
compression: none  
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY  
debug1: SSH2_MSG_KEX_ECDH_REPLY received  
debug1: Server host key: ssh-ed25519 SHA256:Ic1Ti0cdDmFdStj06rfU0cmmNccwAha/ASH2unr6zX0  
[...]  
debug1: rekey out after 4294967296 blocks  
debug1: SSH2_MSG_NEWKEYS sent  
debug1: expecting SSH2_MSG_NEWKEYS  
debug1: SSH2_MSG_NEWKEYS received  
debug1: rekey in after 4294967296 blocks  
[...]  
Authenticated to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com  
([xxx.yyy.zzz.nnn]:22) using "publickey".  
debug1: channel 0: new session [client-session] (inactive timeout: 0)  
[...]  
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.  
sftp>
```

O resultado mostra que a negociação com o cliente ocorreu usando o método `mlkem768x25519-sha256` híbrido pós-quântico e estabeleceu com sucesso uma sessão de SFTP.

Proteção e criptografia de dados

O modelo de [responsabilidade AWS compartilhada modelo](#) de se aplica à proteção de dados em AWS Transfer Family (Transfer Family). Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa toda a AWS nuvem. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos AWS serviços que você usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de](#)

[dados](#). Para obter informações sobre a proteção de dados na Europa, consulte a publicação [Modelo de Responsabilidade Compartilhada e GDPR do AWS](#) no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja as credenciais da AWS conta e configure contas de usuário individuais com Centro de Identidade do AWS 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 AWS os recursos. Oferecemos suporte ao TLS 1.2.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções AWS de criptografia, juntamente com todos os controles de segurança padrão nos AWS serviços.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS, consulte [Federal Information Processing Standard \(FIPS\) 140-2](#).

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de conta dos seus clientes, em campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Transfer Family ou outros AWS serviços usando o console, a API ou AWS os SDKs. AWS CLI Todos os dados de configuração inseridos por você na configuração do serviço Transfer Family ou em configurações de outros serviços poderão ser selecionados para inclusão em logs de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar a solicitação a esse servidor.

Por outro lado, os dados das operações de upload e download que entram e saem dos servidores do Transfer Family são tratados como totalmente privados e nunca existem fora dos canais criptografados, como uma conexão SFTP ou FTPS. Esses dados só podem ser acessados por pessoas autorizadas.

Criptografia de dados no Transfer Family

AWS Transfer Family usa as opções de criptografia padrão que você definiu para seu bucket do Amazon S3 para criptografar seus dados. Ao habilitar a criptografia em um bucket, todos os

objetos são criptografados quando armazenados no bucket. Os objetos são criptografados usando criptografia do lado do servidor com chaves gerenciadas do Amazon S3 (SSE-S3) ou () chaves gerenciadas AWS Key Management Service (AWS KMS). SSE-KMS Para obter mais informações sobre criptografia no lado do servidor, consulte [Proteger dados usando criptografia no lado do servidor](#) no Guia do usuário do Amazon Simple Storage Service.

As etapas a seguir mostram como criptografar dados em AWS Transfer Family.

Para permitir a criptografia em AWS Transfer Family

1. Habilitar a criptografia padrão para o seu bucket do Amazon S3. Para obter mais detalhes, consulte [Criptografia padrão do Amazon S3 para buckets do S3](#) no Guia do usuário do Amazon Simple Storage Service.
2. Atualize a política de função AWS Identity and Access Management (IAM) anexada ao usuário para conceder as permissões necessárias AWS Key Management Service (AWS KMS).
3. Se você estiver usando uma política de sessão para o usuário, a política de sessão deverá conceder as AWS KMS permissões necessárias.

O exemplo a seguir mostra uma política do IAM que concede as permissões mínimas necessárias ao usar AWS Transfer Family com um bucket do Amazon S3 habilitado para AWS KMS criptografia. Inclua essa política de exemplo na política de perfil do IAM do usuário e na política de restrição se estiver usando uma.

```
{
  "Sid": "Stmt1544140969635",
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:GetPublicKey",
    "kms:ListKeyPolicies"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

 Note

A ID de chave do KMS que você especificar nesta política deverá ser a mesma especificada para a criptografia padrão na etapa 1.

A raiz, ou a função do IAM usada pelo usuário, deve ser permitida na política de AWS KMS chaves. Para obter informações sobre a política de AWS KMS chaves, consulte [Usando políticas de chaves no AWS KMS](#) no Guia do AWS Key Management Service desenvolvedor.

AWS Transfer Family criptografia em repouso

Por ser AWS Transfer Family um serviço de transferência de arquivos, ele não gerencia seus dados de armazenamento em repouso. Os serviços e sistemas de armazenamento que AWS Transfer Family oferecem suporte são responsáveis por proteger os dados nesse estado. No entanto, há alguns dados relacionados ao serviço que são AWS Transfer Family gerenciados em repouso.

O que é criptografado?

Os únicos dados tratados AWS Transfer Family em repouso estão relacionados aos detalhes necessários para operar seus servidores de transferência de arquivos e processar transferências. AWS Transfer Family armazena os seguintes dados com criptografia total em repouso no Amazon DynamoDB:

- Configurações do servidor (por exemplo, configurações do servidor, configurações do protocolo e detalhes do endpoint).
- Dados de autenticação do usuário, incluindo chaves públicas SSH e metadados do usuário.
- Detalhes da execução do fluxo de trabalho e configurações de etapas.
- Configurações de conectores e credenciais de autenticação para sistemas de terceiros. Essas credenciais são criptografadas usando chaves de criptografia AWS Transfer Family gerenciadas.

Gerenciamento de chaves

Você não pode gerenciar as chaves de criptografia AWS Transfer Family usadas para armazenar informações no DynamoDB relacionadas à execução de seus servidores e ao processamento de transferências. Essas informações incluem as configurações do servidor, dados de autenticação do usuário, detalhes do fluxo de trabalho e credenciais do conector.

O que não é criptografado?

Embora AWS Transfer Family não controle como seus dados de armazenamento são criptografados em repouso, ainda recomendamos configurar seus locais de armazenamento com o mais alto nível de segurança suportado por eles. Por exemplo, você pode criptografar objetos com chaves de criptografia gerenciadas pelo Amazon S3 SSE-S3 () AWS KMS ou chaves SSE-KMS ().

Saiba mais sobre como os serviços AWS de armazenamento criptografam dados em repouso:

- [Amazon S3](#)
- [Amazon EFS](#)

Gerenciando chaves SSH e PGP no Transfer Family

Nesta seção, você encontrará informações sobre chaves SSH, incluindo como gerá-las e como rotacioná-las. Para obter detalhes sobre como usar o Transfer Family with AWS Lambda para gerenciar chaves, consulte a postagem do blog [Habilitando o gerenciamento de chaves por autoatendimento do usuário com AWS Transfer Family e AWS Lambda](#) Para implantação e gerenciamento automatizados de usuários com várias chaves SSH, consulte [Módulos Transfer Family Terraform](#).

Note

AWS Transfer Family aceita chaves RSA, ECDSA e ED25519 para autenticação SSH.

Esta seção também aborda como gerar e gerenciar chaves de Pretty Good Privacy (PGP).

Para obter uma visão geral abrangente de todos os algoritmos de criptografia e chave compatíveis, incluindo recomendações para diferentes casos de uso, consulte [Visão geral da criptografia e dos principais algoritmos](#).

Visão geral da criptografia e dos principais algoritmos

AWS Transfer Family suporta diferentes tipos de algoritmos para diferentes propósitos. Entender quais algoritmos usar para seu caso de uso específico ajuda a garantir transferências de arquivos seguras e compatíveis.

Referência rápida do algoritmo

Caso de uso	Algoritmo recomendado	Compatível com FIPS	Observações
SSH/SFTP Autenticação	RSA (rsa-sha2-256/512), ECDSA ou ED25519	RSA: Sim, ECDSA: Sim, ED25519: Não	Compatível com todos os clientes e servidores SSH
Geração de chaves PGP	RSA ou ECC (NIST)	Sim	Para decodificação do fluxo de trabalho
Criptografia de arquivos PGP	AES-256	Sim	Determinado pelo software PGP

Algoritmos de autenticação SSH

Esses algoritmos são usados para SSH/SFTP autenticação entre clientes e AWS Transfer Family servidores. Escolha uma delas ao gerar pares de chaves SSH para autenticação de usuário ou chaves de host do servidor.

RSA (recomendado)

Compatível com todos os clientes e servidores SSH, e. FIPS-compliant Use com SHA-2 hashing para aumentar a segurança:

- `rsa-sha2-256`- Recomendado para a maioria dos casos de uso
- `rsa-sha2-512`- Opção de maior segurança

ED25519

Moderno e eficiente. Tamanhos de chave menores com forte segurança:

- `ssh-ed25519`- Rápido e seguro, mas não FIPS-compliant

ECDSA

Opção de curva elíptica. Bom equilíbrio entre segurança e desempenho:

- `ecdsa-sha2-nistp256`- Curva padrão

- `ecdsa-sha2-nistp384`- Maior curva de segurança
- `ecdsa-sha2-nistp521`- Maior curva de segurança

Note

Oferecemos suporte `ssh-rsa` com SHA1 para políticas de segurança mais antigas. Para obter detalhes, consulte [Algoritmos criptográficos](#).

Escolhendo o algoritmo SSH certo

- Para a maioria dos usuários: use RSA com `rsa-sha2-256` ou `rsa-sha2-512`
- Para conformidade com FIPS: use algoritmos RSA ou ECDSA
- Para ambientes modernos: o ED25519 oferece excelente segurança e desempenho

Algoritmos de criptografia e decodificação PGP

O PGP (Pretty Good Privacy) usa dois tipos de algoritmos trabalhando juntos para criptografar e descriptografar arquivos em fluxos de trabalho:

1. Algoritmos de pares de chaves - usados para gerar os pares de public/private chaves para criptografia e assinaturas digitais
2. Algoritmos simétricos - usados para criptografar os dados reais do arquivo (os algoritmos de par de chaves criptografam a chave simétrica)

Algoritmos de pares de chaves PGP

Escolha um desses algoritmos ao gerar pares de chaves PGP para a decodificação do fluxo de trabalho:

RSA (recomendado)

Recomendado para a maioria dos usuários. Amplamente apoiado, bem estabelecido e. FIPS-compliant Oferece um bom equilíbrio entre segurança e compatibilidade.

ECC (criptografia de curva elíptica)

Mais eficiente do que o RSA com tamanhos de chave menores, mantendo uma segurança forte:

- Curvas NIST - Curvas padrão amplamente suportadas e FIPS-compliant
- BrainPool curvas - Curvas alternativas para requisitos específicos de conformidade
- Curve25519 - Curva moderna de alto desempenho que oferece forte segurança com computação eficiente

ElGamal

Algoritmo legado. Suportado para compatibilidade com sistemas mais antigos. Use RSA ou ECC para novas implementações.

Para obter instruções detalhadas sobre como gerar chaves PGP, consulte. [Gerar chaves PGP](#)

Algoritmos de criptografia simétrica PGP

Esses algoritmos criptografam os dados reais do arquivo. O algoritmo usado depende de como o arquivo PGP foi criado pelo seu software PGP:

FIPS-compliant algoritmos (recomendados para ambientes regulamentados)

- AES-128, AES-192, AES-256 - Padrão Avançado de Criptografia (recomendado)
- 3DES - Padrão de criptografia de dados tripla (antigo, use AES quando possível)

Outros algoritmos suportados

- IDEA, CAST5, Blowfish, DES,,,, TwoFish CAMELLIA-128 CAMELLIA-192 CAMELLIA-256

Note

Você não escolhe o algoritmo simétrico diretamente ao usar AWS Transfer Family fluxos de trabalho - ele é determinado pelo software PGP usado para criar o arquivo criptografado. No entanto, você pode configurar seu software PGP para preferir FIPS-compliant algoritmos como o AES-256

Para obter mais informações sobre algoritmos simétricos compatíveis, consulte [Algoritmos de criptografia simétrica compatíveis](#).

Gere chaves SSH para usuários gerenciados por serviços

É possível configurar seu servidor para autenticar os usuários usando o método de autenticação gerenciada por serviço, no qual os nomes de usuário e chaves SSH são armazenados dentro do serviço. A chave SSH pública do usuário é carregada no servidor como propriedade do usuário. Essa chave é usada pelo servidor como parte de um processo padrão de autenticação baseado em chaves. Cada usuário pode ter várias chaves públicas SSH registradas com um servidor individual. Para ver os limites do número de chaves que podem ser armazenadas por usuário, consulte [endpoints e cotas do AWS Transfer Family](#) no Referência geral da Amazon Web Services.

Como alternativa ao método de autenticação gerenciada pelo serviço, você pode autenticar usuários usando um provedor de identidade personalizado ou AWS Directory Service for Microsoft Active Directory. Para acessar mais informações, consulte [Trabalhar com provedores de identidade personalizados](#) ou [Usando o AWS Directory Service para o Microsoft Active Directory](#).

Um servidor só pode autenticar usuários usando um método (serviço gerenciado, serviço de diretório ou provedor de identidade personalizado), e esse método não pode ser alterado após a criação do servidor.

Tópicos

- [Criação de chaves SSH no macOS, Linux ou Unix](#)
- [Criar chaves SSH no Microsoft Windows](#)
- [Convertendo uma chave SSH2 em formato de chave pública SSH](#)

Criação de chaves SSH no macOS, Linux ou Unix

Nos sistemas operacionais macOS, Linux ou Unix, você usa o comando `ssh-keygen` para criar uma chave pública SSH e uma chave privada SSH, também conhecida como par de chaves.

Note

Nos exemplos a seguir, não especificamos uma frase secreta: nesse caso, a ferramenta solicita que você insira sua senha e a repita para verificar. A criação de uma frase secreta oferece melhor proteção para sua chave privada e também pode melhorar a segurança geral do sistema. Você não pode recuperar sua senha: se você a esquecer, deverá criar uma nova chave.

No entanto, se você estiver gerando uma chave de host do servidor, você deverá especificar uma senha vazia, especificando a opção `-N ""` no comando (ou pressionando **Enter** duas

vezes quando solicitado), pois os servidores Transfer Family não podem solicitar uma senha na inicialização.

Para criar chaves SSH em um sistema operacional macOS, Linux ou Unix

1. Nos sistemas operacionais macOS, Linux ou Unix, abra um terminal de comando.
2. AWS Transfer Family aceita RSA-, ECDSA- e chaves. ED25519-formatted Escolha o comando apropriado com base no tipo de par de chaves que você está gerando.

Dica: *key_name* substitua pelo nome real do seu arquivo de key pair SSH.

- Gerar um par de chaves RSA de 4096 bits:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Gerar um par de chaves ECDSA de 521 bits (o ECDSA tem tamanhos de bits de 256, 384 e 521):

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Gerar um par de chaves ED25519:

```
ssh-keygen -t ed25519 -f key_name
```

Confira a seguir um exemplo de saída ssh-keygen.

```
ssh-keygen -t rsa -b 4096 -f key_name
Generating public/private rsa key pair.

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_name.
Your public key has been saved in key_name.pub.
The key fingerprint is:
SHA256:8tDDwPmanTFcEzjTwPGETVW0GW1nVz+gtCCE8hL7PrQ bob.amazon.com
The key's randomart image is:
+---[RSA 4096]-----+
|  . ....E          |
|  . = ...          |
```

```
| . . . = ..o |
| . o + oo = |
| + = .S.= * |
| . o o ..B + o |
| .o.+.* . |
| =o*+*. |
| ..*o*+. |
+----[SHA256]-----+
```

Dica: Quando você executa o `ssh-keygen` comando conforme mostrado anteriormente, ele cria as chaves pública e privada como arquivos no diretório atual.

Seu par de chaves SSH agora está pronto para uso. Siga as etapas 3 e 4 para armazenar a chave pública SSH para seus usuários gerenciados pelo serviço. Esses usuários usam as chaves quando transferem arquivos nos endpoints do servidor Transfer Family.

3. Navegue até o arquivo `key_name.pub` e abra-o.
4. Copie o texto e cole-o na chave pública SSH para o usuário gerenciado pelo serviço.
 - a. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/> e selecione Servidores no painel de navegação.
 - b. Na página Servidores, selecione a ID do servidor que contém o usuário que você deseja atualizar.
 - c. Selecione o usuário para o qual você está adicionando uma chave pública.
 - d. No painel Chaves públicas SSH, escolha Adicionar chave pública SSH.

Transfer Family > Servers > s- > User: OneUser

User: OneUser

[View logs](#) [Delete](#)

User configuration

[Edit](#)

Role

[Role](#)

Posix Profile

User ID

2001

Group ID

2001

Secondary Group IDs

-

Policy

[View](#)

Home directory

/fs- /

Restricted

SSH public keys (1)

[Delete](#) [Add SSH public key](#)

< 1 >

☐	Date imported	Fingerprint
☐	6/14/2022, 12:53:34 PM	SHA256:-

- e. Cole o texto da chave pública que você gerou na caixa de texto da chave pública SSH e escolha Adicionar chave.

Transfer Family > Servers > s- > OneUser > Add key

Add key

SSH public keys

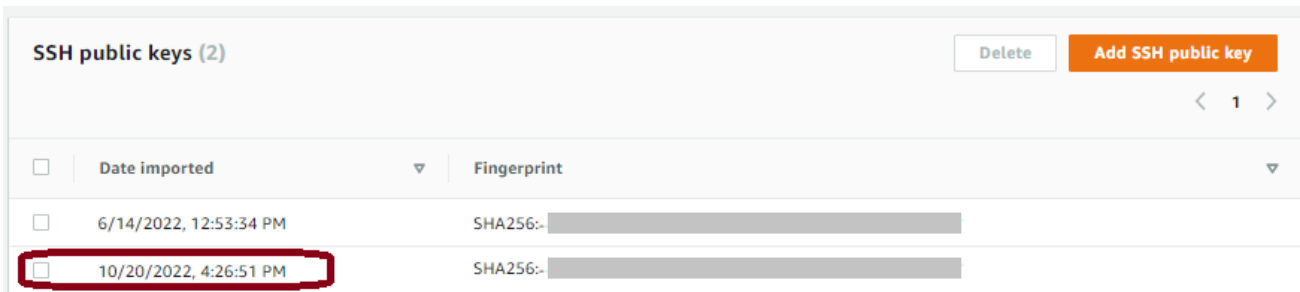
[SSH public key](#) [Info](#)

Paste the contents of SSH public key

Enter SSH public key

[Cancel](#) [Add key](#)

A nova chave está listada no painel de chave pública SSH.



SSH public keys (2)		Delete	Add SSH public key
☐	Date imported	Fingerprint	
☐	6/14/2022, 12:53:34 PM	SHA256:-	
☐	10/20/2022, 4:26:51 PM	SHA256:-	

Criar chaves SSH no Microsoft Windows

O Windows inclui o OpenSSH como um recurso incorporado, que você pode usar para gerar chaves SSH no mesmo formato do Linux ou macOS. Como alternativa, você pode usar ferramentas de terceiros, como o gerador de chaves do PuTTY (PuTTYgen).

Usando o OpenSSH integrado ao Windows

As versões recentes do Windows incluem o OpenSSH por padrão. Você pode usar os mesmos `ssh-keygen` comandos descritos na macOS/Linux seção:

1. Abra o Windows PowerShell ou o prompt de comando.
2. Execute um dos comandos a seguir com base no tipo de chave que você deseja gerar:

- Gerar um par de chaves RSA de 4096 bits:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Para gerar um par de chaves ECDSA de 521 bits:

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Gerar um par de chaves ED25519:

```
ssh-keygen -t ed25519 -f key_name
```

3. Siga as mesmas etapas da macOS/Linux seção para fazer o upload da sua chave pública para AWS Transfer Family.

Usando o PuTTYgen (ferramenta de terceiros)

Alguns clientes SSH de terceiros para Windows, como o PuTTY, usam formatos de chave diferentes. O PuTTY usa o PPK formato para chaves privadas. Se você estiver usando o PuTTY ou ferramentas relacionadas, como o WinSCP, poderá usar o PuTTYgen para criar chaves nesse formato.

Note

Se você apresentar o WinSCP com um arquivo de chave privada que não esteja no formato .ppk, esse cliente oferecerá a você a conversão da chave no formato .ppk.

[Para ver um tutorial sobre a criação de chaves SSH usando o PuTTYgen, consulte o site. SSH.com](#)

Convertendo uma chave SSH2 em formato de chave pública SSH

AWS Transfer Family só aceita chaves SSH-formatted públicas. Se você tiver uma chave pública SSH2, precisará convertê-la. Uma chave pública SSH2 tem o seguinte formato:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20160402"
AAAAB3NzaC1yc2EAAAABJQAAAQEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI
:
:
---- END SSH2 PUBLIC KEY ----
```

Uma chave pública SSH tem o seguinte formato:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

Execute o comando a seguir para converter uma chave SSH2-formatted pública em uma chave SSH-formatted pública. *ssh2-key* Substitua pelo nome da sua chave SSH2 e *ssh-key* pelo nome da sua chave SSH.

```
ssh-keygen -i -f ssh2-key.pub > ssh-key.pub
```

Alterar chaves SSH

Recomendamos as melhores práticas de segurança para mudar as chaves SSH. Geralmente, essa mudança é especificada como parte de uma política de segurança e implementada de forma

automática. Dependendo do nível de segurança, para uma comunicação altamente confidencial, um par de chaves SSH pode ser usado somente uma vez. Isso elimina qualquer risco devido a chaves armazenadas. No entanto, é muito mais comum armazenar credenciais SSH por um período e definir um intervalo que não sobrecarregue excessivamente os usuários. É comum um intervalo de tempo de três meses.

 Note

Para rotação automatizada de chaves SSH usando infraestrutura como código, consulte [Módulos Transfer Family Terraform](#).

Há dois métodos usados para executar a mudança de chaves SSH:

- No console, é possível carregar uma nova chave pública SSH e excluir uma chave pública SSH existente.
- Usando a API, você pode atualizar os usuários existentes usando a [DeleteSshPublicKey](#) API para excluir a chave pública Secure Shell (SSH) de um usuário e a [ImportSshPublicKey](#) API para adicionar uma nova chave pública Secure Shell (SSH) à conta do usuário.

Console

Para executar uma rotação de teclas no console

1. Abra o AWS Transfer Family console em <https://console.aws.amazon.com/transfer/>.
2. Navegue até a página Servidores.
3. Escolha o identificador na coluna ID do servidor para ver a página Configuração do servidor.
4. Em Usuários, marque a caixa de seleção do usuário cuja chave pública SSH você deseja girar, escolha Ações e escolha Adicionar chave para ver a página Adicionar chave.

or

Escolha o nome de usuário para ver a página de Detalhes do usuário e, em seguida, escolha Adicionar chave pública SSH para ver a página Adicionar chave.

5. Insira a nova chave pública SSH e escolha Adicionar chave.

 Important

O formato da chave pública SSH depende do tipo da chave gerada por você.

- Para chaves RSA, o formato é `ssh-rsa` *string*.
- Para chaves ED25519, o formato é `ssh-ed25519` *string*.
- Para chaves ECDSA, o tipo de chave começa com `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384` ou `ecdsa-sha2-nistp521`, dependendo do tamanho da chave que você gerou. A string inicial é então seguida por *string*, semelhante aos outros tipos de chave.

Você retorna à página Detalhes do usuário e a nova chave pública SSH que você acabou de inserir será exibida na seção de chaves públicas SSH.

6. Marque a caixa de seleção das chaves antigas que deseja excluir e selecione Excluir.
7. Confirme a operação de exclusão inserindo a palavra `delete` e selecione Excluir.

API

Para realizar uma rotação de chaves usando a API

1. Nos sistemas operacionais macOS, Linux ou Unix, abra um terminal de comando.
2. Recupere a chave SSH que você deseja excluir digitando o comando a seguir. Para usar esse comando, substitua *serverID* pela ID do servidor do seu servidor Transfer Family e substitua *username* pelo seu nome de usuário.

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

O comando retorna detalhes sobre o usuário. Copie o conteúdo do campo `"SshPublicKeyId":`. Você precisará inserir esse valor posteriormente neste procedimento.

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":  
  "keyID",  
  "DateImported": 1621969331.072 } ],
```

3. Em seguida, importe uma nova chave SSH para seu usuário. No prompt, insira o comando a seguir. Para usar esse comando, substitua *serverID* pela ID do servidor do seu servidor Transfer Family, substitua *username* pelo seu nome de usuário e substitua *public-key* pela impressão digital da sua nova chave pública.

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'
--ssh-public-key-body='public-key'
```

Se o comando for bem-sucedido, nenhuma saída será retornada.

4. Por fim, exclua chave antiga executando o comando a seguir. Para usar esse comando, substitua *serverID* pela ID do servidor do seu servidor Transfer Family, substitua *username* pelo seu nome de usuário e substitua *keyID-from-step-2* pelo valor da ID da chave que você copiou na etapa 2 deste procedimento

```
aws transfer delete-ssh-public-key --server-id='serverID' --user-name='username'
--ssh-public-key-id='keyID-from-step-2'
```

5. (Opcional) Para confirmar que a chave antiga não existe mais, repita a etapa 2.

Gerar chaves PGP

É possível usar a decodificação Pretty Good Privacy (PGP) com os arquivos que o Transfer Family processa com fluxos de trabalho. Para usar a descryptografia em uma etapa do fluxo de trabalho, forneça uma chave PGP. Para obter informações detalhadas sobre algoritmos de chave PGP, incluindo recomendações e conformidade com FIPS, consulte [Algoritmos de pares de chaves PGP](#)

O blog AWS de armazenamento tem uma postagem que descreve como simplesmente descryptografar arquivos sem escrever nenhum código usando fluxos de trabalho do Transfer Family Managed, [criptografar e descryptografar](#) arquivos com PGP e. AWS Transfer Family

O operador que você usa para gerar suas chaves PGP depende do seu sistema operacional e da versão do software de geração de chaves que você está usando.

Se você estiver usando Linux ou Unix, use seu instalador de pacotes para instalar gpg. Dependendo da sua distribuição Linux, um dos comandos a seguir deve funcionar para você.

```
sudo yum install gnupg
```



```
sudo apt-get install gnupg
```

Para Windows ou macOS, você pode baixar o que precisa em. <https://gnupg.org/download/>

Depois de instalar o software gerador de chaves PGP, execute o comando `gpg --full-gen-key` ou `gpg --gen-key` para gerar um par de chaves.

Note

Se você estiver usando o GnuPG versão 2.3.0 ou mais recente, deverá executar `gpg --full-gen-key`. Quando solicitado sobre o tipo de chave a ser criada, escolha RSA ou ECC. Se você escolher ECC, poderá escolher NIST entre BrainPool e Curve25519 para a curva elíptica.

Subcomandos **gpg** úteis

A seguir estão alguns subcomandos úteis para `gpg`:

- `gpg --help` — Esse comando lista as opções disponíveis e pode incluir alguns exemplos.
- `gpg --list-keys` — Esse comando lista os detalhes de todos os pares de chaves que você criou.
- `gpg --fingerprint` — Esse comando lista os detalhes de todos os seus pares de chaves, incluindo a impressão digital de cada chave.
- `gpg --export -a user-name` — Esse comando exporta a parte da chave pública para o *user-name* que foi usada quando a chave foi gerada.

Gerenciar chaves PGP

Para gerenciar suas chaves PGP, use. AWS Secrets Manager

Note

Seu nome secreto inclui a ID do servidor Transfer Family. Isso significa que você já deve ter identificado ou criado um servidor antes de poder armazenar as informações de sua chave PGP em AWS Secrets Manager.

Se quiser usar uma chave e uma senha para todos os seus usuários, é possível armazenar as informações do bloco da chave PGP sob o nome secreto `aws/transfer/server-id/@pgp-default`, onde *server-id* é a ID do seu servidor Transfer Family. O Transfer Family usa essa chave padrão se não houver uma chave que *user-name* corresponda ao usuário que está executando o fluxo de trabalho.

Você pode criar uma chave para um usuário específico. Nesse caso, o formato do nome secreto é `aws/transfer/server-id/user-name`, onde *user-name* corresponde ao usuário que está executando o fluxo de trabalho para um servidor Transfer Family.

 Note

É possível armazenar no máximo 3 chaves privadas PGP por servidor Transfer Family por usuário.

Para configurar chaves PGP para uso com decodificação

1. Dependendo da versão do GPG que você está usando, execute um dos comandos a seguir para gerar um par de chaves PGP.
 - Se você estiver usando a versão 2.3.0 ou mais recente do **GnuPG**, execute o seguinte comando:

```
gpg --full-gen-key
```

Você pode escolher **ouRSA**, se quiser **ECC**, pode escolher entre uma **NIST BrainPool** ou a **Curve25519** curva elíptica. Se você executar `gpg --gen-key` em vez disso, você cria um par de chaves que usa o algoritmo de criptografia ECC Curve 25519.

- Para versões do **GnuPG** anteriores à 2.3.0, é possível usar o comando a seguir, já que RSA é o tipo de criptografia padrão.

```
gpg --gen-key
```

⚠ Important

Durante o processo de geração da chave, você deve fornecer uma senha e um endereço de e-mail. Certifique-se de anotar esses valores. Você deve fornecer a senha ao inserir os detalhes da chave AWS Secrets Manager posteriormente neste procedimento. E você deve fornecer o mesmo endereço de e-mail para exportar a chave privada na próxima etapa.

2. Execute o comando a seguir para exportar a chave privada. Para usar esse comando, substitua *private.pgp* pelo nome do arquivo no qual salvar o bloco de chave privada e *marymajor@example.com* pelo endereço de e-mail que você usou ao gerar o par de chaves.

```
gpg --output private.pgp --armor --export-secret-key marymajor@example.com
```

3. Use AWS Secrets Manager para armazenar sua chave PGP.
 - a. Faça login no Console de gerenciamento da AWS e abra o AWS Secrets Manager console em <https://console.aws.amazon.com/secretsmanager/>.
 - b. No painel de navegação à esquerda, selecione Segredos.
 - c. Na página Segredos, escolha Armazenar um novo segredo.
 - d. Na página Escolher tipo de segredo, em Tipo de segredo, selecione Outro tipo de segredo.
 - e. Na seção Key/value de pares, escolha a Key/valueguia.
 - Chave — Insira **PGPPrivateKey**.

i Note

Você deve inserir a string **PGPPrivateKey** exatamente: não adicione espaços antes ou entre os caracteres.

- valor – cole o texto da sua chave privada no campo de valor. É possível encontrar o texto da sua chave privada no arquivo (por exemplo, *private.pgp*) que você especificou ao exportar sua chave anteriormente neste procedimento. A chave começa com -----BEGIN PGP PRIVATE KEY BLOCK----- e termina com -----END PGP PRIVATE KEY BLOCK-----.

Note

Certifique-se de que o bloco de texto contenha somente a chave privada e também não contenha a chave pública.

f. Selecione Adicionar linha e, na seção de Key/value pares, escolha a Key/value guia.

- Chave — Insira **PGPPassphrase**.

Note

Você deve inserir a string **PGPPassphrase** exatamente: não adicione espaços antes ou entre os caracteres.

- valor — Insira a frase secreta que você usou ao gerar seu par de chaves PGP.

Choose secret type

Secret type [Info](#)

☐ Credentials for Amazon RDS database
 ☐ Credentials for Amazon DocumentDB database
 ☐ Credentials for Amazon Redshift cluster

☐ Credentials for other database
 ☒ Other type of secret
API key, OAuth token, other.

Key/value pairs [Info](#)

Key/value	Plaintext	
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----	Remove
PGPPassphrase	my passphrase	Remove
+ Add row		

Encryption key [Info](#)

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

aws/secretsmanager [Add new key](#)

 Note

É possível adicionar até três conjuntos de chaves e senhas. Para adicionar um segundo conjunto, adicione duas novas linhas, insira **PGPPrivateKey2** e **PGPPassphrase2** para as chaves e cole em outra chave privada e frase secreta. Para adicionar um terceiro conjunto, os valores-chave devem ser **PGPPrivateKey3** e **PGPPassphrase3**.

- g. Escolha Próximo.
- h. Na página Configurar segredo, insira um nome e uma descrição para seu segredo.
 - Se você estiver criando uma chave padrão, ou seja, uma chave que possa ser usada por qualquer usuário do Transfer Family, insira **aws/transfer/server-id/epgp-default**. Substitua **server-id** pela ID do servidor que contém o fluxo de trabalho que tem uma etapa de descriptografia.
 - Se você estiver criando uma chave para ser usada por um usuário específico do Transfer Family, insira **aws/transfer/server-id/user-name**. Substitua **server-id** pela ID do servidor que contém o fluxo de trabalho que tem uma etapa de descriptografia e substitua **user-name** pelo nome do usuário que está executando o fluxo de trabalho. O **user-name** é armazenado no provedor de identidade que o servidor Transfer Family está usando.
- i. Escolha Avançar e aceite os padrões na página Configurar rotação. Em seguida, escolha Próximo.
- j. Na página Revisão, escolha Armazenar para criar e armazenar o segredo.

A captura de tela a seguir mostra os detalhes para o usuário **marymajor** de um servidor Transfer Family específico. Este exemplo mostra três chaves e suas frases secretas correspondentes.

/aws/transfer/s- /marymajor

Replicate secret to other Regions

Secret details

Actions

Encryption key
aws/secretsmanager

Secret name
/aws/transfer/s- /marymajor

Secret ARN
arn:aws:secretsmanager:us-east-2:-:secret:/aws/transfer/s- /marymajor-

Secret description
Contains the PGP secret keys and corresponding passphrases to use for user marymajor on Transfer Family server s-

Secret value Info

Close Edit

Retrieve and view the secret value.

Key/value Plaintext

Secret key	Secret value
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase	mypassphrase
PGPPrivateKey2	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase2	mypassphrase2
PGPPrivateKey3	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase3	mypassphrase3

Cientes PGP compatíveis

Os clientes a seguir foram testados com o Transfer Family e podem ser usados para gerar chaves PGP e criptografar arquivos que você pretende decriptografar com um fluxo de trabalho.

- Gpg4win + Kleopatra.

 Note

Ao selecionar Assinar/Criptografar arquivos, certifique-se de limpar a seleção de Assinar como: atualmente não oferecemos suporte à assinatura de arquivos criptografados.

Sign / Encrypt Files

Prove authenticity (sign)

☐ Sign as: > (certified, created: 11/9/2022)

Encrypt

☒ Encrypt for me: > (certified, created: 11/9/2022)

☐ Encrypt for others: Please enter a name or email address...

☐ Encrypt with password. Anyone you share the password with can read the data.

Output

Output files/folder:

☐ Encrypt / Sign each file separately.

Encrypt **Cancel**

Se você assinar o arquivo criptografado e tentar carregá-lo em um servidor Transfer Family com um fluxo de trabalho de descryptografia, você receberá o seguinte erro:

Encrypted file with signed message unsupported

- Versões principais do GnuPG: 2.4, 2.3, 2.2, 2.0 e 1.4.

Observe que outros clientes PGP também podem funcionar, mas somente os clientes mencionados aqui foram testados com o Transfer Family.

Gerenciamento de identidade e acesso para AWS Transfer Family

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores

do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS Transfer Family os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticação com identidades](#)
- [Gerenciar o acesso usando políticas](#)
- [Como AWS Transfer Family funciona com o IAM](#)
- [AWS Transfer Family exemplos de políticas baseadas em identidade](#)
- [AWS Transfer Family exemplos de políticas baseadas em tags](#)
- [Solução de problemas AWS Transfer Family identidade e acesso](#)
- [Chaves de condição do IAM para governança organizacional](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte [Solução de problemas AWS Transfer Family identidade e acesso](#)).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte [Como AWS Transfer Family funciona com o IAM](#))
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte [AWS Transfer Family exemplos de políticas baseadas em identidade](#))

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login

único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte [Como fazer login em sua Conta da AWS](#) no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte [AWS Signature Version 4 para solicitações de API](#) no Guia do usuário do IAM.

Usuário raiz da conta da AWS

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em [Tarefas que exigem credenciais de usuário-raiz](#) no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte [O que é o IAM Identity Center?](#) no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte [Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias](#) no Guia do usuário do IAM.

Um [grupo do IAM](#) especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte [Casos de uso de usuários do IAM](#) no Guia do usuário do IAM.

Perfis do IAM

Uma [perfil do IAM](#) é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função [mudando de um usuário para uma função do IAM \(console\)](#) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte [Métodos para assumir um perfil](#) no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte [Visão geral das políticas JSON](#) no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Identity-based políticas

Identity-based políticas são documentos de políticas de permissões JSON que você anexa a uma identidade (usuário, grupo ou função). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais 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.

Identity-based as políticas podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do usuário do IAM.

Resource-based políticas

Resource-based políticas são documentos de política JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e 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. É necessário [especificar uma entidade principal](#) em uma política baseada em recursos.

Resource-based políticas são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM 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.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF 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

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do usuário do IAM.
- Políticas de Controle de Serviços (SCPs): as SCPs especificam o número máximo de permissões para uma organização ou uma unidade organizacional no AWS Organizations. Para saber mais, consulte [Políticas de controle de serviço](#) no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs): definem o número máximo de permissões disponíveis para recursos em suas contas. Consulte mais informações em [Resource control policies \(RCPs\)](#) no Guia do usuário do AWS Organizations .
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, 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 AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte [Lógica de avaliação de políticas](#) no Guia do usuário do IAM.

Como AWS Transfer Family funciona com o IAM

Antes de usar o AWS Identity and Access Management (IAM) para gerenciar o acesso AWS Transfer Family, você deve entender quais recursos do IAM estão disponíveis para uso AWS Transfer Family. Para ter uma visão de alto nível de como AWS Transfer Family e outros AWS serviços funcionam com o IAM, consulte [AWS os serviços que funcionam com o IAM](#) no Guia do usuário do IAM.

Tópicos

- [AWS Transfer Family políticas baseadas em identidade](#)
- [AWS Transfer Family Políticas baseadas em recursos](#)
- [Autorização baseada em AWS Transfer Family tags](#)
- [AWS Transfer Family Perfis do IAM](#)

AWS Transfer Family políticas baseadas em identidade

Com as políticas baseadas em identidade do IAM, é possível especificar ações permitidas ou negadas e recursos, bem como as condições sob as quais as ações são permitidas ou negadas. O AWS Transfer Family oferece suporte a ações, recursos e chaves de condição específicos. Para saber mais sobre todos os elementos usados em uma política JSON, consulte [Referência de elementos de política JSON do IAM](#) no AWS Identity and Access Management Guia do usuário do .

Ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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. Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações políticas AWS Transfer Family usam o seguinte prefixo antes da ação: `transfer:`. Por exemplo, para conceder permissão a alguém para criar uma VPC com a operação da API

CreateServer do Transfer Family, inclua a ação `transfer:CreateServer` na política da pessoa. As declarações de política devem incluir um elemento `Action` ou `AWS Transfer Family`. O `NotAction` define seu próprio conjunto de ações que descrevem as tarefas que podem ser executadas com esse serviço.

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

```
"Action": [  
    "transfer:action1",  
    "transfer:action2"
```

Você também pode especificar várias ações utilizando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a ação a seguir:

```
"Action": "transfer:Describe*"
```

Para ver uma lista de AWS Transfer Family ações, consulte [Ações definidas por AWS Transfer Family](#) na Referência de Autorização de Serviço.

Recursos

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao 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. Como prática recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

O recurso de servidor Transfer Family tem o ARN a seguir.

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

Por exemplo, para especificar o servidor do Transfer Family `s-01234567890abcdef` em sua instrução, use o seguinte ARN.

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

Para obter mais informações sobre o formato dos ARNs, consulte os [nomes do recurso da Amazon \(ARN\)](#) na Referência de autorização de serviço, ou [ARNs do IAM](#) no Guia do usuário do IAM.

Para especificar todas as instâncias que pertencem a uma conta específica, use o caractere curinga (*).

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/*"
```

Algumas AWS Transfer Family ações são executadas em vários recursos, como as usadas nas políticas do IAM. Nesses casos, é necessário utilizar o caractere curinga (*).

```
"Resource": "arn:aws:transfer:*:123456789012:server/*"
```

Em alguns casos, você precisa especificar mais de um tipo de recurso, por exemplo, se você criar uma política que permita acesso aos servidores e usuários do Transfer Family. Para especificar vários recursos em uma única declaração, separe os ARNs com vírgulas.

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

Para ver uma lista de AWS Transfer Family recursos, consulte [Tipos de recursos definidos AWS Transfer Family](#) na Referência de Autorização de Serviço.

Chaves de condição

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

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. 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. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

AWS Transfer Family define seu próprio conjunto de chaves de condição e também oferece suporte ao uso de algumas chaves de condição globais. Para ver uma lista de chaves de AWS Transfer Family condição, consulte [Chaves de condição AWS Transfer Family](#) na Referência de autorização de serviço.

Exemplos

Para ver exemplos de políticas AWS Transfer Family baseadas em identidade, consulte. [AWS Transfer Family exemplos de políticas baseadas em identidade](#) Para políticas de IAM específicas do VPC endpoint, consulte. [Limitando o acesso ao VPC endpoint para servidores Transfer Family](#)

AWS Transfer Family Políticas baseadas em recursos

Resource-based políticas são documentos de política JSON que especificam quais ações um diretor específico pode realizar no AWS Transfer Family recurso e sob quais condições. O Amazon S3 oferece suporte a políticas de permissões baseadas em recursos para o Amazon S3. *buckets* Resource-based as políticas permitem que você conceda permissão de uso a outras contas por recurso. Você também pode usar uma política baseada em recursos para permitir que um AWS serviço acesse seu Amazon S3. *buckets*

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a [entidade principal em uma política baseada em recurso](#). Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso estão em AWS contas diferentes, você também deve conceder permissão à entidade principal para acessar o recurso. Conceda permissão anexando 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. Para obter mais informações, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do AWS Identity and Access Management .

O serviço Amazon S3 oferece suporte a apenas um tipo de política baseada em recursos chamada *bucket* política, que é anexada a uma. *bucket* Essa política define quais entidades principais (contas, usuários, perfis e usuários federados) podem realizar ações no objeto.

Exemplos

Para ver exemplos de políticas AWS Transfer Family baseadas em recursos, consulte. [AWS Transfer Family exemplos de políticas baseadas em tags](#)

Autorização baseada em AWS Transfer Family tags

Você pode anexar tags a AWS Transfer Family recursos ou passar tags em uma solicitação para AWS Transfer Family. Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `transfer:ResourceTag/key-name`,

`aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`. Para obter informações sobre como usar tags para controlar o acesso aos AWS Transfer Family recursos, consulte [AWS Transfer Family exemplos de políticas baseadas em tags](#).

AWS Transfer Family Perfis do IAM

Uma [função do IAM](#) é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com AWS Transfer Family

É possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como [AssumeRole](#) ou [GetFederationToken](#).

AWS Transfer Family suporta o uso de credenciais temporárias.

AWS Transfer Family exemplos de políticas baseadas em identidade

Por padrão, os usuários e os perfis do IAM não têm permissão para criar ou modificar recursos do AWS Transfer Family . Eles também não podem realizar tarefas usando a AWS API Console de gerenciamento da AWS CLI, ou. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte [Criar políticas na guia JSON](#) no Guia do usuário do AWS Identity and Access Management .

Tópicos

- [Práticas recomendadas de política](#)
- [Usar o AWS Transfer Family console](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)

Práticas recomendadas de política

Identity-based as políticas determinam se alguém pode criar, acessar ou excluir AWS Transfer Family recursos 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 com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam 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 às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como 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 root, ative Conta da AWS 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 AWS Transfer Family console

Para acessar o AWS Transfer Family console, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os AWS Transfer Family recursos em sua AWS conta. 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 do IAM) com essa política. Para obter mais informações, consulte [Adicionar permissões a um usuário](#) no Guia do usuário do AWS Identity and Access Management .

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

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 programaticamente usando a API AWS CLI ou AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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": "*"
}
]
```

AWS Transfer Family exemplos de políticas baseadas em tags

Veja a seguir exemplos de como controlar o acesso aos AWS Transfer Family recursos com base em tags.

Usando tags para controlar o acesso a AWS Transfer Family recursos

Condições nas políticas do IAM são parte da sintaxe que você usa para especificar permissões para recursos do AWS Transfer Family . Você pode controlar o acesso aos AWS Transfer Family recursos (como usuários, servidores, funções e outras entidades) com base nas tags desses recursos. As tags são pares de chave-valor. Para obter mais informações sobre como marcar recursos, consulte [Como marcar AWS recursos](#) no. Referência geral da AWS

Em AWS Transfer Family, os recursos podem ter tags e algumas ações podem incluir tags. Ao criar uma política do IAM, é possível usar chaves de condição de tag para controlar o seguinte:

- Quais usuários podem realizar ações em um AWS Transfer Family recurso, com base nas tags que o recurso tem.
- Quais tags podem ser transmitidas na solicitação de uma ação.
- Se chaves de tags específicas podem ser usadas em uma solicitação.

Ao usar o controle de acesso baseado em tags, é possível aplicar um controle mais preciso do que no nível da API. Você também pode aplicar um controle mais dinâmico do que usando o controle de acesso baseado em recursos. É possível criar políticas do IAM que permitem ou não uma operação baseada em tags fornecidas na solicitação (tags de solicitação). Você também pode criar políticas do IAM baseadas em tags no recurso em que estão sendo operadas (tags de recurso). Em geral, as tags de recursos são para tags que já estão nos recursos, e as tags de solicitação são para quando você adiciona ou remove tags de um recurso.

Para obter a sintaxe e a semântica completas das chaves de condição de tag, consulte [Controlar o acesso a recursos AWS usando tags](#) no Guia do usuário do IAM. Para obter detalhes sobre a especificação de políticas do IAM com o API Gateway, consulte [Controlar o acesso a uma API com permissões do IAM](#) no Guia do desenvolvedor do API Gateway.

Exemplo 1: negar ações com base em tags de recurso

É possível negar que uma ação seja executada em um recurso com base em tags. O exemplo de política a seguir nega as operações TagResource, UntagResource, StartServer, StopServer, DescribeServer e DescribeUser se o recurso do usuário ou do servidor estiver marcado com a chave stage e o valor prod.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "transfer:TagResource",
        "transfer:UntagResource",
        "transfer:StartServer",
        "transfer:StopServer",
        "transfer:DescribeServer",
        "transfer:DescribeUser"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/stage": "prod"
        }
      }
    }
  ]
}
```

Exemplo 2: permitir ações com base em tags de recursos

É possível permitir que uma ação seja executada em um recurso com base em tags. O exemplo de política a seguir permite as operações TagResource, UntagResource, StartServer,

StopServer, DescribeServer e DescribeUser se o recurso do usuário ou do servidor estiver marcado com a chave stage e o valor prod.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "transfer:TagResource",
        "transfer:UntagResource",
        "transfer:StartServer",
        "transfer:StopServer",
        "transfer:DescribeServer",
        "transfer:DescribeUser"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/stage": "prod"
        }
      }
    }
  ]
}
```

Exemplo 3: negar a criação de um usuário ou servidor com base em tags de solicitação

O exemplo de política a seguir contém duas declarações. A primeira declaração nega a operação CreateServer em todos os recursos se a chave do centro de custo da tag não tiver um valor.

A segunda declaração nega a operação CreateServer se a chave do centro de custo da tag contiver qualquer outro valor além de 1, 2 ou 3.

 Note

Essa política permite criar ou excluir um recurso que contém uma chave chamada costcenter e um valor de 1, 2 ou 3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "transfer:CreateServer"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/costcenter": "true"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "transfer:CreateServer",
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAnyValue:StringNotEquals": {
          "aws:RequestTag/costcenter": [
            "1",
            "2",
            "3"
          ]
        }
      }
    }
  ]
}
```

Solução de problemas AWS Transfer Family identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Transfer Family um IAM.

Tópicos

- [Não estou autorizado a realizar uma ação em AWS Transfer Family](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha AWS conta para acessar minha AWS Transfer Family recursos](#)

Não estou autorizado a realizar uma ação em AWS Transfer Family

Se isso Console de gerenciamento da AWS indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

O erro de exemplo a seguir ocorre quando o usuário `mateojackson` do IAM tenta usar o console para visualizar detalhes sobre um `widget`, mas não tem as permissões `transfer:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
transfer:GetWidget on resource: my-example-widget
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso `my-example-widget` usando a ação `transfer;:GetWidget`.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS Transfer Family.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS Transfer Family. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

O exemplo de política a seguir contém a permissão para transmitir uma função para AWS Transfer Family. **123456789012** Substitua pelo ID da sua conta da AWS e **MyTransferRole** pelo nome real da sua função do IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/MyTransferRole",
      "Effect": "Allow"
    }
  ]
}
```

Quero permitir que pessoas fora da minha AWS conta para acessar minha AWS Transfer Family recursos

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 é AWS Transfer Family compatível com esses recursos, consulte [Como AWS Transfer Family funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todas as Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outra Conta da AWS que você possui](#) no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como [fornecer acesso Contas da AWS 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 saber 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.

Chaves de condição do IAM para governança organizacional

AWS Transfer Family fornece chaves de condição do IAM que permitem restringir as configurações de recursos em qualquer política do IAM. Essas chaves de condição podem ser usadas em políticas baseadas em identidade anexadas a usuários ou funções, ou em Políticas de Controle de Serviços (SCPs) para governança organizacional.

As políticas de controle de serviços são políticas do IAM que se aplicam a toda a AWS organização, fornecendo proteções preventivas em várias contas. Quando usadas em SCPs, essas chaves de condição ajudam a impor os requisitos de segurança e conformidade em toda a organização.

Consulte também

- [Ações, recursos e chaves de condição para Transfer Family](#)
- [Políticas de controle de serviço \(SCPs\)](#)
- Assista a [este vídeo](#) que descreve como aplicar proteções preventivas usando políticas de controle de serviço

Chaves de condição disponíveis

AWS Transfer Family oferece suporte às seguintes chaves de condição para uso em políticas do IAM:

`transfer:RequestServerEndpointType`

Restringe a criação e as atualizações do servidor com base no tipo de endpoint (PUBLIC, VPC, VPC_ENDPOINT). Comumente usado para evitar endpoints voltados para o público.

`transfer:RequestServerProtocols`

Restringe a criação e as atualizações do servidor com base nos protocolos suportados (SFTP, FTPS, FTP, AS2).

`transfer:RequestServerDomain`

Restringe a criação do servidor com base no tipo de domínio (S3, EFS).

`transfer:RequestConnectorProtocol`

Restringe a criação de conectores com base no protocolo (AS2, SFTP).

Ações compatíveis

As chaves de condição podem ser aplicadas às seguintes AWS Transfer Family ações:

- `CreateServer`: Suportes `RequestServerEndpointType` `RequestServerProtocols` e chaves de `RequestServerDomain` condição
- `UpdateServer`: Suportes `RequestServerEndpointType` e chaves de `RequestServerProtocols` condição
- `CreateConnector`: Suporta chave de `RequestConnectorProtocol` condição

Exemplo de política de SCP

O exemplo a seguir, o SCP impede a criação de AWS Transfer Family servidores públicos em sua organização:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyPublicTransferServers",
    "Effect": "Deny",
    "Action": ["transfer:CreateServer", "transfer:UpdateServer"],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "transfer:RequestServerEndpointType": "PUBLIC"
      }
    }
  }]
}
```

Validação de conformidade AWS Transfer Family

Third-party os auditores avaliam a segurança e a conformidade AWS Transfer Family como parte de vários programas de AWS conformidade. Isso inclui SOC, PCI, HIPAA e outros. Para ver a lista completa, consulte [AWS Serviços no escopo por programa de conformidade](#).

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte [AWS serviços no escopo por programa de conformidade](#). Para obter informações gerais, consulte [Programas de conformidade da AWS](#).

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#).

Sua responsabilidade de conformidade ao usar AWS Transfer Family é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Guias de início rápido sobre segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos focados em segurança e conformidade em AWS
- Documento técnico [sobre arquitetura para segurança e conformidade com a HIPAA — Este whitepaper](#) descreve como as empresas podem usar para criar aplicativos. AWS HIPAA-compliant
- [Recursos de compatibilidade da AWS](#): essa coleção de manuais e guias pode ser aplicável a seu setor e local.
- [AWS Config](#) — Esse AWS serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub CSPM](#) — Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência em AWS Transfer Family

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam

o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

AWS Transfer Family suporta até 3 zonas de disponibilidade e é apoiado por uma frota redundante e de escalonamento automático para suas solicitações de conexão e transferência.

Para todos os endpoints da Transfer Family:

- A Zone-level redundância de disponibilidade está incorporada ao serviço.
- Há frotas redundantes para cada AZ.
- Essa redundância é fornecida automaticamente.

 Note

Para endpoints em uma Virtual Private Cloud (VPC), é possível fornecer uma única sub-rede. No entanto, recomendamos que você crie endpoints em várias zonas de disponibilidade em sua VPC, para reduzir o risco de interrupções no serviço durante interrupções na zona de disponibilidade.

Consulte também

- Para obter detalhes sobre como criar servidores Transfer Family em uma VPC, consulte [Crie um servidor em uma VPC \(virtual private cloud\)](#).
- Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte [infraestrutura AWS global](#).
- Para obter um exemplo de como criar maior redundância e minimizar a latência da rede usando o Latency-based roteamento, consulte a postagem do blog [Minimize a latência da rede](#) com seus servidores. AWS Transfer Family

Crie uma conexão privada entre uma VPC e AWS Transfer Family APIs

Você pode estabelecer uma conexão privada entre sua VPC e as AWS Transfer Family APIs criando uma interface VPC endpoint, desenvolvida por [AWS PrivateLink](#) Você pode acessar as AWS

Transfer Family APIs como se elas estivessem em sua VPC, sem usar um gateway de internet, dispositivo NAT, conexão VPN ou conexão AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para a comunicação com APIs do AWS Transfer Family .

Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Para obter mais informações, consulte [Acesse os AWS serviços AWS PrivateLink](#) no AWS PrivateLink Guia. Antes de configurar uma interface VPC endpoint para AWS Transfer Family APIs, leia as [considerações](#) no guia.AWS PrivateLink

Controle do acesso usando políticas de VPC endpoint

Por padrão, o acesso total às AWS Transfer Family APIs é permitido por meio do endpoint. Você pode controlar o acesso ao endpoint de interface usando as políticas de endpoint da VPC. Você pode anexar uma política de endpoint ao seu VPC endpoint que controla o acesso às APIs. AWS Transfer Family Essa política especifica as seguintes informações:

- A entidade principal que pode realizar ações.
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para mais informações, consulte [Controlar o acesso a serviços com VPC endpoints](#) no Guia do usuário da Amazon VPC.

Veja a seguir um exemplo de uma política de endpoint para AWS Transfer Family APIs. Quando anexada a um endpoint, essa política concede acesso a todas as ações de AWS Transfer Family APIs em todos os recursos, exceto aquelas marcadas com chave Environment e valor. Test

```
{
  "Statement": [{
    "Effect": "Deny",
    "Action": "transfer:StartFileTransfer",
    "Principal": "*",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Environment": "Test"
      }
    }
  }], {
    "Effect": "Allow",
```

```
    "Action": "transfer:*",
    "Principal": "*",
    "Resource": "*"
  }]
}
```

Crie uma interface VPC endpoint para AWS Transfer Family APIs

Você pode criar um VPC endpoint para AWS Transfer Family APIs usando o console Amazon VPC ou a interface de linha de comando (). AWS CLI Para obter mais informações, consulte [Create a VPC endpoint](#) (Criar um endpoint da VPC) no Guia do AWS PrivateLink.

Crie um VPC endpoint para AWS Transfer Family APIs usando um dos seguintes nomes de serviço:

- `com.amazonaws.region.transfer`
- `com.amazonaws.region.transfer-fips`— Criar uma interface VPC endpoint que esteja em conformidade com o padrão do governo dos EUA da publicação 140-3 do Federal Information Processing Standard (FIPS).

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API às AWS Transfer Family APIs usando seu nome DNS padrão para a região, por exemplo, `transfer.us-east-1.amazonaws.com`

Segurança da infraestrutura em AWS Transfer Family

Como serviço gerenciado, AWS Transfer Family é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte [AWS Cloud Security](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção](#) de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS Transfer Family pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Suítes de criptografia com sigilo direto perfeito (PFS), como DHE (efêmero) ou ECDHE (curva elíptica efêmera Diffie-Hellman). Diffie-Hellman A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Evite colocar NLBs e NATs na frente de AWS Transfer Family servidores

Note

Servidores configurados com protocolos FTP e FTPS só permitem a configuração com uma VPC: não há endpoint público disponível para. FTP/FTPS

Muitos clientes configuram um Network Load Balancer (NLB) para rotear o tráfego para o servidor. AWS Transfer Family Eles normalmente fazem isso porque criaram seu servidor antes de AWS oferecer uma maneira de acessá-lo de dentro da VPC e da Internet, ou para oferecer suporte a FTP na Internet. Essa configuração não apenas aumenta os custos para os clientes, mas também pode causar outros problemas, que descrevemos nesta seção.

Os gateways NAT são um componente obrigatório quando os clientes estão se conectando a partir de uma rede privada do cliente por trás de um firewall corporativo. No entanto, você deve estar ciente de que quando muitos clientes estão usando o mesmo gateway NAT, isso pode afetar o desempenho e os limites de conexão. Se houver um NLB ou NAT no caminho de comunicação do cliente para o servidor FTP ou FTPS, o servidor não poderá reconhecer com precisão o endereço IP do cliente, pois AWS Transfer Family vê somente o endereço IP do NLB ou NAT.

Se você estiver usando a configuração de um servidor Transfer Family por trás de um NLB, recomendamos que você mude para um endpoint VPC e use um endereço IP elástico em vez de usar um NLB. Ao usar gateways NAT, esteja ciente das limitações de conexão descritas abaixo.

Se você estiver usando o protocolo FTPS, essa configuração não apenas reduz sua capacidade de auditar quem está acessando seu servidor, mas também pode afetar o desempenho. AWS Transfer Family usa o endereço IP de origem para fragmentar suas conexões em nosso plano de dados. Para FTPS, isso significa que, em vez de ter 10.000 conexões simultâneas, os servidores Transfer Family com gateways NLB ou NAT na rota de comunicação estão limitados a apenas 300 conexões simultâneas.

Embora seja recomendável evitar balanceadores de carga de rede na frente dos AWS Transfer Family servidores, se sua implementação de FTP ou FTPS exigir um NLB ou NAT na rota de comunicação do cliente, siga estas recomendações:

- Para um NLB, use a porta 21 para verificações de integridade, em vez das portas 8192-8200.
- Para o AWS Transfer Family servidor, habilite a retomada da sessão TLS configurando.
`TlsSessionResumptionMode = ENFORCED`

Note

Esse é o modo recomendado, pois fornece segurança aprimorada:

- Exige que os clientes usem a retomada da sessão TLS para conexões subsequentes.
- Fornece garantias de segurança mais fortes, garantindo parâmetros de criptografia consistentes.
- Ajuda a evitar possíveis ataques de downgrade.
- Mantém a conformidade com os padrões de segurança enquanto otimiza o desempenho.

- Se possível, deixe de usar um NLB para aproveitar ao máximo os limites de AWS Transfer Family desempenho e conexão.

Para obter orientação adicional sobre alternativas de NLB, entre em contato com a equipe de gerenciamento de AWS Transfer Family produtos por meio do Support AWS . Para obter mais informações sobre como melhorar sua postura de segurança, consulte a postagem do blog [Seis dicas para melhorar a segurança do seu AWS Transfer Family servidor](#).

Segurança da infraestrutura de conectividade VPC

Os conectores SFTP com tipo de saída VPC fornecem segurança aprimorada da infraestrutura por meio do isolamento da rede e da conectividade privada:

Benefícios do isolamento de rede

- Tráfego de rede privada: todo o tráfego de conectores para servidores SFTP privados permanece em sua VPC, nunca atravessando a Internet pública.
- Saída controlada: para endpoints públicos acessados via VPC, o tráfego é roteado por seus gateways NAT, oferecendo controle sobre endereços IP de saída e políticas de rede.
- Controles de segurança da VPC: aproveite os grupos de segurança, as ACLs de rede e as tabelas de rotas existentes da VPC para controlar o acesso à rede do conector.
- Conectividade híbrida: acesse servidores SFTP locais por meio de conexões VPN ou Direct Connect estabelecidas sem exposição adicional à Internet.

Considerações de segurança do Resource Gateway

Os Resource Gateways fornecem pontos de entrada seguros para acesso a Cross-VPC recursos:

- Multi-AZ implantação: os gateways de recursos exigem sub-redes em pelo menos duas zonas de disponibilidade para alta disponibilidade e tolerância a falhas.
- Controles de grupos de segurança: configure grupos de segurança para restringir o acesso às portas SFTP (normalmente a porta 22) somente de fontes autorizadas.
- Posicionamento de sub-rede privada: implante gateways de recursos em sub-redes privadas ao se conectar a servidores SFTP privados para manter o isolamento da rede.
- Limites de conexão: cada Resource Gateway suporta até 350 conexões simultâneas com um tempo limite de inatividade de 350 segundos para conexões TCP.

Adicione um firewall da aplicação web

AWS WAF é um firewall de aplicativos da web que ajuda a proteger aplicativos e APIs da web contra ataques. É possível usá-lo para configurar um conjunto de regras chamado de lista de controle de acesso à web (Web ACL) que permitem, bloqueiam ou contam solicitações da web com base em regras e condições de segurança da web personalizáveis que você define. Para obter mais informações, consulte [Usando AWS WAF para proteger suas APIs](#).

Para adicionar AWS WAF

1. Abra o console do API Gateway em <https://console.aws.amazon.com/apigateway/>.
2. No painel de navegação das APIs, escolha seu modelo de provedor de identidade personalizado.
3. Escolha Estágios.
4. No painel Estágios, escolha o nome do estágio.
5. No painel Editor de estágio, escolha a guia Configurações.
6. Execute um destes procedimentos:
 - Em Web Application Firewall (WAF), para Web ACL, selecione a Web ACL que você deseja associar a esse estágio.
 - Se a Web ACL de que você precisa não existir, você precisará criar uma fazendo o seguinte:
 1. Escolha Criar Web ACL.

2. Na página inicial do serviço AWS WAF, escolha Create web ACL.
 3. Em Detalhes do Web ACL, em Nome, digite o nome do Web ACL.
 4. Em Regras, escolha Adicionar regras e, em seguida, escolha Adicionar minhas próprias regras e grupos de regras.
 5. Em Tipo de regra, escolha conjunto de IPs para identificar uma lista específica de endereços IP.
 6. Em Regra, insira o nome da regra.
 7. Em conjunto de IPs, escolha um conjunto de IPs existentes. Para criar um conjunto de IPs, consulte [Criar um conjunto de IPs](#).
 8. Em Endereço IP para usar como endereço de origem, escolha endereço IP no cabeçalho.
 9. Em Nome do campo de cabeçalho, insira SourceIP.
 10. Em Posição dentro do cabeçalho, escolha Primeiro endereço IP.
 11. Em Fallback para endereço IP ausente, escolha Corresponder ou Não corresponder, dependendo de como você deseja lidar com um endereço IP inválido (ou ausente) no cabeçalho.
 12. Em Ação, escolha a ação do conjunto de IPs.
 13. Em Ação de Web ACL padrão para solicitações que não correspondem a nenhuma regra, escolha Permitir ou Bloquear e clique em Avançar.
 14. Para as etapas 4 e 5, escolha Avançar.
 15. Em Revisar e criar, revise suas escolhas e escolha Criar Web ACL.
7. Escolha Salvar alterações.
 8. Escolha Recursos.
 9. Escolha Ações e Implantar API.

Para obter informações sobre como proteger o Transfer Family com o firewall de aplicativos AWS web, consulte [Protegendo o Transfer Family com o firewall do AWS aplicativo e o Amazon API Gateway](#) no blog AWS de armazenamento.

Cross-service prevenção delegada confusa

O problema "confused deputy" é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executar a ação. Em AWS, a falsificação de identidade entre serviços pode resultar em um problema confuso de

delegado. Cross-service a representação pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta. Para obter uma descrição detalhada desse problema, consulte [o problema de “confused deputy”](#) no Guia do usuário do IAM.

Recomendamos usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` as chaves de contexto nas políticas de recursos para limitar as permissões que a AWS Transfer Family tem para o recurso. Se você utilizar ambas as chaves de contexto de condição global, o valor `aws:SourceAccount` e a conta `aws:SourceArn` no valor deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

A maneira mais eficaz de se proteger contra o problema do “confused deputy” é usar o nome do recurso da Amazon (ARN) exato do recurso que você deseja permitir. Se você estiver especificando vários recursos, use a chave de condição de contexto global `aws:SourceArn` com caracteres curingas (*) para as partes desconhecidas do ARN. Por exemplo, `.arn:aws:transfer::region::account-id:server/*`

AWS O Transfer Family usa os seguintes tipos de funções:

- Função de usuário — Permite que usuários gerenciados pelo serviço acessem os recursos necessários do Transfer Family. AWS Transfer Family assume essa função no contexto de um ARN de usuário do Transfer Family.
- Função de acesso: fornece acesso apenas aos arquivos do Amazon S3 que estão sendo transferidos. Para transferências do AS2 de entrada, a função de acesso usa o nome do recurso da Amazon (ARN) para o contrato. Para transferências do AS2 de saída, a função de acesso usa o ARN para o conector.
- Função de invocação: para uso com o Amazon API Gateway como provedor de identidade personalizada do servidor. O Transfer Family assume essa função no contexto de um ARN do servidor do Transfer Family.
- Função de registro — usada para registrar entradas na Amazon CloudWatch. O Transfer Family usa essa função para registrar em log os detalhes de sucesso e falha com informações sobre transferências de arquivos. O Transfer Family assume essa função no contexto de um ARN do servidor do Transfer Family. Para transferências do AS2 de saída, a função de acesso usa o conector ARN.

- **Função de execução:** permite que um usuário do Transfer Family chame e inicie fluxos de trabalho. O Transfer Family assume essa função no contexto de um ARN de fluxo de trabalho do Transfer Family.

Para obter mais informações, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.

 Note

Nos exemplos a seguir, substitua cada um *user input placeholder* por suas próprias informações.

 Note

Em nossos exemplos, usamos tanto `ArnLike` quanto `ArnEquals`. Eles são funcionalmente idênticos, portanto, é possível usá-los ao criar suas políticas. A documentação do Transfer Family usa `ArnLike` quando a condição contém um caractere curinga, e `ArnEquals` para indicar uma condição de correspondência exata.

AWS A função de usuário do Transfer Family entre serviços confundiu a prevenção adjunta

O exemplo de política a seguir permite que qualquer usuário de qualquer servidor na conta assuma a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
```

```

        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/
*
      }
    }
  ]
}

```

O exemplo de política a seguir permite que qualquer usuário de um servidor específico assuma a função.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/server-id/
*
        }
      }
    }
  ]
}

```

O exemplo de política a seguir permite que um usuário específico de um servidor específico assuma a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/server-id/user-name"
        }
      }
    }
  ]
}
```

AWS Transfer Family: função de fluxo de trabalho entre serviços, prevenção delegada confusa

O exemplo de política a seguir permite que qualquer fluxo de trabalho na conta assuma a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
```

```

        "aws:SourceArn": "arn:aws:transfer:us-west-2:111122223333:workflow/*"
      }
    }
  ]
}

```

O exemplo de política a seguir permite que um fluxo de trabalho específico assuma a função.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-id"
        }
      }
    }
  ]
}

```

AWS A função do conector Transfer Family entre serviços confundiu a prevenção adjunta

O exemplo de política a seguir permite que qualquer conector na conta assuma a função.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "",
    "Effect": "Allow",
    "Principal": {
      "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/*"
      }
    }
  }
]
}

```

O exemplo de política a seguir permite que um conector específico assuma a função.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/connector-id"
        }
      }
    }
  ]
}

```


AWS Transfer Family: a função de registro e invocação entre serviços confundiu a prevenção adjunta

Note

Os exemplos a seguir podem ser usados nas funções de registro e de invocação. Nesses exemplos, você pode remover os detalhes do ARN de um fluxo de trabalho se o servidor não tiver nenhum fluxo de trabalho vinculado a ele.

O exemplo de logging/invoction política a seguir permite que qualquer servidor (e fluxo de trabalho) na conta assumam a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

O exemplo de logging/invoke política a seguir permite que um servidor específico (e fluxo de trabalho) assumam a função.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificServerWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/server-id",
            "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-id"
          ]
        }
      }
    }
  ]
}
```

AWS políticas gerenciadas para AWS Transfer Family

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É preciso tempo e experiência para [criar AWS Identity and Access Management \(IAM\) políticas gerenciadas pelo cliente](#) que forneçam à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre as políticas gerenciadas da AWS, consulte [Políticas gerenciadas da AWS](#) no Guia do usuário do IAM. Para obter uma lista detalhada de todas as políticas AWS gerenciadas, consulte o [guia de referência de políticas AWS gerenciadas](#).

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política `ReadOnlyAccess` AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte [Políticas gerenciadas pela AWS para perfis de trabalho](#) no Guia do usuário do IAM.

AWS política gerenciada: `AWSTransferConsoleFullAccess`

A `AWSTransferConsoleFullAccess` política fornece acesso total ao Transfer Family por meio do AWS Management Console. Para obter mais informações, consulte a [Service-linked função de AWS Transfer Family](#).

AWS política gerenciada: `AWSTransferFullAccess`

A política `AWSTransferFullAccess` concede acesso total aos serviços do Transfer Family. Para obter mais informações, consulte a [Service-linked função de AWS Transfer Family](#).

AWS política gerenciada: `AWSTransferLoggingAccess`

A `AWSTransferLoggingAccess` política concede à AWS Transfer Family acesso total para criar fluxos e grupos de registros e colocar eventos de registro em sua conta. Para obter mais informações, consulte a [Service-linked função de AWS Transfer Family](#).

AWS política gerenciada: `AWSTransferReadOnlyAccess`

A política `AWSTransferReadOnlyAccess` concede acesso somente leitura aos serviços do Transfer Family. Para obter mais informações, consulte a [Service-linked função de AWS Transfer Family](#).

AWS Transferir atualizações do Transfer Family para AWS políticas gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do AWS Transfer Family desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página [Histórico do documento para AWS Transfer Family](#).

Alteração	Descrição	Data
Atualização da documentação	Seções adicionadas para cada uma das políticas gerenciadas pelo Transfer Family.	27 de janeiro de 2022
AWSTransferReadOnlyAccess – atualização para uma política existente	AWS A Transfer Family adicionou novas permissões para permitir a leitura da política AWS Managed Microsoft AD.	30 de setembro de 2021
AWS Transfer Family começou a monitorar as alterações	AWS A Transfer Family começou a monitorar as mudanças em suas políticas AWS gerenciadas.	15 de junho de 2021

Módulos Transfer Family Terraform

[HashiCorpO Terraform](#) é um mecanismo de Infraestrutura como Código (IaC) de código aberto desenvolvido usando a Linguagem de HashiCorp Configuração (HCL). O Terraform fornece um fluxo de trabalho consistente de interface de linha de comando (CLI) que, em conjunto com o Transfer AWS Family para a infraestrutura de back-end, pode gerenciar centenas de serviços em nuvem e codificar APIs em nuvem em arquivos de configuração declarativos.

Você pode usar o Terraform para implantar com segurança servidores SFTP e conectores SFTP da AWS Transfer Family, junto com dependências e personalizações associadas. Para o repositório que contém o código do Terraform para criar os recursos necessários para executar o AWS Transfer Family, consulte o código-fonte do [módulo Terraform Transfer Family](#) em GitHub.

Note

Os módulos AWS Transfer Family para o Terraform são um esforço apoiado pela comunidade. Eles não fazem parte de um AWS serviço. Best-effort o suporte é fornecido pela comunidade AWS de armazenamento.

Servidores SFTP

Essa automação fornece um módulo Terraform personalizável e exemplos completos para criar um endpoint SFTP (PUBLICou VPC tipos de endpoint), integrar-se à Amazon CloudWatch para registro e monitoramento, gerenciar identidades de usuários para acesso ao endpoint e configurar funções do IAM para acesso aos buckets do Amazon S3 onde os arquivos são armazenados. O módulo suporta várias chaves públicas SSH por usuário (até 50 chaves) para maior segurança e recursos de rotação de chaves.

Conectores SFTP

AWS O módulo Transfer Family Terraform agora suporta a implantação de conectores SFTP para transferir arquivos entre o Amazon S3 e servidores SFTP remotos. Os conectores SFTP fornecem uma capacidade totalmente gerenciada e de baixo código para copiar arquivos entre o Amazon S3 e servidores SFTP remotos.

Agora você pode usar o Terraform para provisionar programaticamente seus conectores SFTP, dependências associadas e personalizações em uma única implantação. O módulo também fornece exemplos completos para automatizar fluxos de trabalho de transferência de arquivos com base em uma programação ou acionadores de eventos. O uso do Terraform para implantação elimina a necessidade de configurações manuais demoradas e propensas a erros, além de fornecer uma opção de implantação rápida, repetível e segura que pode ser escalada.

COMO 2

Para mostrar suporte aos modelos AS2 Terraform, adicione uma reação positiva (#) à solicitação de recurso de modelos do [Transfer Family Terraform](#). Você também pode adicionar um comentário descrevendo seu caso de uso.

B2B Data Interchange

AWS B2B Data Interchange automatiza a transformação, validação e geração de documentos de intercâmbio eletrônico de dados (EDI) de e para formatos de dados JSON e XML. [Para mostrar suporte aos modelos do Terraform para B2B Data Interchange, adicione uma reação positiva \(#\) à solicitação de recurso.](#) Você também pode adicionar um comentário descrevendo seu caso de uso.

Solução de problemas AWS Transfer Family

Este capítulo fornece informações sobre solução de problemas comuns que você pode encontrar ao usar AWS Transfer Family. Cada seção se concentra em uma área específica de funcionalidade para ajudá-lo a encontrar rapidamente soluções para seus problemas.

- Para problemas com o IAM no Transfer Family, consulte [Solução de problemas AWS Transfer Family identidade e acesso](#).
- Para problemas com seus aplicativos web Transfer Family, consulte [Solução de problemas em seus aplicativos da web](#).

Tópicos

- [Solução de problemas de autenticação](#)
- [Solução de problemas do conector SFTP](#)
- [Solucionar problemas de conectividade e transferência de SFTP](#)
- [Solucionar problemas de provedores de identidade personalizados](#)
- [Solucionar problemas de fluxo de trabalho](#)
- [Solucionar problemas do EFS](#)
- [Solucionar problemas de armazenamento e criptografia](#)
- [Solucionar problemas de monitoramento e alerta](#)
- [Solucionar problemas de transferência entre regiões](#)
- [Solucionar problemas de implantação do Terraform](#)
- [Solucionar problemas de integração do Web Application Firewall](#)
- [Solucionar problemas de usuários gerenciados pelo serviço](#)
- [Solução de problemas do AS2](#)

Solução de problemas de autenticação

Esta seção descreve possíveis soluções para os seguintes problemas de autenticação.

Tópicos

- [Falhas de autenticação— SSH/SFTP](#)
- [Problema de realm incompatíveis do AD gerenciado](#)

- [Limites de grupos do Active Directory excedidos](#)
- [Problemas de autenticação diversos](#)
- [Solução de problemas do Amazon API Gateway](#)
- [Solução de problemas ao testar seu provedor de identidade](#)
- [Buckets duplicados do Amazon S3 em um aplicativo web](#)

Falhas de autenticação— SSH/SFTP

Descrição

Quando você tenta se conectar ao seu servidor usando o protocolo de transferência de arquivos (SFTP) Secure Shell (SSH), você recebe uma mensagem semelhante à seguinte:

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
Authentication failed.
```

Note

Se você estiver usando um API Gateway e receber este erro, consulte [Muitas falhas de autenticação](#).

Causa

Como você não adicionou um par de chaves RSA para seu usuário, em vez disso você deve se autenticar usando uma senha.

Solução

Quando executar o comando `sftp`, especifique a opção `-o PubkeyAuthentication=no`. Esta opção força o sistema a solicitar sua senha. Por exemplo:

```
sftp -o PubkeyAuthentication=no sftp-user@server-id.server.transfer.region-id.amazonaws.com
```

Problema de realm incompatíveis do AD gerenciado

Descrição

O realm de um usuário e o realm de seu grupo devem corresponder. Ambos devem estar no realm padrão ou no realm confiável.

Causa

Se um usuário e seu grupo não corresponderem, o usuário não poderá ser autenticado pelo Transfer Family. Se você testar o provedor de identidade para o usuário, receberá o erro Nenhum acesso associado encontrado para grupos de usuários.

Solução

Faça referência a um grupo no realm do usuário que corresponda ao realm do grupo (padrão ou confiável).

Limites de grupos do Active Directory excedidos

Descrição

Ao tentar adicionar mais grupos do Active Directory ao seu AWS Transfer Family servidor, você recebe um erro indicando que atingiu o número máximo de grupos permitido.

Causa

AWS Transfer Family tem um limite padrão de 100 grupos do Active Directory por servidor.

Solução

Essas são duas soluções possíveis:

- Consolide seus grupos do Active Directory para reduzir o número total necessário.
- Se seu caso de uso exigir mais de 100 grupos, considere usar uma solução de provedor de identidade personalizada, conforme descrito em [Simplifique a autenticação do Active Directory com um provedor de identidade personalizado para AWS Transfer Family](#).

Problemas de autenticação diversos

Descrição

Você recebe um erro de autenticação e nenhuma das outras soluções de problemas funciona

Causa

Você pode ter especificado um destino para um diretório lógico que contenha uma barra inicial ou final (/).

Solução

Atualize o destino do diretório lógico para garantir que ele comece com uma barra e não contenha uma barra final. Por exemplo, /amzn-s3-demo-bucket/images é aceitável, mas amzn-s3-demo-bucket/images /amzn-s3-demo-bucket/images/ não é.

Solução de problemas do Amazon API Gateway

Esta seção descreve possíveis soluções para os seguintes problemas do API Gateway.

Tópicos

- [Muitas falhas de autenticação](#)
- [Conexão fechada](#)

Muitas falhas de autenticação

Descrição

Quando você tenta se conectar ao seu servidor usando o protocolo de transferência de arquivos (SFTP) Secure Shell (SSH), você recebe o seguinte erro:

```
Received disconnect from 3.15.127.197 port 22:2: Too many authentication failures
Authentication failed.
Couldn't read packet: Connection reset by peer
```

Causa

Você pode ter inserido uma senha incorreta para o seu usuário. Tente digitar a senha correta novamente.

Se a senha estiver correta, o problema pode ser causado por uma função nome do recurso da Amazon (ARN) que não é válida. Para confirmar se esse é o problema, teste o provedor de identidade do seu servidor. Se você vir uma resposta semelhante à seguinte, o ARN da função é apenas um espaço reservado, conforme indicado pelo valor da ID da função de todos os zeros:

```
{
```

```
"Response": "{ \"Role\": \"arn:aws:iam::000000000000:role/MyUserS3AccessRole\",  
  \"HomeDirectory\": \"/\",  
  \"StatusCode\": 200,  
  \"Message\": \"\",  
  \"Url\": \"https://api-gateway-ID.execute-api.us-east-1.amazonaws.com/prod/  
servers/transfer-server-ID/users/myuser/config\"  
}
```

Solução

Substitua o ARN da função de espaço reservado por uma função real que tenha permissão para acessar o servidor.

Para atualizar a função

1. Abra o CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. No painel de navegação à esquerda, selecione Pilhas.
3. Na lista Pilhas, escolha sua pilha e, em seguida, escolha a guia Parameters (Parâmetros).
4. Selecione Atualizar. Na página Atualizar pilha, escolha Usar modelo atual e, em seguida, escolha Próximo.
5. UserRoleArn Substitua por um ARN de função que tenha permissões suficientes para acessar seu servidor Transfer Family.

Note

Para conceder as permissões necessárias, é possível adicionar as políticas gerenciadas AmazonAPIGatewayAdministrator e AmazonS3FullAccess à sua função.

6. Selecione Próximo e Próximo novamente. Na *stack* página de revisão, selecione Eu reconheço que isso AWS CloudFormation pode criar recursos do IAM e, em seguida, escolha Atualizar pilha.

Conexão fechada

Descrição

Quando você tenta se conectar ao seu servidor usando o protocolo de transferência de arquivos (SFTP) Secure Shell (SSH), você recebe o seguinte erro:

Connection closed

Causa

Uma possível causa para esse problema é que sua função de CloudWatch registro na Amazon não tem uma relação de confiança com a Transfer Family.

Solução

Certifique-se de que a função de registro em log do servidor tenha uma relação de confiança com a Transfer Family. Para obter mais informações, consulte [Estabelecer um relacionamento de confiança](#).

Solução de problemas ao testar seu provedor de identidade

Descrição

Se você testar seu provedor de identidade usando o console ou a operação da TestIdentityProvider API, o Response campo estará vazio. Por exemplo:

```
{
  "Response": "{}",
  "StatusCode": 200,
  "Message": ""
}
```

Causa

A causa mais provável é a falha de autenticação por nome de usuário ou senha incorretos.

Solução

Verifique se você está usando as credenciais corretas para seu usuário e atualize o nome de usuário ou a senha, se necessário.

Buckets duplicados do Amazon S3 em um aplicativo web

Descrição

O mesmo bucket do Amazon S3 aparece várias vezes na interface do aplicativo web Transfer Family.

Causa

Isso ocorre quando um usuário pertence a vários grupos do Active Directory que têm concessões para o mesmo bucket do Amazon S3. O aplicativo web lista todas as concessões de nível superior associadas ao UID ou GID do usuário, incluindo concessões duplicadas para o mesmo local do bucket.

Solução

Para evitar listagens duplicadas, consolide as concessões para que cada usuário tenha apenas uma concessão por local do Amazon S3. Revise sua configuração do Amazon S3 Access Grants e remova concessões redundantes para o mesmo bucket em diferentes grupos do Active Directory.

Solução de problemas do conector SFTP

Esta seção descreve possíveis soluções para problemas com conectores SFTP.

Tópicos

- [Solução de problemas ao adicionar chaves de host confiáveis para seu conector SFTP](#)
- [Falha na negociação chave](#)
- [Limitação do conector SFTP](#)
- [Otimizando o desempenho do conector SFTP](#)
- [Solucionar problemas de conectividade da VPC](#)
- [Problemas diversos do conector SFTP](#)

Solução de problemas ao adicionar chaves de host confiáveis para seu conector SFTP

Descrição

Ao criar ou editar um conector SFTP e adicionar uma chave de host confiável, você recebe o seguinte erro: `Failed to edit connector details (Invalid host key format.)`

Causa

Se você colar uma chave pública correta, o problema pode ser que você incluiu a `comment` parte da chave. AWS Transfer Family atualmente não aceita a parte de comentários da chave.

Solução

Exclua a parte de comentário da chave ao colá-la no campo de texto. Por exemplo, suponha que sua chave seja semelhante ao seguinte:

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

Remova o texto que segue os caracteres == e cole somente na parte da chave até e incluindo o ==.

```
ssh-rsa AAAA...==
```

Falha na negociação chave

Descrição

Você recebe um erro em que a negociação de troca de chaves falha. Por exemplo:

```
Key exchange negotiation failed due to incompatible host key algorithms.  
Client offered: [ecdsa-sha2-nistp256, ecdsa-sha2-nistp384,  
ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256] Server offered: [ssh-rsa]
```

Causa

Este erro ocorre porque não há sobreposição entre os algoritmos de chave do host compatíveis com o servidor e aqueles compatíveis com o conector.

Solução

Certifique-se de que o servidor remoto é compatível com pelo menos um dos algoritmos de chave do host do cliente listados na mensagem de erro. Para a lista dos algoritmos compatíveis, consulte [Políticas de segurança para AWS Transfer Family Conectores SFTP](#).

Limitação do conector SFTP

Descrição

Ao usar conectores SFTP para transferências de arquivos, você encontra erros como:

```
{"type":"ExecutionThrottled","details":{},"connectorId":"c-1234567890abcdef0"}
```

Ou você percebe que as transferências de arquivos estão sendo atrasadas ou falhando de forma intermitente durante operações de alto volume.

Causa

Os conectores SFTP têm cotas de serviço que limitam o número de transferências simultâneas de arquivos e operações de API. Quando esses limites são excedidos, ocorre uma limitação para proteger o serviço e garantir o uso justo em todos os clientes.

Solução

Para resolver os problemas do conector SFTP, tente as seguintes soluções:

1. Implemente a lógica de recuo exponencial e tente novamente em seus aplicativos. Por exemplo, crie uma função que repita automaticamente as operações que falharam com o aumento do tempo de espera entre as tentativas.
2. Implemente a limitação de taxa em seu aplicativo:
 - Limite o número de transferências simultâneas.
 - Adicione atrasos entre lotes de transferências.
3. Monitore seu uso em relação às cotas de serviço:
 - Use CloudWatch métricas para monitorar o uso da API.
 - Configure alarmes para notificá-lo quando se aproximar dos limites da cota.
4. Para obter opções para escalar seus conectores SFTP, consulte [Dimensionando seus conectores SFTP](#)
5. Se a limitação persistir e afetar suas operações comerciais, solicite um aumento de cota por meio do console Service Quotas.

Otimizando o desempenho do conector SFTP

Descrição

As transferências do conector SFTP são mais lentas do que o esperado ou você tem um desempenho inconsistente.

Causa

O desempenho do conector SFTP pode ser afetado por vários fatores, incluindo condições de rede, tamanhos de arquivos, configuração do servidor remoto e limites de transferência simultânea.

Solução

Para otimizar o desempenho do conector SFTP:

- Configure seu servidor SFTP remoto para obter um desempenho ideal:
 - Aumente o máximo de sessões e transferências por sessão
 - Otimize os tamanhos das janelas TCP para conexões de alta latência
 - Use compressão se suportada por ambas as extremidades
- Considere a otimização da rede colocando o conector Transfer Family em uma região próxima ao seu servidor SFTP remoto.
- Implemente uma estratégia de monitoramento para identificar gargalos de desempenho:
 - Monitore a taxa de transferência e a latência da rede
 - Analise os registros em busca de padrões em transferências lentas

Solucionar problemas de conectividade da VPC

Esta seção descreve soluções para problemas comuns com conectores VPC_ LATTICE-enabled SFTP.

Conector travado no status PENDENTE

Descrição

Seu conector VPC_ LATTICE-enabled SFTP permanece no PENDING status por um longo período (mais de 10 minutos).

Causa

Isso pode ocorrer devido a atrasos na resolução de DNS, problemas de configuração do Resource Gateway ou problemas de associação de rede de serviços VPC Lattice.

Solução

Entre AWS Support em [contato em Contact AWS](#) para ajudar a analisar a causa raiz do problema. Você também pode tentar a seguinte solução alternativa.

1. Verifique se o Resource Gateway está no ACTIVE status:

```
aws vpc-lattice get-resource-gateway --resource-gateway-  
identifier rgw-1234567890abcdef0
```

2. Verifique se a configuração do recurso está configurada e ativa corretamente:


```
aws vpc-lattice get-resource-configuration --resource-configuration-  
identifier rcfg-1234567890abcdef0
```

3. Certifique-se de que seu Resource Gateway tenha sub-redes em pelo menos duas zonas de disponibilidade compatíveis com o VPC Lattice.
4. Se o problema persistir, exclua e recrie o conector com a mesma configuração.

Conector com status ERRADO

Descrição

Seu conector VPC_ LATTICE-enabled SFTP mostra o ERRORRED status com detalhes do erro.

Causa

As causas comuns incluem ARN de configuração de recursos inválido, endereços IP insuficientes em sub-redes VPC ou tentativas de compartilhamento de recursos entre regiões.

Solução

1. Verifique os detalhes do erro usando `describe-connector`:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

2. Verifique se o ARN da configuração do recurso está correto e na mesma região do seu conector.
3. Certifique-se de que suas sub-redes VPC tenham endereços IP disponíveis suficientes para o Resource Gateway.
4. Verifique se o destino da configuração de recursos (endereço IP ou nome DNS) pode ser acessado pela sua VPC.

Erro de endereço IP público não suportado

Descrição

Você recebe um erro ao tentar criar uma configuração de recursos com um endereço IP público:
`ValidationException: IP address x.x.x.x is not in allowed ranges.`

Causa

As configurações de recursos para endpoints públicos devem usar nomes DNS, não endereços IP.

Solução

Use o nome DNS público do seu servidor SFTP em vez do endereço IP ao criar a Configuração de Recursos:

```
aws vpc-lattice create-resource-configuration \
  --name my-public-server-config \
  --resource-gateway-identifier rgw-1234567890abcdef0 \
  --resource-configuration-definition dnsResource={domainName="my.sftp.server.com"} \
  --port-ranges 22
```

Erro na zona de disponibilidade não suportada

Descrição

Você recebe um erro ao criar um Resource Gateway: Subnet subnet-xxx is not valid because it is not in a supported Availability Zone.

Causa

Nem todas as zonas de disponibilidade oferecem suporte ao VPC Lattice Cross-VPC Resource Access. A mensagem de erro lista as AZs suportadas em sua região.

Solução

1. Crie sub-redes nas zonas de disponibilidade suportadas listadas na mensagem de erro.
2. Atualize seu Resource Gateway para usar sub-redes somente de AZs compatíveis.
3. Certifique-se de ter pelo menos duas sub-redes em diferentes AZs compatíveis.

Tempos limite de conexão com conectores VPC_LATTICE

Descrição

As transferências de arquivos por meio de conectores VPC atingem o tempo limite ou falham de forma intermitente.

Causa

O VPC Lattice tem limites de conexão (350 conexões por recurso) e tempos limite de inatividade (350 segundos para TCP).

Solução

1. Monitore as conexões simultâneas para permanecer dentro do limite de 350 conexões por recurso.
2. Implemente o agrupamento de conexões e a reutilização em seus aplicativos.
3. Configure os valores de tempo limite apropriados em seus aplicativos cliente SFTP (menos de 350 segundos).
4. Considere criar várias configurações de recursos para o mesmo destino para distribuir a carga.

Problemas diversos do conector SFTP

Descrição

Você recebe um erro após a execução `StartFileTransfer`, mas não sabe a causa do problema, e somente a ID do conector é retornada após a chamada da API.

Causa

Esse erro pode ter várias causas. Para solucionar o problema, recomendamos que você teste seu conector e pesquise seus CloudWatch registros.

Solução

- Teste seu conector: Veja [Testar um conector SFTP](#). Se o teste falhar, o sistema enviará uma mensagem de erro com base no motivo pelo qual o teste falhou. Essa seção descreve como testar seu conector no console ou usando o comando da [TestConnection](#) API.
- Visualize CloudWatch os registros do seu conector: Veja [Exemplo de entradas de registro para conectores SFTP](#). Este tópico fornece exemplos de entradas de log do conector SFTP e a convenção de nomenclatura para ajudá-lo a encontrar os registros apropriados.

Solucionar problemas de conectividade e transferência de SFTP

Esta seção descreve possíveis soluções para problemas de conectividade SFTP e transferência de arquivos.

Tópicos

- [Solucionar problemas de conectividade SFTP](#)
- [Solucionar problemas do cliente SFTP](#)
- [Solução de problemas de upload de arquivos](#)

- [Solucionar problemas do conector SFTP do tipo de saída VPC](#)

Solucionar problemas de conectividade SFTP

Descrição

Seu cliente SFTP não pode iniciar a conexão. Esse problema pode ocorrer de forma contínua ou intermitente. Por exemplo, você pode ver a seguinte sequência de eventos nos registros de depuração do cliente SFTP:

```
sftp -vvv username@1.1.1.1
.....
debug1: Local version string .....
kex_exchange_identification: read: Connection reset by peer
Connection reset by 1.1.1.1 port 22
Connection closed.
```

Causa

Há um caso extremo em que o TCP ACK de zero bytes (ACK sem dados), também conhecido como handshake de três vias, é descartado ou atrasado.

Solução

Como solução alternativa, o Transfer Family oferece uma solução que usa uma configuração diferente para resolver esse problema, mas pode causar problemas de compatibilidade com clientes mais antigos. Por esse motivo, essa solução está disponível somente na porta 2223.

No procedimento para criar um servidor Transfer Family em uma VPC ([Crie um servidor em uma VPC \(virtual private cloud\)](#)), ao especificar um grupo de segurança, configure o tráfego SSH para usar a porta 2223.

Solucionar problemas do cliente SFTP

As mensagens do lado do cliente SFTP são descritas em [Mensagens SFTP](#). A melhor maneira de solucionar problemas do cliente SFTP é verificar os registros do cliente SFTP e, se necessário, entrar em contato com o administrador da rede.

Solução de problemas de upload de arquivos

Esta seção descreve possíveis soluções para os seguintes problemas de carregamento de arquivos.

Tópicos

- [Solução de problemas de upload de arquivos do Amazon S3](#)
- [Solução de problemas de arquivos ilegíveis](#)

Solução de problemas de upload de arquivos do Amazon S3

Descrição

Ao tentar fazer upload de um arquivo para o armazenamento do Amazon S3 usando o Transfer Family, você recebe a seguinte mensagem de erro: A AWS Transfer não é compatível com gravações de acesso aleatório em objetos do S3.

Causa

Quando você usa o Amazon S3 para o armazenamento do seu servidor, o Transfer Family não é compatível a várias conexões para uma única transferência.

Solução

Se o seu servidor do Transfer Family estiver usando o Amazon S3 para armazenamento, desative todas as opções do seu software cliente que mencionem o uso de várias conexões para uma única transferência.

Solução de problemas de arquivos ilegíveis

Descrição

Você vê nomes de arquivos corrompidos em alguns dos arquivos enviados. Às vezes, os usuários encontram problemas com transferências por FTP e SFTP que distorcem certos caracteres nos nomes dos arquivos, como tremas, letras com acento ou certos scripts, como chinês ou árabe.

Causa

Embora os protocolos FTP e SFTP possam permitir que a codificação de caracteres dos nomes dos arquivos seja negociada pelos clientes, o Amazon S3 e o Amazon EFS não fazem isso. Em vez disso, eles exigem codificação de UTF-8 caracteres. Como resultado, certos caracteres não são renderizados corretamente.

Solução

Para resolver esse problema, revise seu aplicativo cliente quanto à codificação de caracteres do nome do arquivo e verifique se ela está definida como UTF-8.

Solucionar problemas do conector SFTP do tipo de saída VPC

Se você estiver enfrentando problemas com conectores SFTP do tipo de saída VPC, verifique o seguinte:

O status do conector é PENDENTE

Descrição

Seu conector do tipo de saída VPC permanece no status PENDENTE por vários minutos após a criação e TestConnection retorna “Conector não disponível”.

Causa

A resolução de DNS para conectores VPC pode levar vários minutos para ser concluída após a criação.

Solução

Aguarde até que o status do conector se torne ATIVO antes de tentar transferir arquivos. Esse é um comportamento normal para conectores do tipo de saída VPC.

Tempos limite de conexão

Descrição

Seu conector do tipo de saída VPC expira ao tentar se conectar ao servidor SFTP.

Causa

Grupos de segurança podem não permitir tráfego na porta 22 entre as sub-redes do Resource Gateway e o servidor SFTP de destino.

Solução

Verifique se os grupos de segurança permitem tráfego na porta 22 entre as sub-redes do Resource Gateway e o servidor SFTP de destino.

Erros de configuração de recursos

Descrição

Seu conector do tipo de saída VPC não consegue se conectar devido a problemas de configuração de recursos.

Causa

A configuração de recursos pode apontar para um endereço IP ou nome DNS incorreto, ou o Resource Gateway pode não estar na mesma VPC do seu servidor SFTP (para endpoints privados).

Solução

Certifique-se de que sua configuração de recursos aponte para o endereço IP ou nome DNS correto e que o Resource Gateway esteja na mesma VPC do seu servidor SFTP (para endpoints privados). Consulte mais informações em [Resource configurations](#) no Guia do usuário da Amazon VPC Lattice.

Problemas de endpoints públicos

Descrição

Seu conector do tipo de saída VPC não pode se conectar a endpoints SFTP públicos.

Causa

Para endpoints públicos, você deve usar um nome DNS (não um endereço IP) em sua configuração de recursos, e sua VPC deve ter um gateway NAT para acesso de saída à Internet.

Solução

Verifique se você está usando um nome DNS, não um endereço IP, em sua configuração de recursos. Verifique se sua VPC tem um gateway NAT para acesso externo à Internet.

Problemas com a zona de disponibilidade

Descrição

Você não pode criar um Resource Gateway devido às limitações da Zona de Disponibilidade.

Causa

Os Resource Gateways exigem sub-redes em pelo menos duas zonas de disponibilidade, e nem todas as AZs oferecem suporte ao VPC Lattice.

Solução

Verifique as zonas de disponibilidade compatíveis com o VPC Lattice em sua região e garanta que você tenha sub-redes em pelo menos duas AZs compatíveis.

Solucionar problemas de provedores de identidade personalizados

Esta seção descreve possíveis soluções para problemas relacionados aos provedores de identidade personalizados com o Transfer Family.

Tópicos

- [Solucionar erros de integração do API Gateway](#)
- [Solucionar problemas de tempo limite da função Lambda](#)
- [Solucione problemas consistentes de tempo limite do Lambda](#)
- [Solucionar problemas de exceções KeyError](#)

Solucionar erros de integração do API Gateway

Descrição

Os usuários não podem se autenticar com seu servidor Transfer Family e, ao testar seu provedor de identidade, você vê erros como:

```
{
  "Response": "",
  "StatusCode": 500,
  "Message": "Internal server error"
}
```

Causa

Erros de integração do API Gateway podem ocorrer devido a:

- Configuração incorreta do API Gateway
- Erros da função Lambda que não estão sendo tratados adequadamente
- Problemas de permissão entre o API Gateway e o Lambda
- Respostas malformadas da função Lambda

Solução

Para solucionar erros de integração do API Gateway:

1. Verifique seus registros de funções do Lambda para obter informações detalhadas sobre erros:

- No CloudWatch console, navegue até Grupos de registros >/aws/lambda/your-function-name
- Procure mensagens de erro ou rastreamentos de pilha que indiquem a causa raiz

2. Verifique se sua função Lambda retorna respostas formatadas corretamente:

```
{
  "Role": "arn:aws:iam::123456789012:role/TransferUserRole",
  "HomeDirectory": "/mybucket/home/username"
}
```

3. Ative o CloudWatch registro detalhado para o API Gateway:

- No console do API Gateway, selecione sua API e escolha Estágios
- Selecione seu estágio e Logs/Tracing, em seguida, habilite CloudWatch Registros
- Defina o nível do registro como ERROR ou INFO

4. Teste seu endpoint do API Gateway diretamente:

```
curl -X POST https://your-api-id.execute-api.region.amazonaws.com/prod/servers/your-server-id/users/username/config \
  -H "Content-Type: application/json" \
  -d '{"Password": "password"}'
```

5. Verifique as permissões entre o API Gateway e o Lambda:

- Certifique-se de que o API Gateway tenha permissão para invocar sua função Lambda
- Verifique se a função de execução da sua função Lambda tem as permissões necessárias

Solucionar problemas de tempo limite da função Lambda

Descrição

Quando os usuários tentam se autenticar com seu servidor Transfer Family usando um provedor de identidade personalizado, eles enfrentam longos atrasos seguidos por falhas de autenticação. Em seus registros do Lambda, você vê erros de tempo limite.

Causa

As funções Lambda usadas para provedores de identidade personalizados têm um tempo limite padrão de 3 segundos. Se sua lógica de autenticação demorar mais do que esse tempo limite (por exemplo, ao consultar bancos de dados externos ou fazer chamadas de API para provedores de identidade terceirizados), a função atingirá o tempo limite e a autenticação falhará.

Solução

Para resolver problemas de tempo limite do Lambda:

1. Aumente o tempo limite da função Lambda:

- No console Lambda, navegue até sua função e selecione a guia Configuração
- Em Configuração geral, clique em Editar
- Aumente o valor do tempo limite (recomenda-se até 15 segundos para funções de autenticação)

2. Otimize seu código de função Lambda:

- Use o pool de conexões para consultas ao banco de dados
- Implemente o armazenamento em cache para dados acessados com frequência
- Minimize as chamadas externas de API durante a autenticação

3. Considere usar o Lambda Provisioned Concurrency para eliminar inícios a frio:

```
aws lambda put-provisioned-concurrency-config \  
  --function-name my-authentication-function \  
  --qualifier prod \  
  --provisioned-concurrent-executions 5
```

4. Monitore o desempenho do Lambda usando CloudWatch métricas e configure alarmes para limites de duração

Solucione problemas consistentes de tempo limite do Lambda

Descrição

Os usuários experimentam tempos limite consistentes ao usar uma função Lambda para autenticação.

Causa

O Lambda não consegue acessar o AWS serviço correspondente usado para autenticação (como DynamoDB, Secrets Manager ou outro provedor de identidade).

Solução

Verifique se as sub-redes podem alcançar AWS os serviços. Ou, se estiver se conectando a um provedor de identidade da Internet (como Okta), verifique se a sub-rede da função Lambda pode acessar a Internet por meio de um gateway NAT

Solucionar problemas de exceções **KeyError**

Descrição

Em suas entradas de registro do Transfer Family, você nota as exceções `KeyError` ".

Causa

A causa mais provável é que o usuário ou `identity_provider` registro esteja mal formado ou que faltem campos obrigatórios.

Solução

Examine o `ERRORS` registro, localizado no grupo de `/aws/transfer/your-server-id` registros, em busca de pistas.

Solucionar problemas de fluxo de trabalho

Esta seção descreve possíveis soluções para problemas com fluxos de trabalho gerenciados.

Tópicos

- [Solução de problemas de fluxos de trabalho gerenciados](#)
- [Solução de problemas de decodificação do fluxo de trabalho](#)

Solução de problemas de fluxos de trabalho gerenciados

Esta seção descreve possíveis soluções para os seguintes problemas de fluxo de trabalho.

Tópicos

- [Solucione erros relacionados ao fluxo de trabalho usando a Amazon CloudWatch](#)
- [Solução de problemas de cópia do fluxo de trabalho](#)

Solucione erros relacionados ao fluxo de trabalho usando a Amazon CloudWatch

Descrição

Se você está tendo problemas com seus fluxos de trabalho, você pode usar CloudWatch a Amazon para investigar a causa.

Causa

Pode haver várias causas. Use o Amazon CloudWatch Logs para investigar.

Solução

Transfer Family emite o status de execução do fluxo de trabalho para o CloudWatch Logs. Os seguintes tipos de erros de fluxo de trabalho podem aparecer nos CloudWatch registros:

- "type": "StepErrored"
- "type": "ExecutionErrored"
- "type": "ExecutionThrottled"
- "Service failure on starting workflow"

Você pode filtrar os registros em logs de execução do seu fluxo de trabalho usando diferentes sintaxes de filtros e padrões. Por exemplo, você pode criar um filtro de registro em seus CloudWatch registros para capturar registros de execução do fluxo de trabalho que contenham a ExecutionErrored mensagem. Para obter detalhes, consulte o [Real-time processamento de dados de log com assinaturas](#) e a [sintaxe de filtros e padrões](#) no Guia do usuário do Amazon CloudWatch Logs.

StepErrored

```
2021-10-29T12:57:26.272-05:00
    {"type":"StepErrored","details":
{"errorType":"BAD_REQUEST","errorMessage":"Cannot
tag Efs file","stepType":"TAG","stepName":"successful_tag_step"},
"workflowId":"w-
abcdef01234567890","executionId":"1234abcd-56ef-78gh-90ij-1234klmno567",
"transferDetails":
{"serverId":"s-1234567890abcdef0","username":"lhr","sessionId":"1234567890abcdef0"}}
```

Aqui, StepErrored indica que uma etapa no fluxo de trabalho gerou um erro. Em um único fluxo de trabalho, você pode ter várias etapas configuradas. Este erro informa em qual etapa o erro ocorreu e fornece uma mensagem de erro. Neste exemplo específico, a etapa foi configurada para marcar um arquivo; no entanto, a marcação de um arquivo em um sistema de arquivos do Amazon EFS não é compatível, então a etapa gerou um erro.

ExecutionErrored

```
2021-10-29T12:57:26.618-05:00
    {"type":"ExecutionErrored","details":{},"workflowId":"w-w-
abcdef01234567890",
    "executionId":"1234abcd-56ef-78gh-90ij-1234klmno567","transferDetails":
{"serverId":"s-1234567890abcdef0",
    "username":"lhr","sessionId":"1234567890abcdef0"}}
```

Quando o fluxo de trabalho não consegue executar nenhuma etapa, ele gera uma mensagem `ExecutionErrored`. Por exemplo, se você configurou uma única etapa em um determinado fluxo de trabalho e se a etapa não puder ser executada, o fluxo de trabalho geral falhará.

Executionthrottled

A execução tem controle de utilização se um fluxo de trabalho estiver sendo acionado em uma taxa mais rápida do que o sistema pode suportar. Esta mensagem de registro em log indica que você deve diminuir a taxa de execução dos fluxos de trabalho. [Se você não conseguir reduzir a taxa de execução do fluxo de trabalho, entre em contato em Contato AWS Support . AWS](#)

Falha de serviço ao iniciar o fluxo de trabalho

Sempre que você remove um fluxo de trabalho de um servidor e o substitui por um novo ou atualiza a configuração do servidor (o que afeta a função de execução de um fluxo de trabalho), você deve esperar aproximadamente 10 minutos antes de executar o novo fluxo de trabalho. O servidor do Transfer Family armazena em cache os detalhes do fluxo de trabalho e leva 10 minutos para que o servidor atualize o cache.

Além disso, você deve sair de qualquer sessão ativa de SFTP e, em seguida, fazer login novamente após o período de espera de 10 minutos para ver as alterações.

Solução de problemas de cópia do fluxo de trabalho

Descrição

Se você estiver executando um fluxo de trabalho que contém uma etapa para copiar o arquivo carregado, poderá encontrar o seguinte erro:

```
{
  "type": "StepErrored", "details": {
    "errorType": "BAD_REQUEST", "errorMessage": "Bad Request (Service: Amazon S3;
    Status Code: 400; Error Code: 400 Bad Request;
```

```
Request ID: request-ID; S3 Extended Request ID: request-ID Proxy: null)",
"stepType": "COPY", "stepName": "copy-step-name" },
"workflowId": "workflow-ID",
"executionId": "execution-ID",
"transferDetails": {
  "serverId": "server-ID",
  "username": "user-name",
  "sessionId": "session-ID"
}
}
```

Causa

O arquivo de origem está em um bucket do Amazon S3 que está em um bucket Região da AWS diferente do bucket de destino.

Solução

Se você estiver executando um fluxo de trabalho que inclua uma etapa de cópia, verifique se os buckets de origem e destino estão na mesma Região da AWS.

Solução de problemas de decodificação do fluxo de trabalho

Esta seção descreve possíveis soluções para os seguintes problemas com fluxos de trabalho criptografados.

Tópicos

- [Solucionar problemas de criptografia de destinatários anônimos](#)
- [Solucionar erro do arquivo de criptografia assinado](#)
- [Solucionar erros de um algoritmo FIPS](#)

Solucionar problemas de criptografia de destinatários anônimos

Descrição

Seu fluxo de trabalho de descriptografia falha ao processar determinados arquivos criptografados, mas funciona com outros.

Causa

Os arquivos podem ter sido criptografados sem especificar um destinatário (criptografia anônima), dificultando que o fluxo de trabalho determine qual chave usar para a descriptografia.

Solução

Sempre criptografe arquivos com um destinatário não anônimo usando o `-r` parâmetro. Por exemplo:

```
gpg -e -r user@example.com --openpgp file.txt
```

Para verificar se um arquivo foi criptografado com um destinatário específico ou anonimamente, use o `--list-packets` comando:

```
gpg --list-packets file.txt.gpg
```

Esse comando exibe a estrutura do pacote do GPG-encrypted arquivo sem descriptografar seu conteúdo. Procure uma saída que inclua informações do destinatário, como:

```
:pubkey enc packet: version 3, algo 1, keyid 1A2B3C4D5E6F7G8H
```

Se você ver informações de `keyid`, o arquivo foi criptografado para um destinatário específico. Se essas informações estiverem ausentes, o arquivo pode ter sido criptografado anonimamente, o que pode causar falhas de decodificação nos fluxos de trabalho do Transfer Family.

Você também pode usar esse comando para verificar:

- Quais algoritmos de criptografia foram usados
- Métodos de compressão (se houver)
- Carimbos de data e hora de criação

Para ver a lista de algoritmos de criptografia compatíveis com sua instalação do GPG, use:

```
gpg --version
```

Essas informações podem ajudá-lo a garantir que você esteja usando algoritmos de criptografia compatíveis com os fluxos de trabalho da Transfer Family, especialmente quando a conformidade com o FIPS é necessária.

Solucionar erro do arquivo de criptografia assinado

Descrição

Seu fluxo de trabalho de descryptografia falha e você recebe o seguinte erro:

```
"Encrypted file with signed message unsupported"
```

Causa

Atualmente, o Transfer Family não oferece suporte à assinatura de arquivos criptografados.

Solução

No seu cliente PGP, se houver uma opção para assinar o arquivo criptografado, certifique-se de limpar a seleção, pois o Transfer Family atualmente não oferece suporte à assinatura de arquivos criptografados.

Solucionar erros de um algoritmo FIPS

Descrição

Seu fluxo de trabalho de descryptografia falha, e a mensagem de registro em log é semelhante à seguinte:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "File encryption algorithm not supported with FIPS mode
enabled.",
    "stepType": "DECRYPT",
    "stepName": "step-name"
  },
  "workflowId": "workflow-ID",
  "executionId": "execution-ID",
  "transferDetails": {
    "serverId": "server-ID",
    "username": "user-name",
    "sessionId": "session-ID"
  }
}
```



```
}
```

Causa

Seu servidor do Transfer Family tem o modo FIPS ativado e uma etapa de fluxo de trabalho de criptografia associada. Ao criptografar os arquivos antes de fazer upload para o servidor do Transfer Family, o cliente de criptografia pode gerar arquivos criptografados que usam algoritmos de criptografia simétrica não aprovados pelo FIPS. Nesse cenário, o fluxo de trabalho não consegue criptografar arquivos. No exemplo a seguir, a versão 2.4.0 do GnuPG está usando OCB (um modo de criptografia de bloco não FIPS) para criptografar arquivos: isso faz com que o fluxo de trabalho falhe.

Solução

Você deve editar a chave GPG usada para criptografar seus arquivos e, em seguida, criptografá-los novamente. O procedimento a seguir descreve as etapas que você precisa realizar.

Para editar suas chaves PGP

1. Identifique a chave que você deve editar executando `gpg --list-keys`

Isso retorna uma lista de chaves. Cada chave tem detalhes semelhantes aos seguintes:

```
pub   ed25519 2022-07-07 [SC]
       wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
uid           [ultimate] Mary Major <marymajor@example.com>
sub    cv25519 2022-07-07 [E]
```

2. Identifique a chave que você deseja editar. No exemplo mostrado na etapa anterior, a ID é `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.
3. Executar `gpg --edit-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.

O sistema responde com detalhes sobre o programa GnuPG e a chave especificada.

4. No prompt `gpg>`, insira `showpref`. Os detalhes a seguir são retornados:

```
[ultimate] (1). Mary Major <marymajor@example.com>
Cipher: AES256, AES192, AES, 3DES
AEAD: OCB
Digest: SHA512, SHA384, SHA256, SHA224, SHA1
Compression: ZLIB, BZIP2, ZIP, Uncompressed
```

```
Features: MDC, AEAD, Keyserver no-modify
```

Observe que os algoritmos preferenciais armazenados na chave estão listados.

- Queremos editar a chave para reter todos os algoritmos, exceto o OCB. Execute o comando `setpref`, especificando todos os algoritmos a serem retidos:

```
gpg> setpref AES256, AES192, AES, 3DES, SHA512, SHA384, SHA256, SHA224, SHA1, ZLIB,
BZIP2, ZIP, Uncompressed
```

Isso retorna os seguintes detalhes:

```
Set preference list to:
  Cipher: AES256, AES192, AES, 3DES
  AEAD:
  Digest: SHA512, SHA384, SHA256, SHA224, SHA1
  Compression: ZLIB, BZIP2, ZIP, Uncompressed
  Features: MDC, Keyserver no-modify
Really update the preferences? (y/N)
```

- Digite `y` para atualizar e, em seguida, insira sua senha quando solicitado a confirmar a alteração.
- Salve as alterações.

```
gpg> save
```

Antes de executar novamente seu fluxo de trabalho de descryptografia, você deve criptografar novamente seus arquivos usando a chave editada.

Solucionar problemas do EFS

Esta seção descreve possíveis soluções para problemas com o armazenamento do Amazon EFS.

Tópicos

- [Solução de problemas do Amazon EFS](#)

Solução de problemas do Amazon EFS

Esta seção descreve possíveis soluções para os seguintes problemas do Amazon EFS.

Tópicos

- [Solução de problemas de usuários gerenciados por serviços do Amazon EFS](#)
- [Solução de problemas do perfil POSIX ausente](#)
- [Solução de problemas de diretórios lógicos com o Amazon EFS](#)

Solução de problemas de usuários gerenciados por serviços do Amazon EFS

Descrição

Você executa o comando `sftp` e o prompt não aparece e, no lugar, você vê a seguinte mensagem:

```
Couldn't canonicalize: Permission denied
Need cwd
```

Causa

A função do seu usuário AWS Identity and Access Management (IAM) não tem permissão para acessar o Amazon Elastic File System (Amazon EFS).

Solução

Aumente as permissões da política para o perfil do seu usuário. Você pode adicionar uma política AWS gerenciada, como `AmazonElasticFileSystemClientFullAccess`.

Solução de problemas do perfil POSIX ausente

Descrição

Se você estiver usando o armazenamento Amazon EFS para seu servidor e estiver usando um provedor de identidade personalizado, deverá fornecer à sua AWS Lambda função um perfil POSIX.

Causa

Uma possível causa é que os modelos que fornecemos para criar um método Amazon API Gateway baseado no AWS Lambda no momento não contêm informações POSIX.

Se você forneceu informações POSIX, o formato usado para fornecer as informações POSIX pode não estar sendo analisado corretamente pelo Transfer Family.

Solução

Certifique-se de fornecer um elemento JSON ao Transfer Family para o parâmetro PosixProfile.

Por exemplo, se você estiver usando Python, você pode adicionar a seguinte linha onde você analisa o parâmetro PosixProfile:

```
if PosixProfile:
    response_data["PosixProfile"] = json.loads(PosixProfile)
```

Ou, em JavaScript, você pode adicionar a seguinte linha, onde *uid-value* e *gid-value* são números inteiros, 0 ou maiores, que representam o ID do usuário (UID) e o ID do grupo (GID), respectivamente:

```
PosixProfile: {"Uid": uid-value, "Gid": gid-value},
```

Estes exemplos de código enviam o parâmetro PosixProfile para o Transfer Family como um objeto JSON, em vez de uma string.

Além disso, dentro AWS Secrets Manager, você deve armazenar o PosixProfile parâmetro da seguinte forma. Substitua *your-uid* e *your-gid* por seus valores reais para o GID e o UID.

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

Solução de problemas de diretórios lógicos com o Amazon EFS

Descrição

Se o diretório inicial do usuário não existir e ele executar um comando `ls`, o sistema responderá da seguinte forma:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Causa

Se o seu servidor do Transfer Family usa o Amazon EFS, o diretório inicial do usuário deve ser criado com acesso de leitura e gravação antes que o usuário possa trabalhar em seu diretório inicial

lógico. O usuário não pode criar esse diretório sozinho, pois não teria permissões para `mkdir` em seu diretório inicial lógico.

Solução

Um usuário com acesso administrativo ao diretório pai precisa criar o diretório inicial lógico do usuário.

Solucionar problemas de armazenamento e criptografia

Esta seção descreve possíveis soluções para problemas de armazenamento e criptografia.

Tópicos

- [Solução de problemas de políticas para buckets criptografados do Amazon S3](#)
- [Solução de problemas de exceção `ResourceNotFound`](#)

Solução de problemas de políticas para buckets criptografados do Amazon S3

Descrição

Você tem um bucket criptografado do Amazon S3 que está usando como armazenamento para o seu servidor do Transfer Family. Se você tentar fazer upload de um arquivo para o servidor, receberá o erro `Couldn't close file: Permission denied`.

E se visualizar os registros em log do servidor, você verá os seguintes erros:

```
ERROR Message="Access denied" Operation=CLOSE Path=/bucket/user/test.txt BytesIn=13
ERROR Message="Access denied"
```

Causa

A política do seu usuário do IAM não tem permissão para acessar o bucket criptografado.

Solução

Você deve especificar permissões adicionais em sua política para conceder as permissões AWS Key Management Service (AWS KMS) necessárias. Para obter detalhes, consulte [Proteção e criptografia de dados](#).

Solução de problemas de exceção **ResourceNotFound**

Descrição

Você recebe um erro em que o recurso não pode ser encontrado. Por exemplo, se você executar `UpdateServer`, poderá receber o seguinte erro:

```
An error occurred (ResourceNotFoundException) when calling the UpdateServer operation:  
Unknown server
```

Causa

Há vários motivos para receber uma `ResourceNotFoundException` mensagem. Na maioria dos casos, o recurso que você especificou no comando da API não existe. Se você especificou um recurso existente, a causa mais provável é que sua região padrão seja diferente da região do seu recurso. Por exemplo, se sua região padrão for `us-east-1` e seu servidor do Transfer Family estiver em `us-east-2`, você receberá uma exceção `Unknown resource` (Recurso desconhecido).

Para obter detalhes sobre como definir uma região padrão, consulte [Configuração rápida com o aws configure](#).

Solução

Adicione um parâmetro de região ao comando da API para especificar explicitamente onde encontrar um recurso específico.

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

Solucionar problemas de monitoramento e alerta

Esta seção fornece informações sobre como solucionar problemas de monitoramento e alerta AWS Transfer Family, incluindo CloudWatch métricas ausentes ou incompletas e EventBridge eventos ausentes.

Tópicos

- [Solucionar problemas de métricas ausentes ou incompletas CloudWatch](#)
- [Solucionar problemas de eventos ausentes EventBridge](#)

Solucionar problemas de métricas ausentes ou incompletas CloudWatch

Descrição

CloudWatch as métricas dos seus servidores Transfer Family estão ausentes, incompletas ou não estão sendo atualizadas conforme o esperado.

Causa

Métricas ausentes ou incompletas podem ser causadas por vários fatores:

- Problemas de configuração de registro
- Baixos níveis de atividade que não geram métricas dentro do prazo esperado
- Visualização de métricas com dimensões ou intervalos de tempo incorretos

Solução

Para resolver problemas com CloudWatch métricas ausentes ou incompletas:

1. Certifique-se de que o registro esteja configurado corretamente para seu servidor Transfer Family:
 - No console Transfer Family, verifique se o registro está ativado em Detalhes do servidor > Detalhes adicionais > Função de registro.
 - É muito provável que a função de registro tenha as permissões e relações de confiança necessárias.
2. Ao visualizar métricas no CloudWatch console:
 - Use as dimensões corretas, por exemplo, `ServerId` para métricas em nível de servidor
 - Ajuste o intervalo de tempo para garantir que ele cubra os períodos de atividade
 - Verifique se você está no correto Região da AWS
3. Gere atividades de teste em seu servidor Transfer Family para garantir que as métricas sejam produzidas.

Solucionar problemas de eventos ausentes EventBridge

Descrição

Você configurou EventBridge as regras da Amazon para capturar eventos do Transfer Family, mas os eventos não estão sendo entregues aos seus destinos de destino nem acionando as ações esperadas.

Causa

EventBridge Eventos ausentes podem ser causados por:

- Padrões de eventos configurados incorretamente
- Problemas de permissão com alvos de eventos
- Limites de serviço ou limitação
- Eventos que não estão sendo gerados devido à configuração do servidor

Solução

Para solucionar problemas de EventBridge eventos ausentes:

1. Verifique se o padrão do evento está formatado corretamente para corresponder aos eventos do Transfer Family:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["Transfer State Change"],
  "detail": {
    "serverId": ["s-1234567890abcdef0"]
  }
}
```

2. Verifique se o destino do seu evento tem as permissões necessárias:

- Para destinos Lambda, certifique-se de que a política de recursos da função Lambda permita invocá-la EventBridge
- Para destinos SQS, verifique se a política de fila permite EventBridge enviar mensagens
- Para destinos do SNS, confirme se a política de tópicos permite EventBridge publicar nele

3. Teste sua regra gerando exemplos de eventos:

- Use o EventBridge console para criar um evento de teste que corresponda ao seu padrão
- Execute ações em seu servidor Transfer Family que devem gerar eventos

4. Ative as métricas de EventBridge regras para monitorar invocações e falhas de regras:


```
aws events put-rule --name "TransferStateChangeRule" --event-pattern '{...}' --state
ENABLED --metrics-enabled
```

5. Verifique CloudWatch os registros para ver se há mensagens de erro relacionadas a falhas na entrega de eventos

Solucionar problemas de transferência entre regiões

Esta seção descreve possíveis soluções para problemas relacionados à transferência de arquivos. Regiões da AWS

Tópicos

- [Solucionar problemas de permissão de transferência entre regiões](#)
- [Solucionar problemas de desempenho de transferência entre regiões](#)

Solucionar problemas de permissão de transferência entre regiões

Descrição

Ao tentar transferir arquivos entre buckets do Amazon S3 em diferentes regiões usando fluxos de trabalho do Transfer Family, você encontra erros como:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "Access Denied (Service: Amazon S3; Status Code: 403; Error Code:
AccessDenied)",
    "stepType": "COPY",
    "stepName": "cross_region_copy"
  }
}
```

Causa

Cross-region as transferências exigem permissões específicas do IAM para os buckets de origem e destino. A função do IAM usada pelo servidor ou fluxo de trabalho do Transfer Family pode não ter permissões suficientes para acessar buckets em outras regiões.

Solução

Para resolver problemas de permissão de transferência entre regiões:

1. Certifique-se de que sua função do IAM tenha permissões para os buckets de origem e destino:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::source-bucket-name/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::destination-bucket-name/*"
    }
  ]
}
```

2. Se estiver usando a criptografia KMS, adicione permissões para as chaves KMS de origem e de destino:

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": [
    "arn:aws:kms:source-region:account-id:key/source-key-id",
    "arn:aws:kms:destination-region:account-id:key/destination-key-id"
  ]
}
```

3. Verifique se as políticas de bucket em ambas as regiões permitem o acesso a partir da função IAM do seu servidor Transfer Family
4. Para transferências entre contas, certifique-se de que as permissões corretas entre contas estejam configuradas

Solucionar problemas de desempenho de transferência entre regiões

Descrição

Cross-region as transferências são significativamente mais lentas do que o esperado ou expiram durante transferências de arquivos grandes.

Causa

Cross-region as transferências envolvem inerentemente maior latência e podem ser afetadas pelas condições da rede, pelos tamanhos dos arquivos e pelos limites do serviço. Arquivos grandes ou grandes volumes de arquivos pequenos podem sofrer degradação do desempenho.

Solução

Para melhorar o desempenho da transferência entre regiões:

- Para arquivos grandes, considere usar o Amazon S3 Transfer Acceleration:

```
aws s3 cp --source-region us-east-1 --region us-west-2 \  
s3://source-bucket/large-file.zip s3://destination-bucket/large-file.zip \  
--acl bucket-owner-full-control --s3-accelerate
```

- Para vários arquivos pequenos, agrupe-os antes da transferência:
 - Use a compressão para combinar vários arquivos
 - Use operações em lote do Amazon S3 para transferências em grande escala
- Considere o uso de conectores SFTP Transfer Family com configurações de tempo limite apropriadas para grandes transferências
- Para transferências recorrentes, considere a replicação de dados usando o Amazon Cross-Region S3 Replication (CRR) em vez de transferências ad-hoc
- Monitore o desempenho da transferência usando CloudWatch métricas da Amazon para identificar gargalos

Solucionar problemas de implantação do Terraform

Esta seção descreve possíveis soluções para problemas relacionados à implantação de recursos do Transfer Family usando o Terraform. Para obter informações gerais sobre os módulos do Terraform para Transfer Family, consulte [Módulos Transfer Family Terraform](#).

Tópicos

- [Solucionar problemas de falha na criação de recursos do Terraform](#)
- [Solucionar problemas de gerenciamento de estado do Terraform](#)

Solucionar problemas de falha na criação de recursos do Terraform

Descrição

Ao tentar criar recursos do Transfer Family usando o Terraform, você encontra erros como:

```
Error: error creating Transfer Server: InvalidRequestException: The request is not valid.
Error: error creating Transfer User: InvalidRequestException: Unable to create the user because the server endpoint type is incompatible with the home directory type.
```

Causa

Esses erros geralmente ocorrem devido a parâmetros de configuração incompatíveis ou dependências ausentes na configuração do Terraform. As causas comuns incluem:

- Tipo de endpoint e configurações de armazenamento incompatíveis
- Funções ou políticas necessárias do IAM ausentes
- Especificações incorretas da política de segurança
- Problemas de configuração do VPC endpoint

Solução

Para resolver problemas de implantação do Terraform:

- Certifique-se de que sua configuração do Terraform use combinações de parâmetros compatíveis:
 - Para endpoints públicos, certifique-se de usar o Amazon S3 para armazenamento.
 - Para VPC endpoints, verifique a configuração adequada da VPC e do grupo de segurança.

- Use dependências explícitas com o `depends_on` atributo para garantir que os recursos sejam criados na ordem correta.
- Verifique se todas as funções do IAM têm as relações de confiança e as permissões necessárias.
- Use a versão mais recente do AWS provedor do Terraform para garantir a compatibilidade com todos os recursos do Transfer Family.
- Para implantações complexas e casos de uso simples, considere usar os módulos oficiais do Transfer Family Terraform disponíveis em GitHub . <https://github.com/aws-ia/terraform-aws-transfer-family> Esses módulos fornecem exemplos abrangentes que abrangem casos de uso de clientes simples e complexos, seguem as AWS melhores práticas e podem simplificar a implantação para clientes que precisam de ajuda com a configuração da infraestrutura como código (IaC).

Solucionar problemas de gerenciamento de estado do Terraform

Descrição

Depois de fazer alterações nos recursos do Transfer Family fora do Terraform (via console ou AWS CLI), você encontra desvios de estado ou erros ao executar `terraform plan` ou `terraform apply`.

Causa

O Terraform mantém um arquivo de estado que rastreia os recursos que ele gerencia. Quando as alterações são feitas fora do Terraform, o arquivo de estado fica fora de sincronia com os recursos reais, causando erros ou comportamentos inesperados durante as operações subsequentes do Terraform.

Solução

Para resolver problemas de gerenciamento de estado do Terraform com os recursos da Transfer Family:

1. Use `terraform import` para colocar os recursos existentes sob o gerenciamento do Terraform:

```
terraform import <transfer_family_server.example> s-<server-id>
terraform import <transfer_family_server.example> s-<server-id>/username
```

2. Use `terraform refresh` para atualizar o arquivo de estado com a infraestrutura atual do mundo real

3. Para recursos que não podem ser importados ou têm problemas de estado complexos, considere usá-los `terraform state rm` para removê-los do arquivo de estado e, em seguida, recriá-los com o Terraform
4. Implemente uma política para gerenciar os recursos da Transfer Family exclusivamente por meio do Terraform para evitar futuras mudanças de estado
5. Use armazenamento de estado remoto com bloqueio para evitar modificações simultâneas ao trabalhar em equipes

Solucionar problemas de integração do Web Application Firewall

Esta seção descreve possíveis soluções para problemas relacionados à integração AWS WAF com o Transfer Family.

Tópicos

- [Solucionar problemas de bloqueio de tráfego legítimo pelo WAF](#)
- [Solucione problemas de integração do WAF com provedores de identidade personalizados](#)

Solucionar problemas de bloqueio de tráfego legítimo pelo WAF

Descrição

Depois de configurar AWS WAF com seu endpoint Transfer Family, os usuários legítimos não conseguem se conectar ou enfrentam falhas de conexão intermitentes. Você pode ver respostas HTTP 403 (Proibido) em seus registros.

Causa

Suas AWS WAF regras podem ser muito restritivas ou configuradas incorretamente, causando falsos positivos que bloqueiam o tráfego legítimo. As causas comuns incluem:

- IP-based regras que bloqueiam inadvertidamente redes corporativas ou VPNs
- Rate-based regras com limites muito baixos para seus padrões normais de tráfego
- Grupos de regras gerenciados que são excessivamente agressivos para seu caso de uso

Solução

Para resolver problemas de falsos positivos:

1. Ative o AWS WAF registro para identificar quais regras estão acionando os bloqueios. Para obter instruções, consulte [Registro do tráfego AWS WAF da Web ACL](#).
2. Analise seus registros para identificar padrões nas solicitações bloqueadas.
3. Ajuste suas regras da seguinte forma:
 - Adicionar endereços IP ou intervalos a uma lista de permissões
 - Aumento dos limites de taxa para regras baseadas em taxas
 - Definir regras específicas para o modo de contagem em vez do modo de bloqueio para monitorar sem bloquear
 - Criação de exceções para regras específicas usando exclusões de grupos de regras
4. Teste a configuração atualizada com uma amostra representativa do tráfego legítimo antes da implantação completa.

Solucione problemas de integração do WAF com provedores de identidade personalizados

Descrição

Depois de configurar AWS WAF com seu servidor Transfer Family que usa um provedor de identidade personalizado, a autenticação falha ou os usuários enfrentam problemas de autenticação intermitentes.

Causa

Ao usar um provedor de identidade personalizado com o API Gateway, AWS WAF as regras podem interferir nas chamadas de API entre o Transfer Family e seu provedor de identidade. Isso pode acontecer porque AWS WAF está inspecionando e potencialmente bloqueando o tráfego da API com base em seus conjuntos de regras.

Solução

Para resolver problemas com AWS WAF provedores de identidade personalizados:

- Certifique-se de que sua AWS WAF configuração inclua exceções para os endpoints do API Gateway usados pelo seu provedor de identidade personalizado.
- Adicione o responsável pelo serviço Transfer Family (transfer.amazonaws.com) a uma lista de permissões em suas regras. AWS WAF

- Se estiver usando grupos de regras gerenciados, analise-os em busca de regras que possam afetar os fluxos de autenticação da API e considere a desativação dessas regras específicas.
- Teste seu provedor de identidade diretamente usando a operação da `TestIdentityProvider` API para verificar se ele funciona corretamente sem AWS WAF interferência.

Solucionar problemas de usuários gerenciados pelo serviço

Esta seção descreve possíveis soluções para problemas com usuários gerenciados por serviços.

Tópicos

- [Solução de problemas de usuários gerenciados por serviços](#)

Solução de problemas de usuários gerenciados por serviços

Esta seção descreve possíveis soluções para os seguintes problemas.

Tópicos

- [Solução de problemas de órgão da chave pública longo demais](#)
- [Falha na solução de problemas ao adicionar a chave pública SSH](#)

Solução de problemas de órgão da chave pública longo demais

Descrição

Ao tentar criar um usuário gerenciado pelo serviço, você recebe o seguinte erro:

```
Failed to create user (1 validation error detected:  
'sshPublicKeyBody' failed to satisfy constraint: Member must have length less than or  
equal to 2048)
```

Causa

Talvez você esteja inserindo uma chave PGP para o órgão da chave pública e AWS Transfer Family não ofereça suporte a chaves PGP para usuários gerenciados pelo serviço.

Solução

Se a chave PGP for RSA-based, você poderá convertê-la para o formato PEM. Por exemplo, o Ubuntu fornece uma ferramenta de conversão aqui: <https://manpages.ubuntu.com/manpages/jammy/en/man1/openpgp2ssh.1.html>

Falha na solução de problemas ao adicionar a chave pública SSH

Descrição

Ao tentar adicionar uma chave pública para um usuário gerenciado pelo serviço, você recebe o seguinte erro:

```
Failed to add SSH public key (Unsupported or invalid SSH public key format)
```

Causa

Talvez você esteja tentando importar uma chave SSH2-formatted pública e AWS Transfer Family não ofereça suporte a chaves SSH2-formatted públicas para usuários gerenciados por serviços.

Solução

Você precisa converter a chave para o formato OpenSSH. Esse processo está descrito em [Convertendo uma chave SSH2 em formato de chave pública SSH](#).

Solução de problemas do AS2

Esta seção descreve possíveis soluções para problemas com transferências AS2.

Tópicos

- [Solução de problemas do AS2](#)
- [Problemas com o certificado AS2](#)
- [Problemas de recebimento do AS2 MDN](#)
- [Problemas de monitoramento da expiração do certificado](#)

Solução de problemas do AS2

[Códigos de erro AS2](#), mensagens e dicas de solução de problemas para servidores habilitados para a Declaração de Aplicabilidade 2 (AS2) estão descritas na seção Códigos de falha do AS2 deste guia.

Problemas com o certificado AS2

Descrição

Você está enfrentando erros relacionados ao certificado com as transferências AS2.

Causa

As causas comuns incluem certificados expirados, formatos de certificado incorretos ou cadeias de certificados incompatíveis.

Solução

Experimente as seguintes soluções:

- Verifique se seus certificados não expiraram
- Verifique se os certificados estão no formato correto (para AWS Transfer Family PEM)
- Verifique se a cadeia de certificados está completa e válida
- Confirme se os certificados de assinatura e criptografia coincidem entre os parceiros comerciais
- Alterne os certificados bem antes da expiração para evitar interrupções

Problemas de recebimento do AS2 MDN

Descrição

Você não está recebendo as notificações de disposição de mensagens (mDNS) esperadas para transferências AS2.

Causa

Problemas de MDN podem ocorrer devido a problemas de conectividade de rede, configurações incorretas de endpoint ou incompatibilidades no formato MDN.

Solução

Considere estas soluções:

- Verifique se o URL do MDN está configurado e acessível corretamente
- Verifique a conectividade de rede entre o servidor AS2 e o endpoint MDN

- Certifique-se de que ambos os parceiros comerciais estejam configurados para o mesmo tipo de MDN (síncrono ou assíncrono)
- Revise os registros do AS2 em busca de erros relacionados ao processamento do MDN
- Se estiver usando mDNS síncrono, verifique se os tempos limite estão definidos adequadamente

Problemas de monitoramento da expiração do certificado

Esta seção fornece soluções para problemas comuns relacionados ao monitoramento da expiração de certificados e à DaysUntilExpiry métrica.

DaysUntilExpiry métrica não aparece

Problema: a DaysUntilExpiry métrica não está visível na Amazon CloudWatch após a importação de um certificado.

Solução:

- Aguarde até 24 horas após importar o certificado. Pode levar até um dia inteiro para que o Transfer Family emita a métrica para sua conta.
- Verifique se você está procurando na AWS região correta e abaixo do AWS/Transfer namespace em CloudWatch

Os alarmes de expiração do certificado não estão sendo acionados

Problema: CloudWatch os alarmes de expiração do certificado não são acionados quando esperado.

Solução:

- Verifique se o alarme está configurado com a Maximum estatística e um período de 1 dia.
- Verifique se a comparação do limite está definida para `Less than or equal to` o número de dias desejado.
- Verifique se `Treat missing data as good (not breaching)` está selecionado na configuração do alarme.
- Verifique se as dimensões do alarme correspondem às do seu certificado `Certificateld` e da descrição (se fornecido).
- Verifique se as ações de alarme (tópicos do SNS, notificações por e-mail) estão configuradas e ativas corretamente.

AWS Transfer Family Referência da API

O guia completo de referência de API para Transfer Family está disponível em [AWS Transfer Family API Reference](#).

AWS Transfer Family é um serviço de transferência segura que você pode usar para transferir arquivos para dentro e para fora do armazenamento do Amazon Simple Storage Service (Amazon S3) usando os seguintes protocolos:

- Protocolo de Transferência de Arquivos (SFTP) do Secure Shell (SSH)
- Protocolo de Transferência de Arquivos Seguro (FTPS)
- Protocolo de Transferência de Arquivos (FTP)
- Declaração de Aplicabilidade 2 (AS2)

Servidores, usuários e funções são identificados pelo nome de recurso da Amazon (ARN). Você pode atribuir tags, que são pares de chave-valor, a entidades com um ARN. As tags são metadados que podem ser usados para agrupar ou procurar essas entidades. As tags são úteis, por exemplo, para fins de contabilidade.

As seguintes convenções são observadas nos formatos de AWS Transfer Family ID:

- Os valores `ServerId` assumem a forma `s-01234567890abcdef`.
- Os valores `SshPublicKeyId` assumem a forma `key-01234567890abcdef`.

Os formatos do nome de recurso da Amazon (ARN) assumem a seguinte forma:

- Para servidores, os ARNs assumem a forma `arn:aws:transfer:region:account-id:server/server-id`.

Veja o seguinte exemplo de um servidor ARN: `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

- Para usuários, os ARNs assumem o formato `arn:aws:transfer:region:account-id:user/server-id/username`.

Um exemplo é `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

As entradas DNS (endpoints) em uso são assim:

- Os endpoints de API assumem o formato `transfer.region.amazonaws.com`.
- Os endpoints do servidor assumem o formato `server-id.server.transfer.region.amazonaws.com`.

Essa referência de interface de API AWS Transfer Family contém documentação para uma interface de programação que você pode usar para gerenciar AWS Transfer Family. A estrutura da referência é a seguinte:

- Para uma lista alfabética de ações de API, consulte [Actions](#).
- Para a lista alfabética de tipos de dados, consulte [Types](#).
- Para obter uma lista de parâmetros de consulta comuns, consulte [Parâmetros comuns](#).
- Para obter descrições dos códigos de erro, consulte [Erros comuns](#).

Tip

Em vez de realmente executar um comando, você pode usar o parâmetro `--generate-cli-skeleton` com qualquer chamada de API para gerar e exibir um modelo de parâmetro. Em seguida, você pode usar o modelo gerado para personalizar e usar como entrada em um comando posterior. Para obter detalhes, consulte [Gerar e usar um arquivo esqueleto de parâmetro](#).

Como fazer solicitações de API

Além de usar o console, você pode usar a AWS Transfer Family API para configurar e gerenciar programaticamente seus servidores. Esta seção descreve as AWS Transfer Family operações, a assinatura de solicitações para autenticação e o tratamento de erros. Para obter mais informações sobre as regiões e os endpoints disponíveis para o Transfer Family, consulte [AWS Transfer Family endpoints e quotas](#) no Referência geral da AWS

Note

Você também pode usar os AWS SDKs ao desenvolver aplicativos com o Transfer Family;. Os SDKs AWS para Java, .NET e PHP encapsulam a API subjacente do Transfer Family

para simplificar as tarefas de programação. Para obter informações sobre como fazer download de bibliotecas de SDKs, consulte [Bibliotecas de códigos de exemplo](#).

Cabeçalhos de solicitação obrigatórios do Transfer Family

Esta seção descreve os cabeçalhos requeridos que você precisa enviar em cada solicitação POST ao AWS Transfer Family. Os cabeçalhos HTTP são incluídos para identificar as principais informações sobre a solicitação, como a operação que você deseja invocar, a data da solicitação e informações que indicam sua autorização como remetente da solicitação. Os cabeçalhos diferenciam minúsculas e maiúsculas e a ordem dos cabeçalhos não é importante.

O exemplo a seguir mostra os cabeçalhos que são usados na [ListServers](#) operação.

```
POST / HTTP/1.1
Host: transfer.us-east-1.amazonaws.com
x-amz-target: TransferService.ListServers
x-amz-date: 20220507T012034Z
Authorization: AWS4-HMAC-SHA256 Credential=AKIDEXAMPLE/20220507/us-east-1/transfer/
aws4_request,
    SignedHeaders=content-type;host;x-amz-date;x-amz-target,
    Signature=13550350a8681c84c861aac2e5b440161c2b33a3e4f302ac680ca5b686de48de
Content-Type: application/x-amz-json-1.1
Content-Length: 17

{"MaxResults":10}
```

A seguir encontram-se os cabeçalhos que devem ser incluídos em suas solicitações POST ao Transfer Family. Os cabeçalhos mostrados abaixo que começam com “x-amz” são específicos para AWS. Todos os outros cabeçalhos listados são cabeçalhos comuns usados em transações HTTP.

Entradas e assinaturas de solicitações do Transfer Family

Todas as entradas da solicitação devem ser enviadas como parte da carga JSON no corpo da solicitação. Para ações em que todos os campos de solicitação são opcionais, por exemplo, `ListServers`, você ainda precisa fornecer um objeto JSON vazio no corpo da solicitação, como `{}`. A estrutura da carga útil do Transfer Family request/response está documentada na referência existente da API, por exemplo [DescribeServer](#).

O Transfer Family oferece suporte à autenticação usando o AWS Signature Version 4. Para obter detalhes, veja [Assinatura de solicitações da API da AWS](#).

Respostas de erro

Quando existe um erro, as informações no cabeçalho da resposta contêm:

- Content-Type: application/x-amz-json-1.1
- Um código de status HTTP 4xx ou 5xx apropriado

O corpo de uma resposta de erro contém informações sobre o erro que ocorreu. A resposta de erro de exemplo a seguir mostra a sintaxe de saída dos elementos comuns a todas as respostas de erro.

```
{
  "__type": "String",
  "Message": "String", <!-- Message is lowercase in some instances -->
  "Resource": "String",
  "ResourceType": "String",
  "RetryAfterSeconds": "String"
}
```

A tabela a seguir explica os campos de resposta de erro JSON mostrados na sintaxe anterior.

__type

Uma das exceções de uma chamada de API do Transfer Family.

Tipo: string

Mensagem ou mensagem

Uma das mensagens de código de erro de operação em .

Note

Algumas exceções usam message e outras usam Message. Você pode verificar o código da interface para determinar o caso adequado. Como alternativa, você pode testar cada opção para ver qual funciona.

Tipo: string

Recurso

O recurso para o qual o erro é invocado. Por exemplo, se você tentar criar um usuário que já existe, o Resource será o nome de usuário referente ao usuário existente.

Tipo: string

ResourceType

O recurso para o qual o erro é invocado. Por exemplo, se você tentar criar um usuário que já existe, o ResourceType será User.

Tipo: string

RetryAfterSeconds

O número de segundos a esperar antes de repetir o comando.

Tipo: string

Exemplos de resposta de erro

O corpo JSON a seguir será retornado se você chamar a API DescribeServer e especificar um servidor que não existe.

```
{
  "__type": "ResourceNotFoundException",
  "Message": "Unknown server",
  "Resource": "s-11112222333344444",
  "ResourceType": "Server"
}
```

O corpo JSON a seguir será retornado se a execução de uma API causar o controle de utilização.

```
{
  "__type": "ThrottlingException",
  "RetryAfterSeconds": "1"
}
```

O corpo JSON a seguir será retornado se você usar a API CreateServer e não tiver permissões suficientes para criar um servidor do Transfer Family.


```
{
  "__type": "AccessDeniedException",
  "Message": "You do not have sufficient access to perform this action."
}
```

O corpo JSON a seguir será retornado se você chamar a API `CreateUser` e especificar um servidor que já existe.

```
{
  "__type": "ResourceExistsException",
  "Message": "User already exists",
  "Resource": "Alejandro-Rosalez",
  "ResourceType": "User"
}
```

Bibliotecas disponíveis

AWS fornece bibliotecas, exemplos de código, tutoriais e outros recursos para desenvolvedores de software que preferem criar aplicativos usando APIs específicas da linguagem em vez das ferramentas de linha de comando e da API de consulta. Essas bibliotecas oferecem as funções básicas (não incluídas nas APIs), como autenticação de solicitação, novas tentativas de solicitação e processamento de erros, para que você possa começar a usar com mais facilidade. Veja [as ferramentas para desenvolver AWS](#)

Para obter bibliotecas e código de exemplo em todos os idiomas, consulte [Código de exemplo e bibliotecas](#).

Provedores de identidade

AWS Transfer Family oferece suporte a vários tipos de provedores de identidade para autenticar e gerenciar usuários. Cada servidor pode usar somente um método de autenticação, que deve ser selecionado quando o servidor é criado.

Serviço gerenciado

Com o método de `SERVICE_MANAGED` autenticação, as credenciais do usuário são armazenadas e gerenciadas nele AWS Transfer Family. Os usuários são autenticados usando chaves públicas SSH associadas ao nome de usuário no servidor.

Cada usuário pode ter uma ou mais chaves públicas SSH armazenadas no serviço. Quando um cliente solicita uma operação de arquivo, ele fornece o nome de usuário e a chave privada SSH, que são autenticados na chave pública armazenada.

Directory Service

O método de `AWS_DIRECTORY_SERVICE` autenticação permite a integração com o AWS Directory Service for Microsoft Active Directory (AWS Directory Service for Microsoft Active Directory).

Essa opção permite gerenciar a autenticação e o acesso do usuário por meio de seus grupos existentes do Active Directory. Os usuários podem se autenticar usando suas credenciais do Active Directory.

Há um limite padrão de 100 grupos do Active Directory por servidor, que pode ser aumentado para um máximo de 150 grupos por meio de um aumento no limite de serviço.

Lambda

O método de `AWS_LAMBDA` autenticação permite que você se conecte a um provedor de identidade personalizado usando AWS Lambda.

Essa opção oferece flexibilidade para integração com seus sistemas de gerenciamento de identidade existentes. A função Lambda é responsável por autenticar usuários e retornar as políticas de acesso apropriadas.

Personalizado (API Gateway)

O método de `API_GATEWAY` autenticação (exibido como Personalizado no console) permite que você use um método de autenticação personalizado que fornece autenticação de usuário e controle de acesso.

Este método se baseia no Amazon API Gateway para usar a chamada de API a partir do seu provedor de identidade para validar as solicitações do usuário. Você pode usar esse método personalizado para autenticar usuários em um serviço de diretório, um name/password par de bancos de dados ou algum outro mecanismo.

Para todos os métodos de autenticação, os usuários recebem políticas que definem seu acesso aos buckets do Amazon S3 ou aos sistemas de arquivos do Amazon Elastic File System. O servidor herda a relação de confiança do usuário por meio de uma função do IAM com uma `AssumeRole` ação, permitindo que ele execute operações de arquivo em nome do usuário.

Convenções de nomenclatura

AWS Transfer Family usa formatos padronizados para identificadores de recursos e Amazon Resource Names (ARNs). Compreender essas convenções é importante ao trabalhar com a AWS Transfer Family API.

Formatos de identificação

As seguintes convenções são observadas nos formatos de AWS Transfer Family ID:

IDs do servidor

Os valores `ServerId` assumem a forma `s-01234567890abcdef`.

IDs de chave pública SSH

Os valores `SshPublicKeyId` assumem a forma `key-01234567890abcdef`.

IDs do conector

Os valores `ConnectorId` assumem a forma `c-01234567890abcdef`.

ID do fluxo de trabalho

Os valores `WorkflowId` assumem a forma `w-01234567890abcdef`.

IDs de perfil

Os valores `ProfileId` assumem a forma `p-01234567890abcdef`.

WebApp IDs

Os valores `WebAppId` assumem a forma `webapp-01234567890abcdef`.

Formatos ARN

Os formatos do nome de recurso da Amazon (ARN) assumem a seguinte forma:

ARNs do servidor

Para servidores, os ARNs assumem a forma `arn:aws:transfer:region:account-id:server/server-id`.

Exemplo: `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

ARNs do usuário

Para usuários, os ARNs assumem o formato `arn:aws:transfer:region:account-id:user/server-id/username`.

Exemplo: `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

Conector ARNs

Para conectores, os ARNs assumem o formato `arn:aws:transfer:region:account-id:connector/connector-id`

Exemplo: `arn:aws:transfer:us-east-1:123456789012:connector/c-01234567890abcdef`.

ARNs de fluxo de trabalho

Para fluxos de trabalho, os ARNs assumem o formato.

`arn:aws:transfer:region:account-id:workflow/workflow-id`

Exemplo: `arn:aws:transfer:us-east-1:123456789012:workflow/w-01234567890abcdef`.

WebApp RNs

Para aplicativos da web, os ARNs assumem o formato `arn:aws:transfer:region:account-id:webapp/webapp-id`.

Exemplo: `arn:aws:transfer:us-east-1:123456789012:webapp/webapp-01234567890abcdef`.

Você pode atribuir tags, que são pares de chave-valor, a entidades com um ARN. As tags são metadados que podem ser usados para agrupar ou procurar essas entidades. As tags são úteis, por exemplo, para fins de contabilidade.

DNS e endpoints

AWS Transfer Family usa convenções de nomenclatura de DNS padronizadas para endpoints de API e endpoints de servidor. Compreender esses endpoints é essencial para configurar clientes e fazer chamadas de API.

Endpoints da API

Os endpoints de API são usados para fazer chamadas de API para gerenciar AWS Transfer Family recursos. Esses endpoints assumem as seguintes formas:

Endpoints de API padrão

Os endpoints padrão da API assumem o formato `transfer.region.amazonaws.com`.

Exemplo: `transfer.us-east-1.amazonaws.com`

Dual-Stack Endpoints da API

AWS Transfer Family oferece endpoints de API de pilha dupla que podem ser acessados usando solicitações IPv4 ou IPv6:

- `https://transfer.region-code.api.aws`
- `https://transfer-fips.region-code.api.aws`

Endpoints do servidor

Os endpoints do servidor são usados pelos clientes de transferência de arquivos para se conectarem aos AWS Transfer Family servidores. Esses endpoints assumem as seguintes formas:

Endpoints de servidor padrão

Os endpoints de servidor padrão assumem o formato `server-id.server.transfer.region.amazonaws.com`.

Exemplo: `s-01234567890abcdef.server.transfer.us-east-1.amazonaws.com`

Nomes de host personalizados

Você também pode configurar nomes de host personalizados para seus AWS Transfer Family servidores. Nomes de host personalizados podem ser usados para fornecer uma experiência mais amigável ou de marca para seus usuários.

Para usar um nome de host personalizado, você deve:

1. Possuir o nome de domínio
2. Forneça um certificado válido
3. Configure os registros DNS para apontar para o seu servidor AWS Transfer Family

Para obter uma lista completa de AWS Transfer Family endpoints por AWS região, consulte os [AWS Transfer Family endpoints e as cotas](#) no. Referência geral da AWS

Histórico do documento para AWS Transfer Family

A tabela a seguir descreve a documentação desta versão do AWS Transfer Family.

- Versão da API: transfer-2018-11-05
- Última atualização da documentação: 19 de novembro de 2025

Alteração	Descrição	Data
Suporte a endpoints VPC para aplicativos web Transfer Family	AWS Transfer Family os aplicativos web agora oferecem suporte a endpoints hospedados em VPC, permitindo que você hospede seu endpoint de aplicativos web em uma nuvem privada virtual para transferências de dados privados de e para o Amazon S3 sem atravessar a Internet pública. Para obter detalhes, consulte Crie um aplicativo web Transfer Family em uma VPC .	19 de novembro de 2025
Suporte a IPv6	AWS Transfer Family agora oferece suporte a endpoints de pilha dupla (IPv4 e IPv6) para endpoints públicos SFTP, endpoints para conectores SFTP e AS2 e VPC-internal endpoints de API. SFTP/FTPS /FTP/AS2 Para obter detalhes, consulte Suporte IPv6 para servidores Transfer Family .	30 de junho de 2025

Alteração	Descrição	Data
Aprimoramentos na experiência do usuário dos conectores SFTP	• Capacidade de autoatendimento de conexões simultâneas para seus conectores • Capacidade de fornecer chave privada SSH no formato OpenSSH que é usada para autenticar conexões • Capacidade de descobrir a chave pública do host de servidores remotos usando seus conectores SFTP Para obter detalhes, consulte Crie um conector SFTP com saída gerenciada por serviços.	9 de abril de 2025
Capacidade de os conectores SFTP excluïrem, renomearem e moverem arquivos no servidor SFTP remoto	Agora você pode organizar seus arquivos armazenados em servidores SFTP remotos excluïndo, renomeando ou movendo os arquivos de origem para locais de arquivamento após serem copiados do servidor remoto. Para obter detalhes, consulte Mover ou renomear arquivos ou diretórios no servidor SFTP remoto.	7 de abril de 2025

Alteração	Descrição	Data
Support para aplicativos AWS Transfer Family da web	AWS Transfer Family aplicativos web são um novo recurso que os clientes podem usar para criar uma interface simples para acessar seus dados no Amazon S3 por meio de um navegador da web. Para obter detalhes, consulte Aplicativos web Transfer Family .	1.º de dezembro de 2024
Referência de API movida para um guia separado	Para melhorar a experiência do cliente, a Referência da API agora é publicada separadamente do guia do usuário. Para a referência separada da API, consulte Bem-vindo à AWS Transfer Family API .	31 de julho de 2024
Capacidade de conectores SFTP listar arquivos e diretórios remotos	A Transfer Family adicionou a capacidade de nossos clientes usarem conectores SFTP para listar arquivos armazenados em servidores SFTP remotos. Para obter detalhes, consulte Listar o conteúdo de um diretório remoto	23 de abril de 2024

Alteração	Descrição	Data
Capacidade de usar o certificado TLS autoassinado de um parceiro comercial com troca de mensagens AS2	AWS Transfer Family adicionou a opção de importar e usar o certificado TLS público e autoassinado de um parceiro comercial para enviar mensagens da Declaração de Aplicabilidade 2 (AS2) ao servidor via HTTPS.	12 de abril de 2024
Adição de políticas de segurança para conectores SFTP	AWS Transfer Family adicionou políticas de segurança para uso com conectores SFTP. Para obter detalhes, consulte Políticas de segurança para AWS Transfer Family Conectores SFTP .	5 de abril de 2024
Integre com a Amazon EventBridge	AWS Transfer Family agora publica automaticamente eventos na Amazon EventBridge para todas as operações de transferência de arquivos. Para obter detalhes, consulte Gerenciamento Transfer Family eventos usando Amazon EventBridge .	8 de fevereiro de 2024

Alteração	Descrição	Data
Adição de novas políticas de segurança	AWS Transfer Family adicionou novas políticas de segurança FIPS e não FIPS. Além disso, a política de segurança padrão atribuída aos servidores é sempre a política de segurança mais recente. Para obter detalhes, consulte Políticas de segurança para AWS Transfer Family servidores .	5 de fevereiro de 2024
Support para endereços IP estáticos para conectores SFTP e AS2	O Transfer Family agora fornece endereços IP estáticos para conectores SFTP e AS2. Isso permite a conexão com servidores SFTP remotos protegidos por controles de lista de permissões de IP. Para o AS2, estamos introduzindo endereços IP estáticos para respostas MDN assíncronas dos servidores AS2.	16 de janeiro de 2024
O guia do usuário foi reorganizado para se alinhar mais de perto com a versão mais recente do. AWS Transfer Family	O Transfer Family adicionou vários recursos desde o início do guia, necessitando de uma reestruturação do guia.	3 de janeiro de 2024

Alteração	Descrição	Data
Aprimoramentos nos mapeamentos lógicos de diretórios Otimização de desempenho da lista Amazon S3	O Transfer Family agora oferece suporte a mapeamentos lógicos de diretórios de até 2,1 MB. Agora você também pode declarar se o mapeamento de um usuário é para um arquivo. Para obter mais informações, consulte Regras para usar diretórios lógicos. Ao criar ou atualizar um servidor que usa o Amazon S3 para armazenamento, agora você pode otimizar o desempenho da listagem de seus diretórios (ou pastas) do S3. Para obter mais informações, consulte Configurando um endpoint de servidor SFTP, FTPS ou FTP.	17 de novembro de 2023
Porta alternativa para servidores SFTP com endpoints de nuvem privada virtual (VPC)	Agora você pode habilitar uma porta alternativa não padrão para seus servidores SFTP Transfer Family que tenham VPC endpoints. Para obter mais informações, consulte Crie um servidor em uma VPC (virtual private cloud).	17 de novembro de 2023

Alteração	Descrição	Data
Suporte para conectores SFTP	Os conectores SFTP ampliam os recursos AWS Transfer Family de comunicação com servidores remotos na nuvem e no local. Para obter mais informações, consulte Usando conectores SFTP .	25 de julho de 2023
Suporte para autenticação AS2 Basic	O Transfer Family agora oferece suporte ao uso da autenticação básica para servidores que usam o protocolo Applicability Statement 2 (AS2). Para obter mais informações, consulte Autenticação básica para conectores AS2 .	30 de junho de 2023
Suporte para logs estruturados em JSON	O Transfer Family agora suporta a entrega de registros JSON estruturados para a Amazon CloudWatch, o agrupamento de fluxos de registros em grupos de registros personalizados e a realização de consultas de registros comuns entre protocolos. Para obter mais informações, consulte CloudWatch Registro na Amazon para AWS Transfer Family servidores .	24 de junho de 2023

Alteração	Descrição	Data
Suporte para vários métodos de autenticação	O Transfer Family tem suporte para autenticação usando uma senha, um public/private key pair ou ambos. Isso está disponível para servidores que usam o protocolo SFTP e um provedor de identidade e personalizado. Para obter mais informações, consulte Crie um SFTP-enabled servidor .	17 de maio de 2023
É possível usar a decodificação Pretty Good Privacy (PGP) com os arquivos que o Transfer Family processa com fluxos de trabalho	O Transfer Family tem suporte integrado paracriptografia Pretty Good Privacy (PGP). É possível usar acriptografia PGP em arquivos enviados por SFTP, FTPS ou FTP para o Amazon Simple Storage Service (Amazon S3) ou o Amazon Elastic File System (Amazon EFS). Para obter mais informações, consulte Gerar chaves PGP e Use acriptografia PGP em seu fluxo de trabalho .	21 de dezembro de 2022

Alteração	Descrição	Data
Compatível com servidores Transfer Family: suporte totalmente gerenciado para o protocolo de transferência de arquivos Applicability Statement 2 (AS2)	Você pode criar servidores que usam o protocolo AS2 para enviar e receber informações de e para parceiros comerciais que estejam dentro ou fora do AWS ambiente. Para obter mais informações, consulte Configurar AS2 .	25 de julho de 2022
Suporte para exibir banners ao criar um servidor	É possível adicionar mensagens personalizadas ao criar servidores. É possível exibir uma mensagem de pré-autenticação (todos os protocolos) e uma mensagem de pós-autenticação (para servidores FTP e FTPS). Para obter mais informações, consulte Crie um SFTP-enabled servidor , Crie um FTPS-enabled servidor ou Crie um FTP-enabled servidor .	17 de fevereiro de 2022

Alteração	Descrição	Data
Support for AWS Lambda como provedor de identidade	Agora você pode se conectar a um provedor de identidade personalizado usando AWS Lambda seus servidores Transfer Family. Anteriormente, era necessário fornecer um URL Amazon API Gateway para integrar um provedor de identidade personalizado. Para obter mais informações, consulte Usando AWS Lambda para integrar seu provedor de identidade .	16 de novembro de 2021
Suporte para fluxos de trabalho gerenciados de transferência de arquivos	Os fluxos de trabalho gerenciados de transferência de arquivos fornecem abstrações de processamento pós-upload para as tarefas comuns que você executa manualmente no momento. Para obter mais informações, consulte AWS Transfer Family fluxos de trabalho gerenciados .	2 de setembro de 2021

Alteração	Descrição	Data
Support for AWS Directory Service for Microsoft Active Directory	Além dos provedores de identidade personalizados e gerenciados por serviços, agora você pode usar AWS Directory Service for Microsoft Active Directory para gerenciar o acesso do usuário para autenticação e autorização. Para obter mais informações, consulte Usando o AWS Directory Service para o Microsoft Active Directory .	24 de maio de 2021
Novo Regiões da AWS	AWS Transfer Family agora está disponível na região da África (Cidade do Cabo). Para obter mais informações sobre os endpoints do Transfer Family, consulte AWS Transfer Family endpoints e cotas no Referência geral da AWS.	24 de fevereiro de 2021
Novo Regiões da AWS	AWS Transfer Family agora está disponível nas regiões Ásia-Pacífico (Hong Kong) e Oriente Médio (Bahrein). Para obter mais informações sobre os endpoints do Transfer Family, consulte AWS Transfer Family endpoints e cotas no Referência geral da AWS.	17 de fevereiro de 2021

Alteração	Descrição	Data
Suporte para o Amazon EFS como armazenamento de dados	O Transfer Family agora oferece suporte à transferências de arquivos para dentro e fora do Amazon Elastic File System (Amazon EFS). O Amazon EFS é um sistema de arquivos NFS elástico simples, escalável e totalmente gerenciado. Para obter mais informações, consulte Configurar um sistema de arquivos Amazon EFS .	6 de janeiro de 2021
Support for AWS WAF	O Transfer Family agora oferece suporte AWS WAF a um firewall de aplicativos da web que ajuda a proteger os aplicativos da web e as operações de API contra ataques. Para obter mais informações, consulte Adicione um firewall da aplicação web .	24 de novembro de 2020
Suporte para vários grupos de segurança em uma nuvem privada virtual (VPC)	Agora é possível anexar vários grupos de segurança a um servidor em uma VPC. Para obter mais informações, consulte Crie um servidor em uma VPC (virtual private cloud) .	15 de outubro de 2020

Alteração	Descrição	Data
Novo Regiões da AWS	O Transfer Family agora está disponível nas AWS GovCloud (US) regiões. Para obter mais informações sobre endpoints Transfer Family para AWS GovCloud (US) regiões, consulte AWS Transfer Family endpoints e cotas no. Referência geral da AWS Para obter informações sobre como usar o Transfer Family nas AWS GovCloud (US) regiões, consulte AWS Transfer Family o Guia AWS GovCloud (US) do usuário.	30 de setembro de 2020
Uma política de segurança com algoritmos criptográficos compatíveis agora pode ser anexada ao seu servidor	Agora é possível anexar uma política de segurança que contém um conjunto de algoritmos criptográficos compatíveis ao seu servidor. Para obter mais informações, consulte Políticas de segurança para AWS Transfer Family servidores .	12 de agosto de 2020

Alteração	Descrição	Data
Compatibilidade com endpoints do padrão FIPS (Padrão federal de processamento de informações)	FIPS-enabled Os endpoints agora estão disponíveis na América Regiões da AWS do Norte. Para saber as regiões disponíveis, consulte Endpoints e cotas do AWS Transfer Family em Referência a geral da AWS. Para habilitar o FIPS para um endpoint de SFTP-enabled servidor, consulte. Crie um SFTP-enabled servidor Para habilitar o FIPS para um endpoint de FTPS-enabled servidor, consulte. Crie um FTPS-enabled servidor Para habilitar o FIPS para um endpoint de FTP-enabled servidor, consulte. Crie um FTP-enabled servidor	12 de agosto de 2020
Aumento do tamanho dos caracteres do nome de usuário e caracteres adicionais permitidos	Os nomes de usuário agora podem conter sinais (@) e pontos (.) e podem ter no máximo 100 caracteres. Para adicionar um usuário, consulte Gerenciando usuários para endpoints de servidor .	12 de agosto de 2020

Alteração	Descrição	Data
Support para criação automática de funções do Amazon CloudWatch Logging AWS Identity and Access Management (IAM)	O Transfer Family agora oferece suporte à criação automática de uma função de CloudWatch registro do IAM para visualizar a atividade do usuário final. Para obter mais informações, consulte Crie um SFTP-enabled servidor , Crie um FTPS-enabled servidor ou Crie um FTP-enabled servidor .	30 de julho de 2020
AWS Transfer Family agora oferece suporte ao IP de origem como um fator de autorização.	O Transfer Family adiciona suporte ao uso dos endereços IP de origem dos usuários finais como um fator de autorização, permitindo que você aplique uma camada adicional de segurança ao autorizar o acesso via Secure File Transfer Protocol (SFTP), File Transfer Protocol (FTPS) ou File Transfer Protocol (FTP). Para obter mais informações, consulte Trabalhar com provedores de identidade personalizados .	9 de junho de 2020

Alteração	Descrição	Data
AWS A transferência para SFTP está agora AWS Transfer Family e adiciona suporte para FTP e FTPS.	Agora é possível usar dois protocolos adicionais para as transferências de arquivos de seus usuários: File Transfer Protocol Secure (FTPS) e File Transfer Protocol (FTP). Os usuários podem mover, executar, proteger e integrar fluxos de trabalho baseados em FTP over SSL (FTPS) e FTP de texto simples AWS, além do suporte existente ao Secure File Transfer Protocol (SFTP).	23 de abril de 2020
Suporte para grupos de segurança de nuvem privada virtual (VPC) e endereços IP elásticos	Agora é possível criar uma lista de permissões para endereços IP de entrada usando grupos de segurança , fornecendo uma camada adicional de segurança para servidores. Você também pode associar endereços IP elásticos ao endpoint do seu servidor. Ao fazer isso, é possível permitir que os usuários protegidos por firewalls permitam o acesso a esse endpoint. Para obter mais informações, consulte Crie um servidor em uma VPC (virtual private cloud) .	10 de janeiro de 2020

Alteração	Descrição	Data
Suporte para trabalhar em uma VPC	Agora é possível criar um servidor em uma VPC. É possível usar o servidor para transferir dados em SFTP de e para um bucket do Amazon S3 sem passar pela internet pública. Para obter mais informações, consulte Crie um servidor em uma VPC (virtual private cloud) ..	27 de março de 2019
Primeira versão do AWS Transfer Family lançado.	Esta versão inicial inclui a configuração de direções, descreve como começar, e fornece informações sobre a configuração do cliente, a configuração do usuário e a atividade de monitoramento.	25 de novembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.