



Guia do usuário

AWS DataSync



AWS DataSync: Guia do usuário

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais 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 desprestigie 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 DataSync?	1
Casos de uso	2
Benefícios	3
Recursos adicionais	3
Como funciona	4
DataSync arquitetura de transferência	4
Transferência entre armazenamento local e AWS	4
Transferência entre serviços AWS de armazenamento	5
Transferência entre serviços AWS de armazenamento e sistemas de armazenamento em outras nuvens	6
Conceitos e terminologia	7
Agente	8
Local	8
Tarefa	8
Execução de tarefas	8
Como DataSync transfere arquivos, objetos e diretórios	8
Como DataSync prepara sua transferência de dados	9
Como DataSync transfere seus dados	10
Como DataSync verifica a integridade dos seus dados	11
Como DataSync funciona com arquivos abertos e bloqueados	11
Opções de transferência recorrentes	12
Começar	13
Inscreva-se para um Conta da AWS	13
Criar um usuário com acesso administrativo	13
Permissões de IAM necessárias para usar DataSync	15
AWS políticas gerenciadas	15
Políticas gerenciadas pelo cliente	15
Onde posso usar DataSync?	15
Como posso usar DataSync?	16
Quanto vai DataSync custar?	16
Componentes de código aberto usados por DataSync	16
Eu preciso de um agente?	16
Situações em que você precisa de um DataSync agente	17
Situações em que você não precisa de um DataSync agente	17

Usando vários DataSync agentes	17
Próximas etapas	18
Requisitos do agente	18
Requisitos de hipervisor	18
Requisitos do agente para DataSync transferências	19
Requisitos de agente para Região da AWS partições	20
Requisitos de gerenciamento de agente	20
Implantação do agente	21
Implantando seu agente em VMware	21
Implantação do agente no KVM	22
Implantação do agente no Microsoft Hyper-V	23
Implantando seu agente da Amazon EC2	24
Implantação do agente no AWS Snowball Edge	29
Implantando seu agente em AWS Outposts	29
Escolha de um endpoint de serviço para o agente	30
Escolha um endpoint de serviço público	30
Escolha de um endpoint de serviço FIPS	30
Escolha um endpoint de serviço da VPC	31
Ativação do agente do	33
Pré-requisitos	33
Obtenção de uma chave de ativação	34
Ativação do agente do	36
Próximas etapas	39
Verificação das conexões de rede para o agente	39
Acesso ao console local do agente	39
Verificação da conexão do agente com sistema de armazenamento	40
Verificando a conexão do seu agente com o serviço DataSync	41
Próximas etapas	42
Conexão da sua rede	43
1. Conexão de rede entre o sistema de armazenamento e o agente	43
2. Conexão de rede entre seu agente e o DataSync serviço	43
Conexão da sua rede de armazenamento à AWS	44
Escolher um endpoint de serviço	44
3. Conexão de rede entre o DataSync serviço e o serviço AWS de armazenamento	44
Trabalho em rede quando você não precisa de um DataSync agente	45
Como e onde DataSync o tráfego flui pela rede	45

Segurança de rede para DataSync	45
Requisitos de rede	45
Requisitos de rede para armazenamento on-premises, autogerenciado, em outra nuvem e a na borda	46
Requisitos de rede para serviços de armazenamento AWS	51
Requisitos de rede para endpoints de serviço públicos ou FIPS	52
Requisitos de rede para endpoints de serviço da VPC	59
Interfaces de rede para transferências de dados	62
Interfaces de rede para transferências com agentes	62
Interfaces de rede para transferências sem agentes	63
Visualizar suas interfaces de rede	64
Exemplos de arquitetura e roteamento com o Direct Connect	65
Usando o Direct Connect com um DataSync endpoint de serviço VPC	65
Usando o Direct Connect com um DataSync endpoint de serviço público ou FIPS	68
Próximas etapas	69
Configurando seu agente para vários NICs	69
Transferir dados	71
Para onde posso transferir meus dados?	72
Transferências suportadas no mesmo Conta da AWS	72
Transferências suportadas em Contas da AWS	74
Transferências suportadas no mesmo Região da AWS	75
Transferências compatíveis entre Regiões da AWS	75
Determinar se sua transferência requer um DataSync agente	76
Transferir de ou para o armazenamento on-premises	76
Configurar transferências com um servidor de arquivos NFS	77
Configurar transferências com um servidor de arquivos NFS	81
Configuração de transferências com um cluster do HDFS	93
Configurar transferências com um sistema de armazenamento de objetos	97
Transferindo de ou para o armazenamento AWS	102
Configurar transferências de com o Amazon S3	102
Configurar transferências com o Amazon EFS	135
Configurando transferências com o FSx Windows File Server	145
Configurando transferências com FSx for Lustre	150
Configurando transferências com FSx para OpenZFS	153
Configurando transferências com o FSx for ONTAP	156
Transferir de ou para outro armazenamento em nuvem	165

Planejando transferências de ou para sistemas de armazenamento em nuvem de terceiros	165
Configurar transferências com o Google Cloud Storage	168
Configurar transferências com o Microsoft Azure Blob Storage	177
Configurando transferências com Microsoft Azure Files	195
Configurar transferências com outro armazenamento de objetos na nuvem	199
Transferindo de ou para um armazenamento compatível com S3 no Snowball Edge	206
Pré-requisitos	206
Fornecendo DataSync acesso ao armazenamento compatível com S3	206
Criação de um DataSync agente em seu ambiente de armazenamento local	208
Configurar o local de origem para sua transferência	210
Configurar o local de destino para sua transferência	211
Definir as configurações de transferência	211
Iniciar sua transferência.	212
Limitações	212
Criando uma tarefa para transferir dados	212
Criação da tarefa do	213
Status da tarefa	215
Particionamento de grandes conjuntos de dados com várias tarefas	216
Segmentação de dados transferidos com várias tarefas	217
Escolhendo um modo de tarefa para sua transferência	217
Escolha de quais dados transferir	222
Verificar a integridade dos dados	261
Definir limites de banda	264
Programar sua tarefa	266
Marcar suas tarefas	271
Iniciando uma tarefa para transferir dados	274
Iniciando sua tarefa	274
Status de execução de tarefa	276
Como saber quando a tarefa está na fila	277
Cancelamento da execução da tarefa	277
Monitorando transferências de dados	279
Entendendo os contadores de desempenho de transferência de dados	279
Monitorando transferências de dados com CloudWatch métricas	296
CloudWatch métricas para DataSync	296
Monitorando transferências de dados com relatórios de tarefas	300

Casos de uso	300
Relatórios de tarefas somente resumidos	301
Relatórios de tarefas padrão	301
Exemplos de relatórios de tarefa	304
Limitações	308
Criação de relatórios de tarefa	308
Visualização de relatórios de tarefa	319
Monitorando transferências de dados com o CloudWatch Logs	319
DataSync Permitindo o upload de registros para um grupo de CloudWatch registros	319
Configurando o registro para sua tarefa DataSync	322
Visualizando registros de DataSync tarefas	325
Fazendo login com CloudTrail	326
Trabalhando com DataSync informações em CloudTrail	326
Entendendo as entradas do arquivo de DataSync log	327
Monitoramento com EventBridge	329
DataSync eventos de transferência	329
Monitoramento do com ferramentas manuais	331
Monitorando sua transferência usando o DataSync console	331
Monitorando sua transferência usando o AWS CLI	332
Monitorando sua transferência usando o utilitário watch	334
Gerenciar recursos	335
Gerenciando seu DataSync agente	335
Testando a conectividade e os recursos do sistema do seu DataSync agente	335
Substituindo seu DataSync agente	335
Limpando DataSync recursos	335
Reutilizando a infraestrutura de um DataSync agente	335
Gerenciar seu agente	335
Atualizações de software de agente	336
Status de agentes	336
Solução de problemas de seu agente	337
Manutenção do agente	337
Acesso ao console local do agente	337
Configuração das definições de DHCP e DNS do agente	338
Verificando os recursos do sistema do seu agente	341
Sincronizando a hora em seu agente VMware	343
Execução de comandos relacionados à manutenção para agente	344

Substituir seu agente	345
Criar um novo agente	345
Atualizando sua localização com o novo agente	346
Próximas etapas	351
Recursos de filtragem DataSync	352
Parâmetros para filtragem	352
Filtrando por local	353
Filtrando por tarefa	354
Limpando DataSync recursos	355
Excluindo um agente DataSync	355
Reutilizando a infraestrutura de um DataSync agente	356
Excluindo um local DataSync	356
Excluindo uma tarefa DataSync	357
Segurança	359
Proteção de dados	360
Criptografia em trânsito	360
Criptografia em repouso	363
Privacidade do tráfego entre redes	364
Gerenciamento de identidade e acesso	364
Gerenciamento de acesso	365
AWS políticas gerenciadas	370
Políticas gerenciadas pelo cliente	381
Usar perfis vinculados a serviço	384
Marcação de recursos durante a criação	388
Prevenção contra o ataque do “substituto confuso” em todos os serviços	390
Validação de conformidade	392
Resiliência	393
Segurança da infraestrutura	394
Protegendo as credenciais do local de armazenamento	394
Usando um segredo gerenciado pelo serviço criptografado com uma chave padrão	395
Usando um segredo gerenciado pelo serviço criptografado com uma chave personalizada	
AWS KMS	395
Usando um segredo que você gerencia	397
Cotas	400
Limites do sistema de armazenamento, arquivos e objetos	400
DataSync cotas	400

Solicitar um aumento da cota	406
Solução de problemas	407
Solução de problemas do agente	407
Como faço para me conectar ao console local de um EC2 agente da Amazon?	407
O que significa o erro Falha ao recuperar a chave de ativação do agente?	408
Ainda não consigo ativar um agente usando um endpoint de serviço VPC	408
O que eu faço se meu agente estiver off-line?	408
Não sei o que está acontecendo com meu agente. Alguém pode me ajudar?	409
Solução de problemas de localização	410
Falha na minha tarefa com um erro de permissões do NFS negadas	410
Falha na minha tarefa com um erro de montagem do NFS	411
Falha na minha tarefa com um erro de montagem do Amazon EFS	411
A propriedade do arquivo não é mantida com a transferência do NFS	412
Minha tarefa não consegue acessar um local SMB que usa Kerberos	412
Minha tarefa falhou com um erro de entrada/saída	413
Erro: FsS3UnableToConnectToEndpoint	414
Erro: FsS3HeadBucketFailed	415
A tarefa falha com um Unable to list Azure Blobs on the volume root erro... ..	415
Erro: FsAzureBlobVolRootListBlobsFailed	415
Erro: SrcLocHitAccess	416
Erro: SyncTaskErrorLocationNotAdded	416
A tarefa com o local de origem do S3 falha HeadObject ou GetObjectTagging erro	416
Solução de problemas de tarefas	417
Erro: SyncOption valor inválido. Opção: TransferModePreserveDeletedFiles,, Valor: TUDO, REMOVE.	417
A execução da tarefa falha com um EniNotFounderro	417
A execução da tarefa falha com um erro Não é possível alocar memória	418
A execução da tarefa tem um status de lançamento, mas nada parece estar acontecendo ..	418
A execução da tarefa parece paralisada no status de preparação	418
A execução da tarefa é interrompida antes que a transferência termine	419
A execução da tarefa falha ao transferir de um bucket do Google Cloud Storage	419
Há incompatibilidades entre os registros de data e hora da execução da tarefa	420
A execução da tarefa falha com NoMem erro	420
Falha na transferência do objeto para Azure Blob Storage com user metadata key erro	420
Há uma /.aws-datasync pasta no local de destino	420

Não é possível transferir links simbólicos entre locais usando SMB	421
Erros do relatório de tarefas	421
Solução de problemas de verificação de dados	422
Há incompatibilidades entre o conteúdo de um arquivo	422
Há uma incompatibilidade entre os metadados SMB de um arquivo	423
Os arquivos a serem transferidos não estão mais no local de origem	424
DataSync não é possível verificar os dados de destino	425
DataSync não consigo ler os metadados do objeto	426
Há uma incompatibilidade nos metadados definidos pelo sistema de um objeto	427
Entendendo a duração da verificação de dados	428
Solução de problemas de custos de armazenamento do S3 com DataSync	429
Tutoriais	430
Transferência de on-premises para S3 entre contas	430
Visão geral	430
Pré-requisito: permissões necessárias na conta de origem	431
Pré-requisito: permissões necessárias na conta de destino	433
Etapa 1: na sua conta de origem, crie um DataSync agente	434
Etapa 2: na sua conta de origem, crie uma função DataSync do IAM para acesso ao bucket de destino	434
Etapa 3: na conta de destino, atualize a política do bucket do S3	436
Etapa 4: na sua conta de destino, desative ACLs o bucket do S3	438
Etapa 5: na sua conta de origem, crie um local de DataSync origem para seu armazenamento local	438
Etapa 6: na sua conta de origem, crie um local de DataSync destino para seu bucket do S3	439
Etapa 7: na sua conta de origem, crie e inicie sua DataSync tarefa	440
Recursos relacionados	440
Transferência entre buckets do S3 em várias contas	442
Visão geral	442
Pré-requisito: permissões necessárias na conta de origem	444
Pré-requisito: permissões necessárias na conta de destino	446
Etapa 1: na sua conta de origem, crie uma função DataSync do IAM para acesso ao bucket de destino	447
Etapa 2: na conta de destino, atualize a política do bucket do S3	449
Etapa 3: na sua conta de destino, desative ACLs o bucket do S3	450
Etapa 4: na sua conta de origem, crie seus DataSync locais	451

Etapa 5: na sua conta de origem, crie e inicie sua DataSync tarefa	453
Solução de problemas	454
Relacionado: transferências entre contas com buckets S3 usando criptografia no servidor ..	453
Executando uma grande migração	455
O que é uma grande migração de dados?	455
Estágios principais de uma grande migração de dados	455
Recursos adicionais	456
Etapa 1: Planejando sua migração	456
Requisitos de coleta	457
Execução de uma prova de conceito	463
Estimando os cronogramas de migração	464
Etapa 2: Implementando sua migração	467
Acelerando sua migração com particionamento	467
Executando suas DataSync tarefas	469
Monitorando suas transferências	471
DataSync API	472
Ações	472
CancelTaskExecution	475
CreateAgent	477
CreateLocationAzureBlob	482
CreateLocationEfs	489
CreateLocationFsxLustre	495
CreateLocationFsxOntap	499
CreateLocationFsxOpenZfs	504
CreateLocationFsxWindows	509
CreateLocationHdfs	514
CreateLocationNfs	521
CreateLocationObjectStorage	526
CreateLocationS3	534
CreateLocationSmb	541
CreateTask	550
DeleteAgent	560
DeleteLocation	562
DeleteTask	564
DescribeAgent	566
DescribeLocationAzureBlob	571

DescribeLocationEfs	576
DescribeLocationFsxLustre	582
DescribeLocationFsxOntap	585
DescribeLocationFsxOpenZfs	590
DescribeLocationFsxWindows	594
DescribeLocationHdfs	598
DescribeLocationNfs	603
DescribeLocationObjectStorage	607
DescribeLocationS3	612
DescribeLocationSmb	617
DescribeTask	623
DescribeTaskExecution	633
ListAgents	650
ListLocations	654
ListTagsForResource	658
ListTaskExecutions	662
ListTasks	666
StartTaskExecution	670
TagResource	677
UntagResource	680
UpdateAgent	683
UpdateLocationAzureBlob	685
UpdateLocationEfs	690
UpdateLocationFsxLustre	694
UpdateLocationFsxOntap	697
UpdateLocationFsxOpenZfs	700
UpdateLocationFsxWindows	703
UpdateLocationHdfs	707
UpdateLocationNfs	713
UpdateLocationObjectStorage	717
UpdateLocationS3	723
UpdateLocationSmb	727
UpdateTask	734
UpdateTaskExecution	741
Tipos de dados	743
AgentListEntry	746

AzureBlobSasConfiguration	748
CmkSecretConfig	749
CustomSecretConfig	751
Ec2Config	753
FilterRule	755
FsxProtocol	757
FsxProtocolNfs	758
FsxProtocolSmb	759
FsxUpdateProtocol	761
FsxUpdateProtocolSmb	763
HdfsNameNode	765
LocationFilter	766
LocationListEntry	768
ManagedSecretConfig	770
ManifestConfig	771
NfsMountOptions	773
OnPremConfig	775
Options	776
Platform	785
PrivateLinkConfig	786
QopConfiguration	788
ReportDestination	789
ReportDestinationS3	790
ReportOverride	792
ReportOverrides	793
ReportResult	795
S3Config	796
S3ManifestConfig	797
SmbMountOptions	799
SourceManifestConfig	801
TagListEntry	802
TaskExecutionFilesFailedDetail	803
TaskExecutionFilesListedDetail	805
TaskExecutionListEntry	807
TaskExecutionResultDetail	809
TaskFilter	812

TaskListEntry	814
TaskReportConfig	816
TaskSchedule	818
TaskScheduleDetails	820
Erros comuns	821
Parâmetros gerais	823
Histórico do documento	826
AWS Glossário	841
.....	dcccxl

O que é AWS DataSync?

AWS DataSync é um serviço de transferência de dados on-line que simplifica a migração de dados e ajuda você a transferir de forma rápida, fácil e segura seus dados de arquivos ou objetos para, de e entre AWS serviços de armazenamento.

Transferências de armazenamento on-premises

DataSync funciona com os seguintes sistemas de armazenamento local:

- [Network File System \(NFS\)](#)
- [Server Message Block \(SMB\)](#)
- [Hadoop Distributed File System \(HDFS\)](#)
- [Armazenamento de objetos](#)

AWS transferências de armazenamento

DataSync funciona com os seguintes serviços AWS de armazenamento:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)
- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Outras transferências de armazenamento em nuvem

DataSync funciona com os seguintes serviços de armazenamento em outras nuvens:

- [Google Cloud Storage](#)
- [Microsoft Azure Blob Storage](#)
- [Microsoft Azure Files](#)
- [Wasabi Cloud Storage](#)

- [DigitalOcean Spaces](#)
- [Oracle Cloud Infrastructure Object Storage](#)
- [Cloudflare R2 Storage](#)
- [Backblaze B2 Cloud Storage](#)
- [NAVER Cloud Object Storage](#)
- [Alibaba Cloud Object Storage Service](#)
- [IBM Cloud Object Storage](#)
- [Seagate Lyve Cloud](#)

Transferências de armazenamento de borda

DataSync funciona com os seguintes serviços e dispositivos de armazenamento de borda:

- [Armazenamento compatível com Amazon S3 em AWS Snowball Edge](#)

Casos de uso

Esses são alguns dos principais casos de uso de DataSync:

- Migre dados — transfira rapidamente conjuntos de dados ativos pela rede para serviços AWS de armazenamento. DataSync inclui criptografia automática e validação da integridade dos dados para ajudar a garantir que seus dados cheguem com segurança, intactos e prontos para uso.
- Arquive dados inativos: mova dados inativos armazenados no armazenamento on-premises diretamente para classes de armazenamento de longo prazo duráveis e seguras, como S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Ao fazer isso, é possível liberar capacidade de armazenamento on-premises e desligar os sistemas de armazenamento herdados.
- Replique dados: copie dados em qualquer classe de armazenamento do Amazon S3, escolhendo a classe de armazenamento mais econômica para suas necessidades. Você também pode enviar dados para o Amazon EFS, FSx para o Windows File Server, FSx para o Lustre ou FSx para o OpenZFS para um sistema de arquivos em espera.
- Transfira dados para processamento oportuno na nuvem — Transfira dados para dentro ou AWS para fora para processamento. Essa abordagem pode acelerar fluxos de trabalho críticos de nuvem híbrida em diversos setores. Eles incluem machine learning no setor de ciências biológicas, produção de vídeos no setor de mídia e entretenimento, análise de big data no setor financeiro e pesquisa sísmica no setor de petróleo e gás.

Benefícios

Ao usar DataSync, você pode obter os seguintes benefícios:

- Automatize a movimentação de dados — DataSync facilita a transferência de dados pela rede entre sistemas e serviços de armazenamento. DataSync automatiza o gerenciamento dos processos de transferência de dados e a infraestrutura necessária para transferências de dados seguras e de alto desempenho.
- Transfira dados com segurança — DataSync fornece end-to-end segurança, incluindo criptografia e validação da integridade dos dados, para ajudar a garantir que seus dados cheguem com segurança, intactos e prontos para uso. DataSync acessa seu AWS armazenamento por meio de mecanismos AWS de segurança integrados, como funções AWS Identity and Access Management (IAM). Ele também é compatível com endpoints de nuvem privada virtual (VPC), oferecendo a opção de transferir dados sem atravessar a internet pública e aumentando ainda mais a segurança dos dados copiados on-line.
- Mova dados com mais rapidez — DataSync usa um protocolo de rede específico e uma arquitetura paralela e multisegmentada para acelerar suas transferências. Essa abordagem acelera migrações, fluxos de trabalho de processamento de dados recorrentes para análise e machine learning e processos de proteção de dados.

Recursos adicionais

Recomendamos que você leia o seguinte:

- [DataSync recursos](#) — Inclui blogs, vídeos e outros materiais de treinamento
- [AWS re:POST](#) — Veja a última discussão sobre DataSync
- [Definição de preço do AWS DataSync](#)

Como AWS DataSync funciona

Aprenda os principais conceitos e a terminologia relacionados às AWS DataSync transferências, incluindo como os dados são transferidos de locais locais e na nuvem.

DataSync arquitetura de transferência

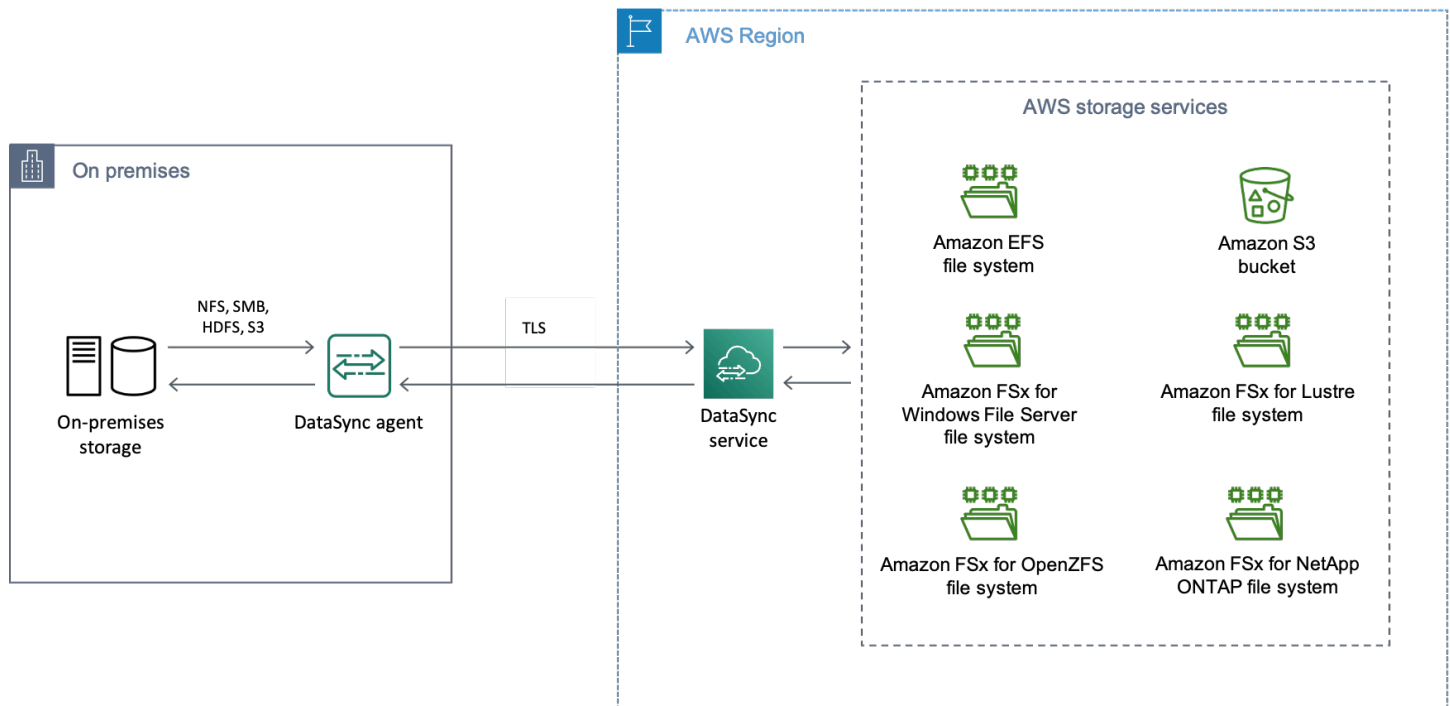
Os diagramas a seguir mostram como e onde DataSync normalmente transfere dados de armazenamento. Para obter uma lista completa dos sistemas e serviços de armazenamento DataSync compatíveis, consulte [Para onde posso transferir meus dados com AWS DataSync?](#)

Tópicos

- [Transferência entre armazenamento local e AWS](#)
- [Transferência entre serviços AWS de armazenamento](#)
- [Transferência entre serviços AWS de armazenamento e sistemas de armazenamento em outras nuvens](#)

Transferência entre armazenamento local e AWS

O diagrama a seguir mostra uma visão geral de alto nível da DataSync transferência de arquivos entre sistemas de armazenamento autogerenciados e locais e. Serviços da AWS

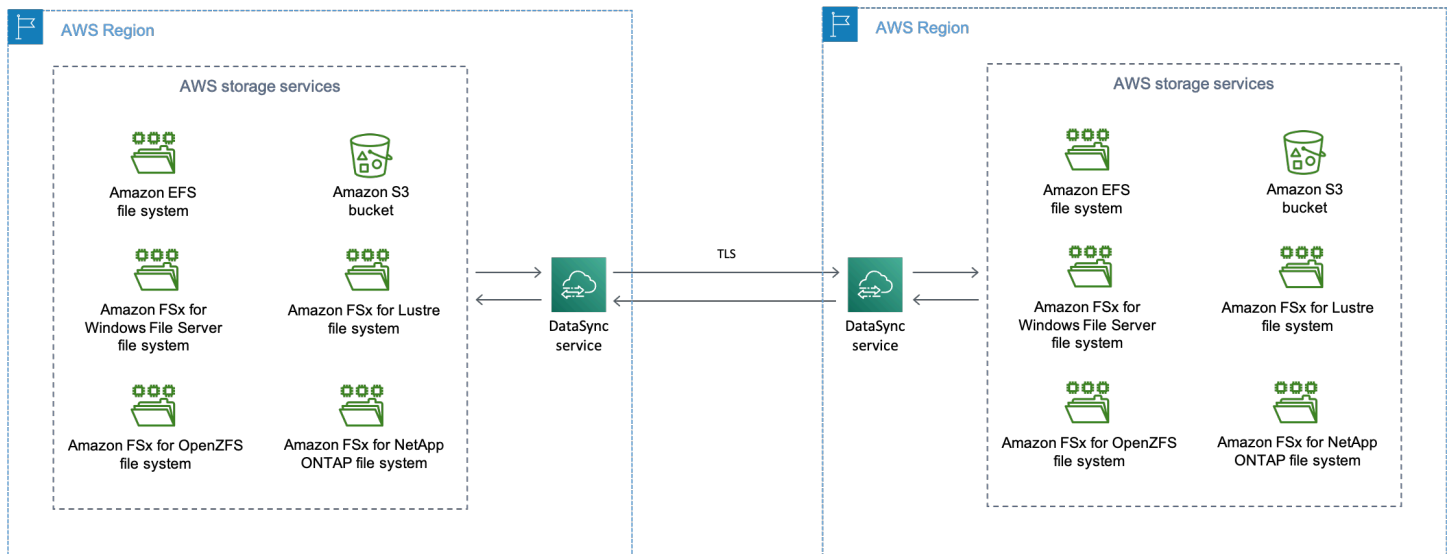


O diagrama ilustra um caso de DataSync uso comum:

- Um DataSync agente copiando dados de um sistema de armazenamento local.
- Dados transferidos para dentro AWS, criptografados usando Transport Layer Security (TLS).
- DataSync copiando dados para um serviço AWS de armazenamento compatível.

Transferência entre serviços AWS de armazenamento

O diagrama a seguir mostra uma visão geral de alto nível da DataSync transferência de arquivos entre os Serviços da AWS mesmos. Conta da AWS



O diagrama ilustra um caso de DataSync uso comum:

- DataSync copiando dados de um serviço AWS de armazenamento compatível.
- Dados em movimento Regiões da AWS, criptografados usando TLS.
- DataSync copiando dados para um serviço AWS de armazenamento compatível.

Ao transferir entre serviços AWS de armazenamento (seja no mesmo Região da AWS ou entre eles Regiões da AWS), seus dados permanecem na AWS rede e não atravessam a Internet pública.

Important

Você paga pelos dados transferidos entre Regiões da AWS. Isso é cobrado como transferência de dados PARA FORA da região de origem para a região de destino. Para obter mais informações, consulte [Preço de transferência de dados](#).

Transferência entre serviços AWS de armazenamento e sistemas de armazenamento em outras nuvens

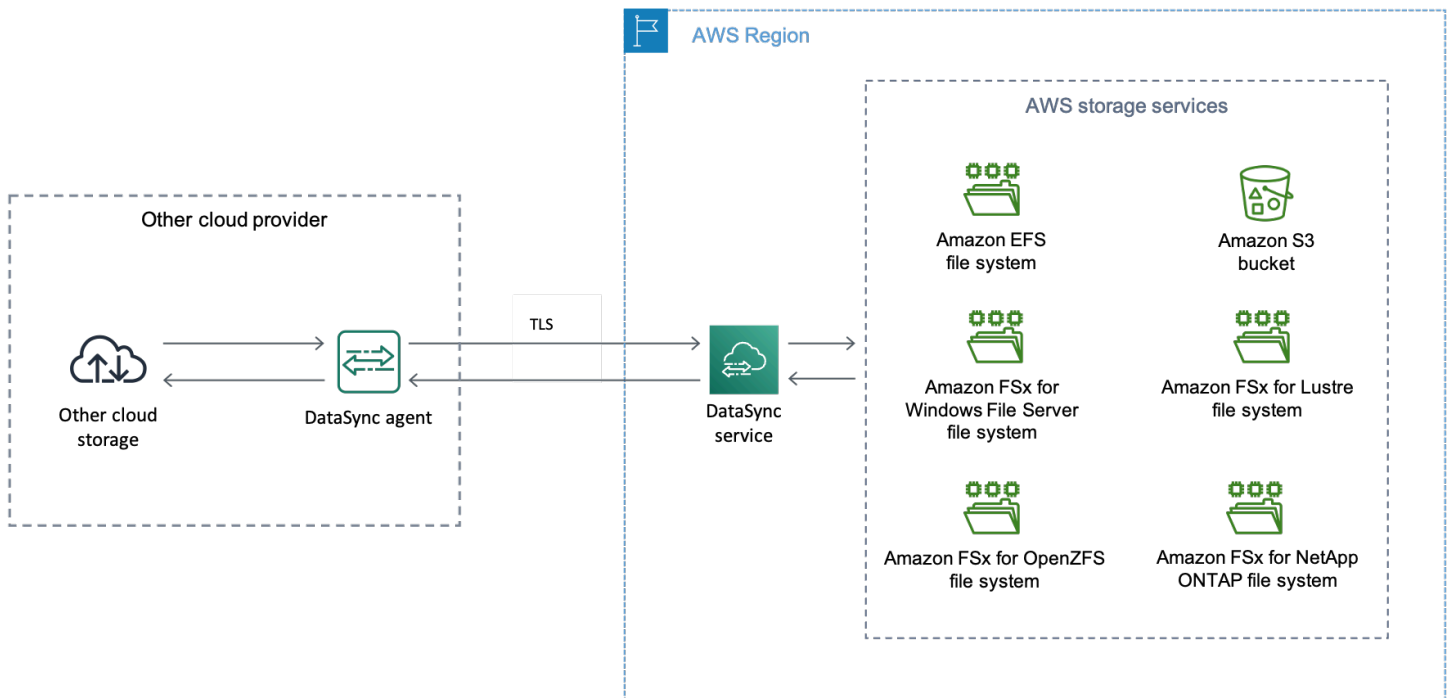
Com DataSync, você pode transferir dados entre outros sistemas de armazenamento em nuvem Serviços da AWS e. Nesse contexto, os sistemas de armazenamento em nuvem podem incluir:

- Sistemas de armazenamento autogerenciados, como um servidor de arquivos NFS em sua nuvem privada virtual (VPC) na AWS.

- Sistemas ou serviços de armazenamento hospedados por outro provedor de nuvem. Para obter mais informações, consulte [Transferindo de ou para outro armazenamento em nuvem com AWS DataSync](#).

DataSync pode copiar dados de e para outras nuvens com ou sem o uso de um agente. Para obter mais informações sobre quando usar um agente, consulte [Preciso de um AWS DataSync agente?](#).

O diagrama a seguir mostra uma visão geral de alto nível da DataSync transferência de dados entre serviços AWS de armazenamento e outro provedor de nuvem.



Conceitos e terminologia

Familiarize-se com os recursos DataSync de transferência.

Tópicos

- [Agente](#)
- [Local](#)
- [Tarefa](#)
- [Execução de tarefas](#)

Agente

Um agente é um dispositivo de máquina virtual (VM) que DataSync usa para ler e gravar no armazenamento durante uma transferência.

Você pode implantar um agente em seu ambiente de armazenamento em uma máquina virtual baseada em VMware ESXi kernel Linux (KVM) ou em hipervisores Microsoft Hyper-V. Para armazenamento em uma nuvem privada virtual (VPC) em AWS, você pode implantar um agente como uma instância da Amazon EC2.

Para começar, consulte o [Eu preciso de um AWS DataSync agente?](#).

Local

Um local descreve o local de ou para onde você está copiando os dados. Cada DataSync transferência (também conhecida como tarefa) tem um local de origem e destino. Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

Tarefa

Uma tarefa descreve uma DataSync transferência. Ele identifica um local de origem e destino junto com detalhes sobre como copiar dados entre esses locais. Você também pode especificar como uma tarefa lida com metadados, arquivos excluídos e permissões.

Execução de tarefas

A execução de uma tarefa é uma execução individual de uma tarefa de DataSync transferência. Há várias fases envolvidas na execução de uma tarefa. Para obter mais informações, consulte [Status de execução de tarefa](#).

Como DataSync transfere arquivos, objetos e diretórios

Durante a [execução de uma tarefa](#), DataSync prepara, transfere e verifica seus dados. DataSync A forma como essas ações são executadas depende de como você configura suas opções de DataSync tarefa, como o [modo de tarefa](#). As tarefas do modo básico preparam, transferem e verificam seus dados sequencialmente, enquanto as tarefas do modo Avançado fazem isso em paralelo.

Tópicos

- [Como DataSync prepara sua transferência de dados](#)
- [Como DataSync transfere seus dados](#)
- [Como DataSync verifica a integridade dos seus dados](#)
- [Como DataSync funciona com arquivos abertos e bloqueados](#)
- [Opções de transferência recorrentes](#)

Como DataSync prepara sua transferência de dados

DataSync por padrão, prepara sua transferência examinando seus locais de origem e destino para determinar o que transferir. Isso é feito digitalizando o conteúdo e os metadados de ambos os locais para identificar diferenças entre os dois.

Note

Se você configurar sua tarefa para [transferir todos os dados](#), não há preparação. Quando você inicia sua tarefa, transfere DataSync imediatamente tudo da origem para o destino sem comparar locais.

A forma como DataSync prepara sua transferência também depende do seu modo de tarefa:

Preparação aprimorada do modo	Preparação do modo básico
DataSync prepara objetos à medida que são encontrados no local de origem. A preparação continua durante toda a execução da tarefa até que não haja mais objetos listados na origem. Ao contrário do modo Básico, DataSync pode preparar um número praticamente ilimitado de objetos com cada execução de tarefa.	A preparação pode levar apenas alguns minutos, algumas horas ou até mais, dependendo do número de arquivos, objetos ou diretórios nos dois locais e do desempenho do seu armazenamento. Os itens que DataSync inventários em sua origem e destino contam para suas cotas de tarefas. Essas cotas não se baseiam no número de itens que são DataSync transferidos durante a execução de cada tarefa.

DataSync pode pular alguns arquivos, objetos e diretórios durante a preparação. Os motivos para isso podem depender de vários fatores, como a forma como você configura suas tarefas e as permissões do sistema de armazenamento. Veja alguns exemplos:

- Existe um arquivo nos locais de origem e de destino. O arquivo na origem não foi modificado desde a execução anterior da tarefa. Como você está [transferindo apenas dados que foram alterados](#), DataSync não transfere esse arquivo na próxima vez que executar sua tarefa.
- Um objeto que existe em ambas as suas localizações muda em sua fonte. Ao executar sua tarefa, DataSync ignora esse objeto em seu destino porque sua tarefa não [sobrescreve os dados no destino](#).
- DataSync ignora um objeto em seu local de origem que está usando uma [classe de armazenamento de arquivamento](#) e não foi restaurado. Você deve restaurar um objeto arquivado DataSync para poder lê-lo.
- DataSync ignora um arquivo, objeto ou diretório em seu local de origem porque não consegue lê-lo. Se isso acontecer e não for esperado, verifique as permissões de acesso do seu armazenamento e certifique-se de que ele DataSync possa ler o que foi ignorado.

Como DataSync transfere seus dados

DataSync copia seus dados (incluindo metadados) da origem para o destino com base nas suas opções de tarefa. Por exemplo, você pode especificar quais [metadados](#) serão copiados, [excluir](#) determinados arquivos e limitar o DataSync uso [da largura de banda](#), entre outras opções.

A forma como DataSync transfere seus dados também depende do seu modo de tarefa:

Transferência de modo aprimorada	Transferência de modo básico
DataSync transfere cada objeto assim que ele é preparado.	Depois de DataSync preparar todos os seus dados, a transferência começa.

DataSync pode pular alguns itens durante a transferência. Se você configurar sua tarefa para [transferir todos os dados](#), isso pode acontecer com um objeto em seu local de origem que está usando uma [classe de armazenamento de arquivamento](#) e não foi restaurado.

Como DataSync verifica a integridade dos seus dados

DataSync sempre realiza verificações de integridade em seus dados durante uma transferência. Ao final de uma transferência, também DataSync pode realizar verificações adicionais apenas nos dados transferidos ou em todo o conjunto de dados em ambos os locais. Para obter mais informações, consulte [Configurando como AWS DataSync verifica a integridade dos dados](#).

Ao verificar a integridade dos dados, DataSync calcula e compara a soma de verificação e os metadados dos arquivos, objetos ou diretórios em seus locais. Se DataSync notar diferenças entre os locais, a verificação falhará com um erro. Por exemplo, você pode ver erros como `Checksum failureMetadata failure,Files were added,` ou `Files were removed`.

A forma como a verificação funciona depende do seu modo de tarefa e se você configura DataSync para verificar a integridade dos dados no final da transferência.

Verificação de modo aprimorada	Verificação do modo básico
DataSync verifica cada objeto à medida que ele é transferido para o seu destino.	Ao final da transferência, DataSync verifica a integridade dos seus dados.
Com o modo Avançado, DataSync verifica somente os dados transferidos .	Dependendo de como você configura a verificação de dados , isso pode levar um tempo significativo para grandes conjuntos de dados.

Como DataSync funciona com arquivos abertos e bloqueados

Tenha em mente o seguinte ao tentar transferir arquivos que estejam abertos (em uso) ou bloqueados:

- Em geral, DataSync pode transferir arquivos abertos sem quaisquer limitações.
- Se um arquivo estiver aberto e estiver sendo gravado durante uma transferência, DataSync poderá detectar esse tipo de inconsistência durante a fase de verificação da tarefa de transferência. Para obter a versão mais recente do arquivo, execute a tarefa novamente.
- Se um arquivo estiver bloqueado e o servidor DataSync impedir sua abertura, o arquivo será DataSync ignorado durante a transferência e registrará um erro.
- DataSync não consegue bloquear ou desbloquear arquivos.

Opções de transferência recorrentes

Além de transferências únicas, DataSync pode transferir dados de forma recorrente. Algumas das opções para essas situações incluem:

- [Agendamento](#) de quando a tarefa é executada.
- Transferência [apenas os dados que foram alterados](#) desde a execução anterior da tarefa.
- [Exclusão de dados no local de destino](#) que não existem mais na origem.

Começando com AWS DataSync

Antes de começar AWS DataSync, você precisa se inscrever em um, Conta da AWS se não tiver um. Também recomendamos saber onde DataSync podem ser usados e quanto pode custar transferir seus dados.

Inscreva-se para um Conta da AWS

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

Para se inscrever em um Conta da AWS

1. Abra a <https://portal.aws.amazon.com/billing/inscrição>.
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 um 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](#).

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando <https://aws.amazon.com/e> escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login [AWS Management Console](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

Para obter ajuda ao fazer login usando o usuário-raiz, consulte [Fazer login como usuário-raiz](#) no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

Para obter instruções, consulte [Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz \(console\) no Guia](#) do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

Para obter instruções, consulte [Habilitar o AWS IAM Identity Center](#) no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte [Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM](#) no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte [Como fazer login no portal de AWS acesso](#) no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte [Criar um conjunto de permissões](#) no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

Para obter instruções, consulte [Adicionar grupos](#) no Guia do usuário do AWS IAM Identity Center .

Permissões de IAM necessárias para usar DataSync

DataSync pode transferir seus dados para um bucket do Amazon S3, sistema de arquivos Amazon EFS ou [vários outros serviços de AWS armazenamento](#). Para levar seus os dados para onde você quiser, você precisa que as permissões certas do IAM sejam concedidas à sua identidade. Por exemplo, a função do IAM que você usa DataSync precisa de permissão para usar as operações do Amazon S3 necessárias para transferir dados para um bucket do S3.

Você pode conceder essas permissões com as políticas do IAM fornecidas por AWS ou criando suas próprias políticas.

Sumário

- [AWS políticas gerenciadas](#)
- [Políticas gerenciadas pelo cliente](#)

AWS políticas gerenciadas

AWS fornece as seguintes políticas gerenciadas para casos de DataSync uso comuns:

- `AWSDataSyncReadOnlyAccess`— Fornece acesso somente para leitura a. DataSync
- `AWSDataSyncFullAccess`— DataSync Fornece acesso total e mínimo às suas dependências.

Para obter mais informações, consulte [AWS políticas gerenciadas para AWS DataSync](#).

Políticas gerenciadas pelo cliente

Você pode criar políticas personalizadas do IAM para usar com DataSync. Para obter mais informações, consulte [Políticas gerenciadas pelo cliente do IAM para o AWS DataSync](#).

Onde posso usar DataSync?

Para obter uma lista Regiões da AWS de endpoints DataSync compatíveis, consulte [AWS DataSync endpoints e cotas](#) no. Referência geral da AWS

Como posso usar DataSync?

Existem várias maneiras de usar DataSync:

- [DataSync console](#), que faz parte do AWS Management Console.
- [DataSync API](#) ou o [AWS CLI](#) para configurar e gerenciar programaticamente. DataSync
- [AWS CloudFormation](#) ou [Terraform](#) para provisionar seus DataSync recursos.
- [AWS SDKs](#) para criar aplicativos que usem DataSync.

Quanto vai DataSync custar?

Na página [DataSync de preços](#), crie uma estimativa personalizada usando a quantidade de dados que você planeja transferir.

Componentes de código aberto usados por DataSync

Para ver os componentes de código aberto usados pelo DataSync, baixe o link a seguir:

- [datasync-open-source-components.zip](#)

Eu preciso de um AWS DataSync agente?

Para usar AWS DataSync, você pode precisar de um agente. Um agente é um dispositivo de máquina virtual (VM) que você implanta em seu ambiente de armazenamento para transferências de dados.

A necessidade de um agente depende de vários fatores, incluindo o tipo de armazenamento para ou do qual você está transferindo, se você está transferindo e entre Contas da AWS o qual Regiões da AWS está se transferindo. Antes de continuar lendo, [verifique se é DataSync compatível com a transferência na qual você está interessado](#).

Depois de determinar se é DataSync compatível com seu cenário de transferência, revise as informações a seguir para ajudá-lo a entender se você precisa de um agente.

Situações em que você precisa de um DataSync agente

A maioria das situações que exigem um DataSync agente envolve armazenamento gerenciado por você ou por outro provedor de nuvem.

- Transferência entre serviços AWS de armazenamento e armazenamento local
- Transferência entre Amazon EFS ou Amazon FSx e armazenamento em outras nuvens
- Transferindo de ou para o armazenamento do Edge
- Transferência entre alguns serviços AWS de armazenamento Contas da AWS (quando nenhum serviço de armazenamento é o Amazon S3)

Para obter mais informações, consulte [Transferências suportadas em Contas da AWS](#).

- Transferência entre um comercial Região da AWS e outro em AWS GovCloud (US) que a origem e o destino são o Amazon EFS ou a Amazon FSx.

Situações em que você não precisa de um DataSync agente

As situações que não exigem um agente se aplicam se você estiver se transferindo na [mesma Região da AWS](#) ou [entre regiões](#).

- Transferência entre serviços AWS de armazenamento no mesmo Conta da AWS
- Transferência entre o Amazon S3 e um serviço de armazenamento AWS diferente em Contas da AWS
- Transferência entre o Amazon S3 e o armazenamento de objetos em outras nuvens
- Transferência entre um comercial Região da AWS e um em que a AWS GovCloud (US) origem ou o destino seja o Amazon S3

Usando vários DataSync agentes

Embora a maioria das transferências precise apenas de um agente, o uso de vários agentes pode acelerar as transferências de grandes conjuntos de dados com milhões de arquivos ou objetos. Nessas situações, recomendamos executar tarefas de transferência em paralelo. Essa abordagem distribui a carga de trabalho de transferência em várias tarefas, com cada tarefa usando seu próprio agente. Também ajuda a reduzir o tempo necessário DataSync para preparar e transferir seus dados. Para obter mais informações, consulte [Particionamento de grandes conjuntos de dados com várias tarefas](#).

Outra opção, especialmente se você tiver milhões de arquivos pequenos, é usar vários agentes com um local de transferência. Por exemplo, você pode conectar até quatro agentes ao seu serviço de arquivos do Network File System (NFS), Sistema de Arquivos de Rede on-premises. Essa opção pode acelerar sua transferência, embora o tempo necessário DataSync para prepará-la não mude.

Com qualquer uma das duas abordagens, lembre-se de que elas podem aumentar as operações de E/S no armazenamento e afetar a largura de banda da rede. Para obter mais informações sobre o uso de vários agentes para suas DataSync transferências, consulte o [blog AWS de armazenamento](#).

Se você está pensando em usar vários agentes, lembre-se do seguinte:

- Usar vários agentes em um local não oferece alta disponibilidade. Todos os agentes associados a um local devem estar on-line antes que você possa iniciar sua tarefa de transferência. Se um dos agentes estiver [off-line](#), você não poderá executar sua tarefa.
- Se você estiver [usando um endpoint de serviço de nuvem privada virtual \(VPC\)](#) para se comunicar com o DataSync serviço, todos os agentes devem usar o mesmo endpoint e sub-rede.

Próximas etapas

- Se você precisar de um agente, analise os [requisitos do agente](#) para entender o que faz sentido para seu ambiente de armazenamento.
- Se você não precisar de um agente para a transferência, você pode começar a [configurar a transferência](#).

Requisitos para AWS DataSync agentes

Antes de [implantar](#) um AWS DataSync agente em seu ambiente de armazenamento, certifique-se de compreender os requisitos do hipervisor e dos recursos do agente.

Requisitos de hipervisor

Você pode executar um DataSync agente nos seguintes hipervisores:

- VMware ESXi (versão 6.5, 6.7, 7.0 ou 8.0): [VMware ESXi está disponível no site da Broadcom](#). Você também precisa de um cliente VMware vSphere para se conectar ao host.
- Linux Kernel-based Virtual Machine (KVM): uma tecnologia de virtualização gratuita e de código aberto. O KVM está incluído nas versões 2.6.20 e mais recentes do Linux. DataSync é testado

e compatível com as distribuições CentOS/RHEL 7 e 8, Ubuntu 16.04 LTS e Ubuntu 18.04 LTS. Qualquer outra distribuição do Linux moderna poderá funcionar, mas não garantimos o funcionamento nem o desempenho. Você deve habilitar a virtualização acelerada por hardware em seu host KVM para implantar seu agente. DataSync

Recomendamos esta opção se você já tiver um ambiente de KVM em funcionamento e já estiver familiarizado com o funcionamento da KVM.

A execução do KVM na Amazon EC2 não é suportada e não pode ser usada por DataSync agentes.

- Microsoft Hyper-V (versão 2012 R2, 2016 ou 2019): para essa configuração, você precisa de um Microsoft Hyper-V Manager em um computador cliente Microsoft Windows para se conectar ao host.

O DataSync agente é uma máquina virtual (VM) de primeira geração. Para obter mais informações sobre as diferenças entre a geração 1 e a geração 2 VMs, consulte [Devo criar uma máquina virtual de primeira ou segunda geração no Hyper-V?](#)

- Amazon EC2: DataSync fornece uma Amazon Machine Image (AMI) que contém a DataSync imagem. Para obter os tipos de instância recomendados, consulte [Requisitos de EC2 instância da Amazon](#).

Requisitos do agente para DataSync transferências

Para DataSync transferências, seu agente deve atender aos seguintes requisitos de recursos.

Important

Lembre-se de que os requisitos do agente para trabalhar com até 20 milhões de arquivos, objetos ou diretórios são diretrizes gerais. Seu agente pode precisar de mais recursos devido a outros fatores, como quantos diretórios você tem e o tamanho dos metadados do objeto. Por exemplo, a instância m5.2xlarge para um EC2 agente da Amazon ainda pode não ser suficiente para uma transferência de menos de 20 milhões de arquivos.

Sumário

- [Requisitos de máquina virtual](#)
- [Requisitos de EC2 instância da Amazon](#)

Requisitos de máquina virtual

Ao implantar um DataSync agente que não está em uma EC2 instância da Amazon, a VM do agente exige os seguintes recursos:

- Processores virtuais: quatro processadores virtuais atribuídos à VM.
- Espaço em disco: 80 GB de espaço em disco para instalar a imagem da VM e os dados do sistema.
- RAM: dependendo do seu cenário de transferência, você precisa da seguinte quantidade de memória:
 - 32 GB de RAM atribuídos à VM para execuções de tarefas trabalhando com até 20 milhões de arquivos, objetos ou diretórios.
 - 64 GB de RAM atribuídos à VM para execuções de tarefas trabalhando com mais de 20 milhões de arquivos, objetos ou diretórios.

Requisitos de EC2 instância da Amazon

Ao implantar um DataSync agente em uma EC2 instância da Amazon, o tamanho da instância deve ser pelo menos 2xlarge.

É recomendável usar um dos tamanhos de instância a seguir:

- m5.2xlarge: para execuções de tarefas trabalhando com até 20 milhões de arquivos, objetos ou diretórios.
- m5.4xlarge: para execuções de tarefas trabalhando com mais de 20 milhões de arquivos, objetos ou diretórios.

Requisitos de agente para Região da AWS partições

DataSync as imagens do agente estão associadas a [Região da AWS partições](#) específicas. Por exemplo, por padrão, você não pode baixar um agente em um comercial Região da AWS e depois ativá-lo em um AWS GovCloud (US) Region.

Requisitos de gerenciamento de agente

Depois de [ativar](#) seu DataSync agente, AWS gerencia o agente para você. Para obter mais informações, consulte [Gerenciando seu AWS DataSync agente](#).

Implantando seu agente AWS DataSync

Ao criar um AWS DataSync agente, a primeira etapa é implantar o agente em seu ambiente de armazenamento. Você pode implantar um agente como uma máquina virtual (VM) em VMware ESXi uma máquina virtual baseada em kernel Linux (KVM) e hipervisores Microsoft Hyper-V. Você também pode implantar um agente como uma EC2 instância da Amazon em uma nuvem privada virtual (VPC) interna. AWS



Tip

Antes de começar, confirme se você [precisa de um DataSync agente](#).

Implantando seu agente em VMware

Você pode baixar um agente do DataSync console e implantá-lo em seu VMware ambiente.

Antes de começar: certifique-se de que seu ambiente de armazenamento possa oferecer suporte a um DataSync agente. Para obter mais informações, consulte [Requisitos de máquina virtual](#).

Para implantar um agente em VMware

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação à esquerda, escolha Agentes e, em seguida, escolha Criar agente.
3. Para Hypervisor, escolha e VMWare ESXi, em seguida, escolha Baixar a imagem.

O agente faz o download em um arquivo .zip que contém um arquivo de imagem .ova.

4. Para minimizar a latência da rede, implante o agente o mais próximo possível do sistema de armazenamento que DataSync precisa ser acessado (a mesma rede local, se possível). Para obter mais informações, consulte [Requisitos de rede para armazenamento on-premises, autogerenciado, em outra nuvem e a na borda](#).

Se necessário, consulte a documentação do seu hipervisor sobre como implantar um .ova arquivo em um VMware host.

5. Ligue o hipervisor, faça login no agente da VM e obtenha o endereço IP do agente. Você precisa desse endereço IP para ativar o agente.

As credenciais padrão do agente da VM são formadas pelo login **admin** e a senha **password**. Se necessário, altere a senha por meio do [console local da VM](#).

Próxima etapa: [Escolha de um endpoint de serviço para o agente do AWS DataSync](#)

Implantação do agente no KVM

Você pode baixar um agente do DataSync console e implantá-lo em seu ambiente KVM.

Antes de começar: certifique-se de que seu ambiente de armazenamento possa oferecer suporte a um DataSync agente. Para obter mais informações, consulte [Requisitos de máquina virtual](#).

Para implantar um agente no KVM

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação à esquerda, escolha Agentes e, em seguida, escolha Criar agente.
3. Para Hypervisor, escolha Máquina Virtual Baseada em Kernel (KVM) e, em seguida, escolha Baixar a imagem.

O agente faz o download em um arquivo .zip que contém um arquivo de imagem .qcow2.

4. Para minimizar a latência da rede, implante o agente o mais próximo possível do sistema de armazenamento que DataSync precisa ser acessado (a mesma rede local, se possível). Para obter mais informações, consulte [Requisitos de rede para armazenamento on-premises, autogerenciado, em outra nuvem e a na borda](#).
5. Execute o seguinte comando para instalar a imagem do .qcow2.

```
virt-install \
  --name "datasync" \
  --description "DataSync agent" \
  --os-type=generic \
  --ram=32768 \
  --vcpus=4 \
  --disk path=datasync-yyyymmdd-x86_64.qcow2,bus=virtio,size=80 \
  --network default,model=virtio \
  --graphics none \
  --virt-type kvm \
  --import
```


Para obter informações sobre como gerenciar essa VM e seu host KVM, consulte a documentação do seu hipervisor.

6. Ligue o hipervisor, faça login na sua VM e obtenha o endereço IP do agente. Você precisa desse endereço IP para ativar o agente.

As credenciais padrão do agente da VM são formadas pelo login **admin** e a senha **password**. Se necessário, altere a senha por meio do [console local da VM](#).

Próxima etapa: [Escolha de um endpoint de serviço para o agente do AWS DataSync](#)

Implantação do agente no Microsoft Hyper-V

Você pode baixar um agente do DataSync console e implantá-lo em seu ambiente Microsoft Hyper-V.

Antes de começar: certifique-se de que seu ambiente de armazenamento possa oferecer suporte a um DataSync agente. Para obter mais informações, consulte [Requisitos de máquina virtual](#).

Para implantar um agente no Hyper-V

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação à esquerda, escolha Agentes e, em seguida, escolha Criar agente.
3. Para Hypervisor, escolha Microsoft Hyper-V e, em seguida, escolha Baixar a imagem.

O agente faz o download em um arquivo .zip que contém um arquivo de imagem .vhd.

4. Para minimizar a latência da rede, implante o agente o mais próximo possível do sistema de armazenamento que DataSync precisa ser acessado (a mesma rede local, se possível). Para obter mais informações, consulte [Requisitos de rede para armazenamento on-premises, autogerenciado, em outra nuvem e a na borda](#).

Se necessário, consulte a documentação do seu hipervisor sobre como implantar um arquivo .vhd em um host Hyper-V.

Warning

Você pode notar um desempenho de rede ruim se habilitar a fila de máquinas virtuais (VMQ) em um host Hyper-V que esteja usando um adaptador de rede Broadcom.

Para obter informações sobre uma solução alternativa, consulte a [documentação da Microsoft](#).

5. Ligue o hipervisor, faça login na sua VM e obtenha o endereço IP do agente. Você precisa desse endereço IP para ativar o agente.

As credenciais padrão do agente da VM são formadas pelo login **admin** e a senha **password**. Se necessário, altere a senha por meio do [console local da VM](#).

Próxima etapa: [Escolha de um endpoint de serviço para o agente do AWS DataSync](#)

Implantando seu agente da Amazon EC2

Você pode implantar um DataSync agente como uma EC2 instância da Amazon ao transferir dados entre:

- Um sistema de armazenamento em nuvem autogerenciado (por exemplo, um servidor de arquivos NFS em AWS) e um serviço AWS de armazenamento.
- Um provedor de armazenamento em nuvem (como Microsoft Azure Blob Storage ou Google Cloud Storage) e um serviço AWS de armazenamento.
- Um bucket S3 em um comercial Região da AWS e um bucket S3 em um. AWS GovCloud (US) Region
- [Amazon S3 ativado AWS Outposts](#) e um serviço de AWS armazenamento.

Warning

Não recomendamos o uso de um EC2 agente da Amazon com armazenamento local devido ao aumento da latência da rede. Em vez disso, implante o agente como uma máquina virtual VMware, KVM ou Hyper-V em seu data center o mais próximo possível do armazenamento local.

Implantando seu agente EC2

Para escolher o agente AMI para seu Região da AWS

1. Abra um terminal e copie o AWS CLI comando a seguir para obter a ID mais recente DataSync da Amazon Machine Image (AMI) para a região em que você deseja implantar seu EC2 agente da Amazon.

```
aws ssm get-parameter --name /aws/service/datasync/ami --region your-region
```

2. Execute o comando. Na saída, anote a "Value" propriedade com o ID da DataSync AMI.

Example Exemplo de comando e saída

```
aws ssm get-parameter --name /aws/service/datasync/ami --region us-east-1

{
  "Parameter": {
    "Name": "/aws/service/datasync/ami",
    "Type": "String",
    "Value": "ami-1234567890abcdef0",
    "Version": 6,
    "LastModifiedDate": 1569946277.996,
    "ARN": "arn:aws:ssm:us-east-1::parameter/aws/service/datasync/ami"
  }
}
```

Para implantar seu EC2 agente da Amazon

 Tip

Para evitar custos de transferência entre as zonas de disponibilidade, implante o agente de modo que ele não exija tráfego de rede entre as zonas de disponibilidade. (Para saber mais sobre os preços de transferência de dados para todas as Regiões da AWS, consulte os [preços do Amazon EC2 Data Transfer](#).)

Por exemplo, implante o agente na zona de disponibilidade em que o sistema autogerenciado de armazenamento na nuvem está localizado.

1. Copie o seguinte URL:

```
https://console.aws.amazon.com/ec2/v2/home?region=agent-region#LaunchInstanceWizard:ami=ami-id
```

- Substitua *agent-region* pela região na qual você deseja implantar o agente.
 - *ami-id* Substitua pela ID da DataSync AMI que você obteve.
2. Cole o URL no navegador.

A página de lançamento da EC2 instância da Amazon é AWS Management Console exibida.
 3. Em Tipo de instância, escolha uma das [EC2 instâncias recomendadas da Amazon](#) para DataSync.
 4. Em Par de chaves, escolha um par de chaves existente ou crie outro.
 5. Em Configurações da rede, escolha Editar e, em seguida, faça o seguinte:
 - a. Em VPC, escolha uma VPC na qual você deseja implantar o agente.
 - b. Em Atribuição automática de IP público, escolha se você deseja que seu agente possa ser acessado pela Internet pública.

Mais tarde, use o endereço IP público ou privado da instância para ativar seu agente.
 - c. Em Firewall (grupos de segurança), crie ou selecione um grupo de segurança que faça o seguinte:
 - Se necessário, permite tráfego de entrada para a EC2 instância da Amazon na porta 80 (HTTP). Algumas opções para [obter uma chave de ativação do agente](#) exigem essa conexão.
 - Permite tráfego de entrada e saída entre a EC2 instância da Amazon e o sistema de armazenamento para o qual você está transferindo dados. Para obter mais informações, consulte [Requisitos de rede para armazenamento on-premises, autogerenciado, em outra nuvem e a na borda](#).

 Note

Há mais configurar portas para serem configuradas dependendo do tipo de [endpoint de serviço](#) que o agente usa.

6. (Recomendado) Para aumentar a performance ao transferir de um sistema de arquivos baseado na nuvem, expanda Detalhes avançados e escolha um valor de Grupo de posicionamento onde o armazenamento está localizado.
7. Escolha Launch instance para iniciar sua EC2 instância Amazon.
8. Quando o status da instância for Em execução, escolha a instância.
9. Se você configurou sua instância para ser acessada pela Internet pública, anote o endereço IP público da instância. Caso contrário, anote o endereço IP privado.

Você precisa desse endereço IP para [ativar seu agente](#).

Exemplos: implantando seu EC2 agente em um Região da AWS

A orientação a seguir pode ajudar com cenários comuns se você implantar um agente DataSync em uma Região da AWS.

Tópicos

- [Implantando seu agente para transferências entre armazenamento em nuvem e serviços AWS de armazenamento](#)
- [Implantando seu agente para transferências entre o Amazon S3 AWS e sistemas de arquivos](#)

Implantando seu agente para transferências entre armazenamento em nuvem e serviços AWS de armazenamento

Para transferir dados entre Contas da AWS ou entre sistemas de armazenamento em nuvem, o DataSync agente deve estar localizado no mesmo sistema de arquivos de origem Região da AWS e Conta da AWS onde reside. Esse tipo de transferência inclui os seguintes campos:

- Transferências entre o Amazon EFS ou FSx o Amazon para AWS armazenamento em um local diferente Conta da AWS.
- Transferências de sistemas de arquivos autogerenciados para serviços AWS de armazenamento.

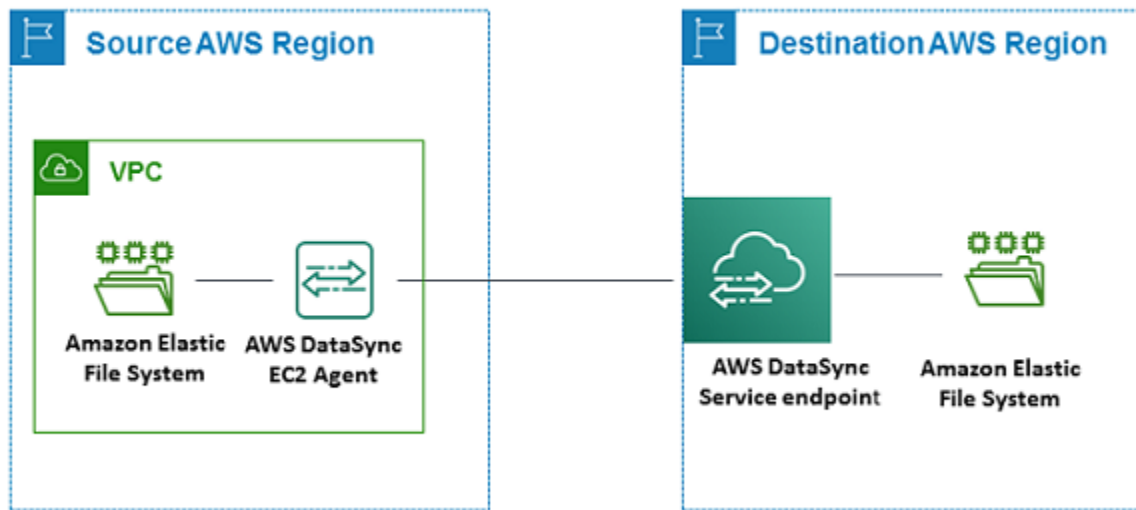
Important

Implante seu agente de forma que ele não exija tráfego de rede entre as zonas de disponibilidade (para evitar cobranças por esse tráfego).

- Para acessar seu sistema de arquivos Amazon EFS ou FSx Windows File Server, implante o agente em uma zona de disponibilidade que tenha um destino de montagem em seu sistema de arquivos.
- Para sistemas de arquivos autogerenciados, implante o agente na zona de disponibilidade em que seu sistema de arquivos reside.

Para saber mais sobre os preços de transferência de dados para todas as Regiões da AWS, consulte os [preços do Amazon EC2 On-Demand](#).

Por exemplo, o diagrama a seguir mostra uma visão de alto nível da DataSync arquitetura para transferir dados do Network File System (NFS) na nuvem para o NFS na nuvem ou Amazon S3.

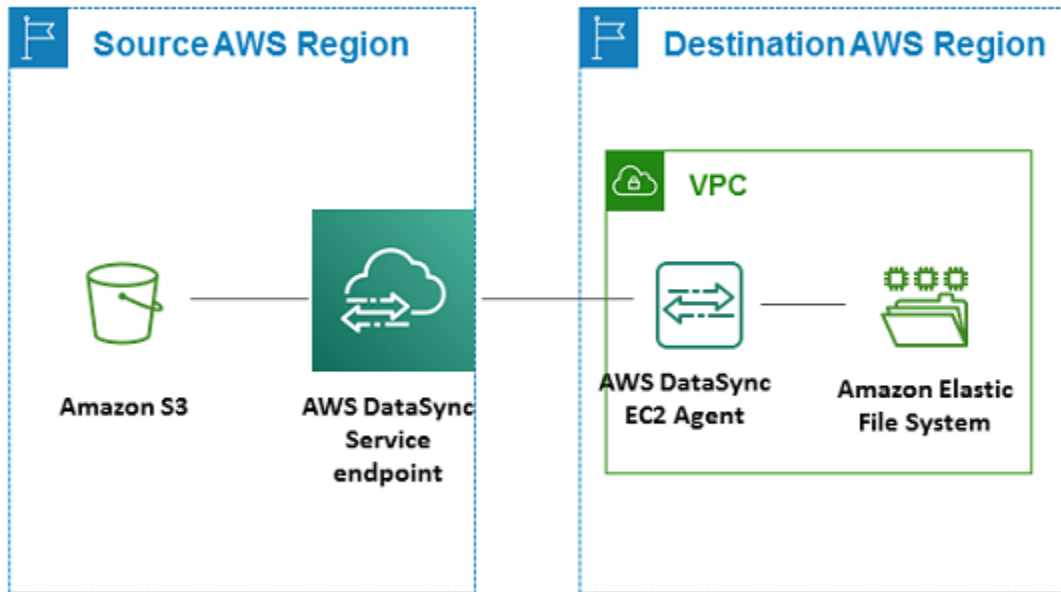


Lembre-se do seguinte ao transferir entre Contas da AWS serviços AWS de armazenamento:

- Ao transferir entre sistemas de arquivos Amazon EFS ou sistemas de FSx arquivos Amazon usando o protocolo NFS, configure seu sistema de arquivos de origem como um local [NFS](#).
- Ao transferir entre sistemas de FSx arquivos da Amazon usando o protocolo SMB, configure seu sistema de arquivos de origem como um local [SMB](#).

Implantando seu agente para transferências entre o Amazon S3 AWS e sistemas de arquivos

O diagrama a seguir fornece uma visão de alto nível da DataSync arquitetura de transferência de dados do Amazon S3 para AWS um sistema de arquivos, como o Amazon EFS ou o Amazon FSx. Você pode usar essa arquitetura para transferir dados de um Conta da AWS para outro ou transferir dados do Amazon S3 para um sistema de arquivos autogerenciado na nuvem.



Implantação do agente no AWS Snowball Edge

Para obter mais informações e instruções, consulte [Criação de um DataSync agente em seu ambiente de armazenamento local](#) para armazenamento compatível com o Amazon S3.

Implantando seu agente em AWS Outposts

Você pode iniciar uma EC2 instância DataSync da Amazon em seu Outpost. Para saber mais sobre como iniciar uma AMI em AWS Outposts, consulte [Executar uma instância em seu Outpost](#) no Guia do AWS Outposts usuário.

Ao usar DataSync para acessar o Amazon S3 em Outposts, você deve iniciar o agente em uma VPC que tenha permissão para acessar seu ponto de acesso Amazon S3 e ativar o agente na região principal do Outpost. O agente também deve ser capaz de rotear o bucket para o endpoint do Amazon S3 no Outposts. Para saber mais sobre como trabalhar com o Amazon S3 em endpoints do Outposts, consulte [Trabalhando com o Amazon S3 no Outposts](#) no Guia do usuário do Amazon S3.

Escolha de um endpoint de serviço para o agente do AWS DataSync

Um [endpoint de serviço](#) é a forma como seu AWS DataSync [agente se comunica com o DataSync](#) serviço. DataSync oferece suporte aos seguintes tipos de endpoints de serviço:

- Endpoint público: os dados são enviados pela Internet pública.
- Endpoint de serviço Federal Information Processing Standard (FIPS): os dados são enviados pela Internet pública usando processos conformes com o FIPS.
- Endpoint de serviço da nuvem privada virtual (VPC): os dados são enviados pela VPC em vez de pela Internet pública, aumentando a segurança dos dados transferidos.

Você precisa de um endpoint de serviço FIPS para [ativar o agente](#). Ao escolher um endpoint de serviço, lembre-se do seguinte:

- Um agente só pode usar um tipo de endpoint. Se você precisar transferir dados usando diferentes tipos de endpoints, crie um agente para cada tipo.
- Como você [conecta sua rede de armazenamento à AWS](#) determina quais endpoints de serviço você pode usar.

Escolha um endpoint de serviço público

Se você usa um endpoint de serviço público, toda a comunicação entre seu DataSync agente e o DataSync serviço ocorre pela Internet pública.

1. Determine o [endpoint de serviço DataSync público](#) que você deseja usar.
2. [Configure sua rede](#) para permitir o tráfego necessário para usar endpoints de serviço DataSync público.

Próxima etapa: [Ativando seu agente AWS DataSync](#)

Escolha de um endpoint de serviço FIPS

DataSync fornece alguns endpoints de serviço que estão em conformidade com o FIPS. Para obter mais informações, consulte [Endpoints FIPS](#) no Referência geral da AWS.

1. Determine o [endpoint do serviço DataSync FIPS](#) que você deseja usar.
2. [Configure sua rede](#) para permitir o tráfego necessário para usar os endpoints de serviço DataSync FIPS.

Próxima etapa: [Ativando seu agente AWS DataSync](#)

Escolha um endpoint de serviço da VPC

Se você usa um endpoint de serviço VPC, seus dados não são transferidos pela Internet pública. DataSync em vez disso, transfere dados por meio de uma VPC baseada no serviço Amazon VPC.

Sumário

- [Como DataSync os agentes trabalham com os endpoints de serviço da VPC](#)
- [DataSync limitações com VPCs](#)
- [Criação de um endpoint de serviço VPC para DataSync](#)

Como DataSync os agentes trabalham com os endpoints de serviço da VPC

Os endpoints de serviço VPC são fornecidos pela AWS PrivateLink. Esses tipos de endpoints permitem que você se conecte de forma privada com suporte Serviços da AWS à sua VPC. Quando você usa um endpoint de serviço de VPC com DataSync, toda a comunicação entre seu DataSync agente e o DataSync serviço permanece na sua VPC.

O endpoint do serviço VPC (junto com as [interfaces de rede](#) DataSync criadas para o tráfego de transferência de dados) são endereços IP privados que só podem ser acessados de dentro da sua VPC. Para obter mais informações, consulte [Conexão da sua rede para transferências do AWS DataSync](#).

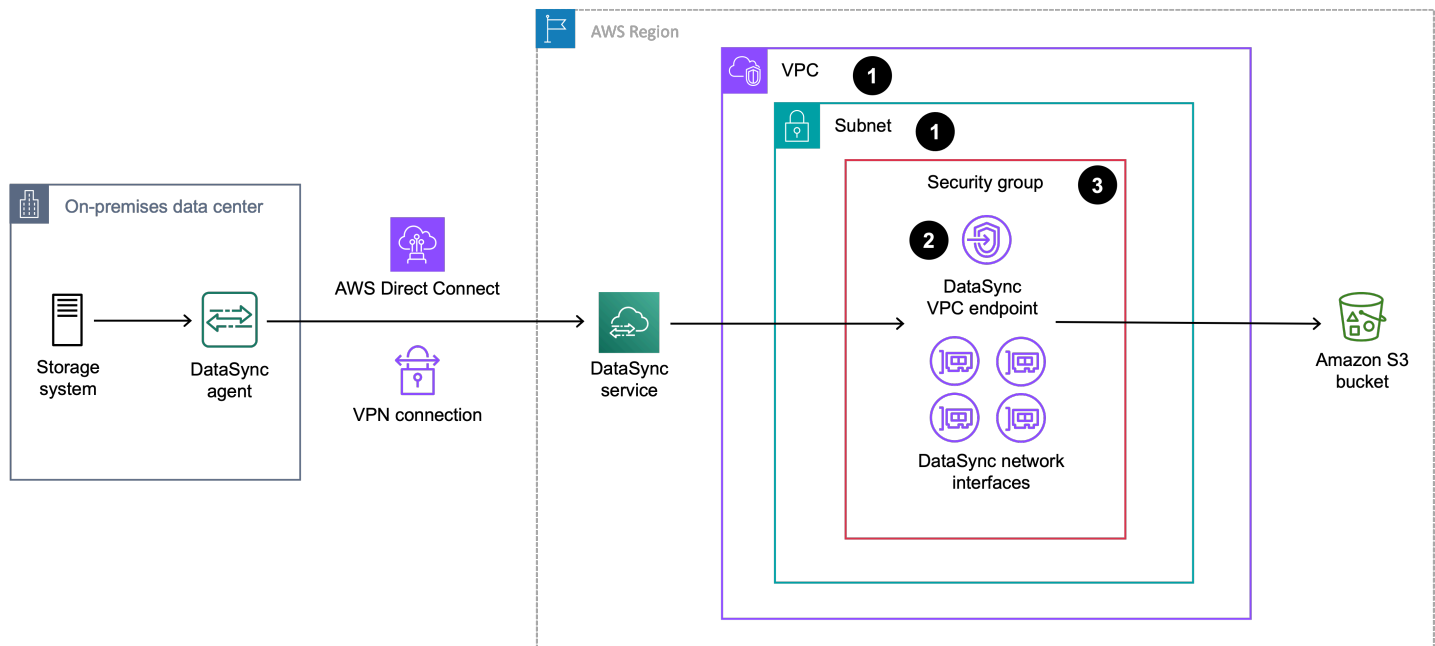
DataSync limitações com VPCs

- VPCs que você usa com DataSync deve ter locação padrão. VPCs com locação dedicada não são suportadas.
- DataSync não suporta [compartilhamento VPCs](#).
- DataSync Suporte somente para endpoints de serviço VPC. IPv4 [IPv6 e as opções de pilha dupla não são suportadas](#).

Criação de um endpoint de serviço VPC para DataSync

Você cria um endpoint de serviço de VPC para DataSync uma VPC que você gerencia. Seu endpoint de serviço, VPC DataSync e agente devem pertencer ao mesmo. Conta da AWS

O diagrama a seguir mostra um exemplo do DataSync uso de um endpoint de serviço VPC para transferência de um sistema de armazenamento local para um bucket do Amazon S3. As legendas numeradas correspondem às etapas para criar um endpoint de serviço da VPC.



Para criar um endpoint de serviço VPC para DataSync

1. [Crie](#) ou determine uma VPC e uma sub-rede em que você deseja criar o endpoint de serviço da VPC.

Se você estiver transferindo de ou para um armazenamento externo AWS, a VPC deve se estender a esse ambiente de armazenamento (por exemplo, seu ambiente de armazenamento pode ser um data center onde seu servidor de arquivos NFS local está localizado). Você pode fazer isso usando regras de roteamento pela [AWS Direct Connect](#) ou pela VPN.

2. Crie um endpoint de serviço DataSync VPC fazendo o seguinte:
 - a. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
 - b. No painel de navegação, selecione Endpoints e depois Criar endpoint.
 - c. Em Service category (Categoria de serviço), escolha Serviços da AWS.

- d. Em Serviços, pesquise **datasync** e escolha o endpoint da região em que você está (por exemplo, com `.amazonaws.us-east-1.datasync`).
- e. Em VPC, escolha a VPC na qual você deseja criar o endpoint de serviço da VPC.
- f. Expanda Configurações adicionais e desmarque a caixa de seleção Habilitar nome DNS privado para desabilitar essa configuração.

Recomendamos desabilitar essa configuração se você tiver agentes na mesma VPC que precisem usar um endpoint de serviço público. Um agente não pode acessar um [endpoint de serviço público](#) pela rede quando essa configuração está habilitada.

- g. Em Sub-rede, escolha a sub-rede na qual você deseja criar o endpoint de serviço da VPC. Anote o ARN da sub-rede (você precisa disso ao ativar o agente).
 - h. Escolha Criar endpoint. Anote o ID do endpoint (você precisa disso ao ativar o agente).
3. Na sua VPC, configure um [grupo de segurança](#) que permita o tráfego necessário para usar os endpoints de serviço da DataSync [VPC](#). Anote o ARN do grupo de segurança (você precisa disso ao ativar o agente).

O grupo de segurança deve permitir que o agente se conecte aos endereços IP privados do endpoint do serviço da VPC e às [interfaces de rede](#) (que são criadas quando você cria a tarefa).

Próxima etapa: [Ativando seu agente AWS DataSync](#)

Ativando seu agente AWS DataSync

Para concluir a criação do seu AWS DataSync agente, você deve ativá-lo. Esta etapa associa o agente ao seu Conta da AWS.

Note

Você não pode ativar um agente em mais de um Conta da AWS e Região da AWS ao mesmo tempo.

Pré-requisitos

Para ativar seu DataSync agente, verifique se você tem as seguintes informações:

- O [endpoint DataSync de serviço](#) com o qual você está ativando seu agente.

Se você estiver usando um endpoint de serviço da VPC, precisará destes detalhes:

- ID do endpoint de serviço da VPC.
- A sub-rede em que o endpoint de serviço da VPC está localizado.
- O grupo de segurança que permite o tráfego necessário para usar endpoints de [serviço DataSync VPC](#).
- O endereço IP ou o nome do domínio do agente.

Como você encontra isso depende do tipo de agente que você [implanta](#). Por exemplo, se seu agente for uma EC2 instância da Amazon, você pode encontrar seu endereço IP acessando a página da instância no EC2 console da Amazon.

Obtenção de uma chave de ativação

Você pode obter uma chave de ativação para seu DataSync agente implantado de algumas maneiras diferentes. Algumas opções requerem acesso ao agente na porta 80 (HTTP). Se você usar uma dessas opções, DataSync feche a porta depois de ativar o agente.

Note

As chaves de ativação do agente expiram em 30 minutos se não forem usadas.

DataSync console

Ao [ativar seu agente no DataSync console](#), você DataSync pode obter a chave de ativação para você usando a opção Obter automaticamente a chave de ativação do seu agente.

Para usar essa opção, é necessário que o navegador possa alcançar o agente na porta 80.

Agent local console

Ao contrário das outras opções para obter uma chave de ativação, essa opção não exige que o agente esteja acessível na porta 80.

1. Faça login no [console local](#) da máquina virtual (VM) do seu agente ou EC2 instância da Amazon.
2. No menu principal AWS DataSync Ativação - Configuração, digite **0** para obter uma chave de ativação.

3. Insira o em Região da AWS que você está ativando seu agente.
4. Insira o tipo de endpoint de serviço que seu agente está usando.
5. Copie a chave de ativação exibida.

Por exemplo: F0EFT-7FPPR-GG7MC-3I9R3-27D0H

Você especifica essa chave ao [ativar o agente](#).

CLI

Com as ferramentas padrão do Unix, você pode executar uma solicitação de `curl` no endereço IP do agente para obter a chave de ativação.

Para usar essa opção, é necessário que o cliente possa alcançar o agente na porta 80. Você pode executar o seguinte comando para verificar:

```
nc -vz agent-ip-address 80
```

Depois de confirmar que pode alcançar o agente, execute um dos comandos a seguir, dependendo do tipo de endpoint de serviço que você esteja usando:

- Endpoints de serviço público:

```
curl "http://agent-ip-address?gatewayType=SYNC&activationRegion=your-region&no_redirect"
```

- Endpoints de serviço FIPS:

```
curl "http://agent-ip-address?gatewayType=SYNC&activationRegion=your-region&endpointType=FIPS&no_redirect"
```

- Endpoints de serviço da VPC:

```
curl "http://agent-ip-address?gatewayType=SYNC&activationRegion=your-region&privateLinkEndpoint=vpc-endpoint-ip-address&endpointType=PRIVATE_LINK&no_redirect"
```

Para encontrar o *vpc-endpoint-ip-address*, abra o [console da Amazon VPC](#), escolha Endpoints e selecione seu endpoint de serviço VPC DataSync. Na guia Sub-redes, localize o endereço IP da [sub-rede do endpoint de serviço da VPC](#). Esse é o endereço IP do endpoint.

Esse comando retorna uma chave de ativação. Por exemplo:

F0EFT-7FPPR-GG7MC-3I9R3-27D0H

Você especifica essa chave ao [ativar o agente](#).

Ativação do agente do

Você tem várias opções para ativar seu DataSync agente. Depois de ativado, a AWS [gerencia o agente](#) para você.

DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação à esquerda, escolha Agentes e, em seguida, escolha Criar agente.
3. Na seção Endpoint de serviço, faça o seguinte para especificar o endpoint de serviço para o agente:
 - Para um endpoint de serviço público, escolha Endpoints de serviço público em. *your current Região da AWS*
 - Para um endpoint de serviço FIPS, escolha endpoints de serviço FIPS em. *your current Região da AWS*
 - Para um endpoint de serviço da VPC, faça o seguinte:
 - Escolha Endpoints da VPC usando AWS PrivateLink.
 - Em Endpoint da VPC, escolha o endpoint de serviço da VPC que você deseja que o agente use.
 - Em Sub-rede, escolha a sub-rede em que seu endpoint de serviço da VPC está localizado.
 - Em Grupo de segurança, escolha o grupo de segurança que permite o tráfego necessário para usar endpoints de [serviço DataSync VPC](#).
4. Na seção Chave de ativação, faça uma das seguintes alternativas para especificar a chave de ativação do agente:
 - Escolha Obter automaticamente a chave de ativação do seu agente DataSync para obter a chave para você.
 - Em Endereço do agente, insira o endereço IP ou nome de domínio do agente.

- Escolha Obter chave.

Se houver falha na ativação, [verifique sua configuração de rede](#) com base no tipo de endpoint de serviço que você está usando.

- Escolha Inserir a chave de ativação do agente manualmente se não quiser uma conexão entre o navegador e o agente.
- [Obtenha a chave](#) no console local do agente ou usando um comando `curl`.
- De volta ao DataSync console, insira a chave no campo Chave de ativação.

5. (Recomendado) Em Nome do agente, dê ao agente um nome de que você possa se lembrar.
6. (Opcional) Em Tags, insira valores nos campos Chave e Valor para marcar seu agente.

Tags ajudam a gerenciar, filtrar e procurar recursos AWS .

7. Escolha Criar agente.
8. Na página Agentes, verifique o agente está usando o serviço correto para o tipo endpoint.

 Note

Nesse ponto, talvez você note que o agente está offline. Isso acontece por um breve tempo após a ativação do agente.

AWS CLI

1. Depois de [obter a chave de ativação](#), copie um dos seguintes comandos `create-agent`, dependendo do tipo de endpoint de serviço que você está usando:

- Endpoint de serviço público ou FIPS:

```
aws datasync create-agent \  
  --activation-key activation-key \  
  --agent-name name-for-agent
```

- Endpoint de serviço da VPC:

```
aws datasync create-agent \  
  --activation-key activation-key \  
  --agent-name name-for-agent \  
  --vpc-endpoint-id vpc-endpoint-id \  
  --region region
```

```
--subnet-arns subnet-arn \  
--security-group-arns security-group-arn
```

2. Em `--activation-key`, especifique a [chave de ativação do agente](#).
3. (Recomendado) Em `--agent-name`, especifique um nome para o agente de que você possa se lembrar.
4. Se você estiver usando um endpoint de serviço da VPC, especifique as seguintes opções:
 - Em `--vpc-endpoint-id`, especifique o ID do endpoint de serviço da VPC que você está usando.
 - Em `--subnet-arns`, especifique o ARN da sub-rede em que o endpoint de serviço da VPC está localizado.
 - Para `--security-group-arns`, especifique o ARN do grupo de segurança que permite o tráfego necessário para usar endpoints de serviço DataSync [VPC](#).
5. Execute o comando `create-agent`.

Você recebe uma resposta com o ARN do agente que acabou de ativar. Por exemplo:

```
{  
  "AgentArn": "arn:aws:datasync:us-east-1:111222333444:agent/  
agent-0b0addbeef44baca3"  
}
```

6. Verifique se o agente está ativado executando o comando `list-agents`:

```
aws datasync list-agents
```



Note

Nesse ponto, talvez você note que o Status do agente é OFFLINE. Isso acontece por um breve tempo após a ativação do agente.

DataSync API

Depois de [obter sua chave de ativação](#), ative seu agente usando a [CreateAgent](#) operação.

 Note

Quando terminar, talvez você note que o agente está offline. Isso acontece por um breve tempo após a ativação do agente.

Próximas etapas

- [Verifique a conexão do seu agente](#) com seu sistema de armazenamento e com o DataSync serviço.
- Se você tiver problemas ao tentar ativar o agente, obtenha ajuda em [solução de problemas](#).
- Crie o DataSync local que você deseja usar com seu agente. Pode ser um local [on-premises](#) ou em [outra nuvem](#).

Verificação das conexões de rede para o agente

Depois de ativar seu AWS DataSync agente, certifique-se de que ele tenha conectividade de rede com seu sistema de armazenamento e com o DataSync serviço.

Acesso ao console local do agente

Como você acessa o console local depende do tipo de agente que você está usando.

Acessando o console local (VMware ESXiLinux KVM ou Microsoft Hyper-V)

Por motivos de segurança, você não pode se conectar remotamente ao console local da máquina virtual (VM) do DataSync agente.

- Se for a primeira vez que você usa o console local, faça login com as credenciais padrão. O nome de usuário padrão é **admin** e a senha é **password**.

 Note

É recomendável alterar a senha padrão. Para fazer isso, no menu principal do console, digite **5** (ou **6** para VMware VMs) e execute o **passwd** comando para alterar a senha.

Acessando o console local (Amazon EC2)

Para se conectar ao console local de um EC2 agente da Amazon, você deve usar SSH.

Antes de começar: certifique-se de que o grupo de segurança da sua EC2 instância permita acesso com SSH (porta TCP 22).

1. Abra um terminal e copie o seguinte comando ssh:

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-ip-address
```

- Para */path/key-pair-name*, especifique o caminho e o nome do arquivo (.pem) da chave privada necessária para se conectar à sua instância.
 - Em *instance-user-name*, especifique admin.
 - Para *instance-public-ip-address*, especifique o endereço IP público da sua instância.
2. Execute o comando ssh para se conectar à instância.

Uma vez conectado, o menu principal do console local do agente é exibido.

Verificação da conexão do agente com sistema de armazenamento

Teste se seu DataSync agente pode se conectar ao seu sistema de armazenamento. Para obter mais informações, consulte [1. Conexão de rede entre o sistema de armazenamento e o agente](#).

1. [Acesse o console local do agente](#).
2. No menu principal AWS DataSync Ativação - Configuração, digite **3**.
3. Insira uma das seguintes opções:
 - a. Digite **1** para testar uma conexão com o servidor NFS.
 - b. Digite **2** para testar uma conexão de servidor SMB.
 - c. Enter **3** para testar uma conexão com o servidor de armazenamento de objetos.
 - d. Digite **4** para testar uma conexão HDFS.
 - e. Digite **5** para testar uma conexão Microsoft Azure Blob Storage.
4. Insira o endereço IP ou o nome do domínio do servidor de armazenamento.

Lembre-se do seguinte ao inserir o endereço IP ou o nome do domínio:

- Não inclua um protocolo. Por exemplo, insira **mystorage.com** em vez de **https://mystorage.com**.
 - Para HDFS, insira o endereço IP ou o nome de domínio do NameNode ou DataNode no cluster do Hadoop.
5. Se solicitado, insira a porta TCP para conexão com o servidor de armazenamento (por exemplo, **443**).

Veja se o resultado do teste de conectividade foi APROVADO ou REPROVADO.

Verificando a conexão do seu agente com o serviço DataSync

Teste se seu DataSync agente pode se conectar ao DataSync serviço. Para obter mais informações, consulte [2. Conexão de rede entre seu agente e o DataSync serviço](#).

1. [Acesse o console local do agente](#).
2. No menu principal AWS DataSync Ativação - Configuração, insira **2** para começar a testar a conectividade de rede.

Se o agente estiver ativado, a opção Testar conectividade da rede pode ser iniciada sem nenhuma entrada adicional do usuário, porque a região e o tipo de endpoint são obtidos das informações do agente ativado.

3. Insira o tipo de endpoint de DataSync serviço que seu agente usa:
 - a. Para endpoints de serviço público, insira **1** e o Região da AWS local em que seu agente está ativado.
 - b. Para endpoints de serviço FIPS, insira **2** e a região onde o agente está ativado.
 - c. Para endpoints de serviço da VPC, insira **3**.

Você vê uma mensagem APROVADO ou REPROVADO.

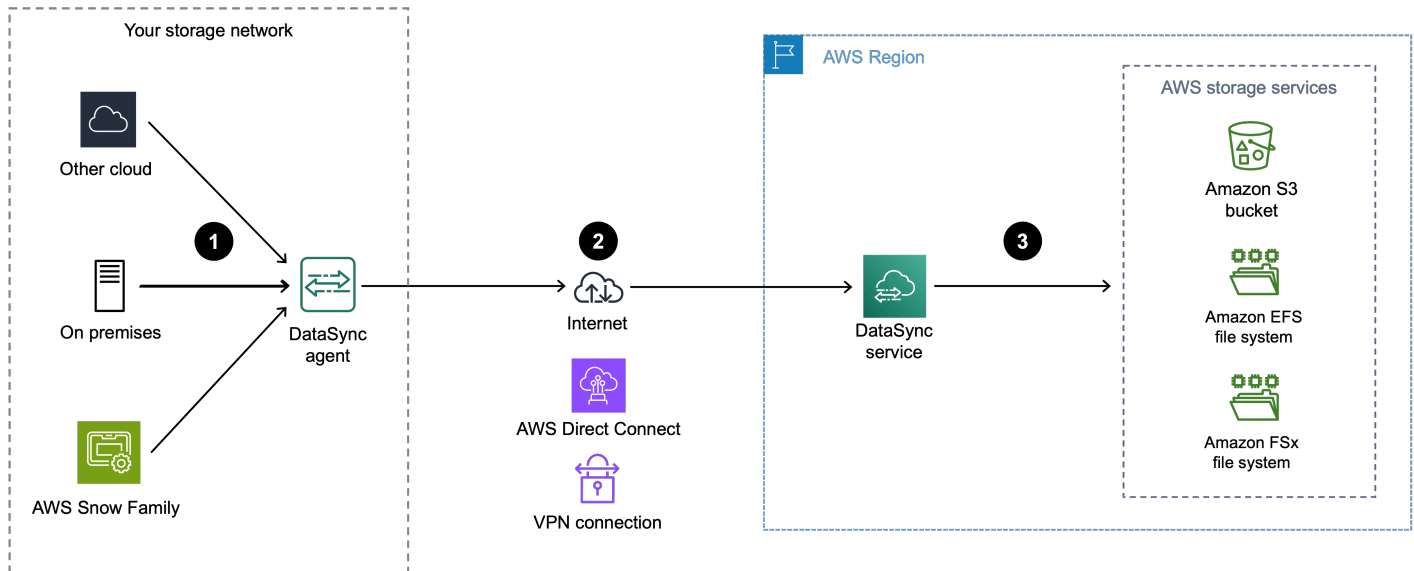
4. Se você vir uma mensagem REPROVADO, verifique sua configuração de rede. Para obter mais informações, consulte [AWS DataSync requisitos de rede](#).

Próximas etapas

Crie o DataSync local que você deseja usar com seu agente. Pode ser um local [on-premises](#) ou em [outra nuvem](#).

Conexão da sua rede para transferências do AWS DataSync

Se [você precisar de um AWS DataSync agente](#), deverá estabelecer várias conexões de rede para uma transferência de dados. O diagrama a seguir mostra as três conexões de rede em uma DataSync transferência de um sistema de armazenamento (que pode estar no local, em outra nuvem ou na borda) para um serviço AWS de armazenamento.



1. Conexão de rede entre o sistema de armazenamento e o agente

Seu DataSync agente se conecta ao seu sistema de armazenamento local, em outra nuvem ou na borda. Para obter mais informações, consulte [Requisitos de rede para armazenamento on-premises, autogerenciado, em outra nuvem e a na borda](#).

2. Conexão de rede entre seu agente e o DataSync serviço

Há alguns aspectos para conectar seu agente ao DataSync serviço. Primeiro, você deve conectar sua rede de armazenamento AWS a. Em segundo lugar, seu agente precisa de um ponto final de serviço com DataSync o qual se comunicar.

Sumário

- [Conexão da sua rede de armazenamento à AWS](#)
- [Escolher um endpoint de serviço](#)

Conexão da sua rede de armazenamento à AWS

Ao usar DataSync, considere as seguintes opções para conectar sua rede de armazenamento a AWS:

- AWS Direct Connect: com o [Direct Connect](#), você pode criar uma conexão dedicada entre a rede de armazenamento e a AWS. De uma DataSync perspectiva, isso permite que você:
 - Transfira dados por um caminho privado para sua nuvem privada virtual (VPC), o que evita o roteamento pela internet pública.
 - Obtenha uma conexão mais previsível do que usar uma rede privada virtual (VPN) para conectar sua rede de armazenamento AWS (especialmente se seu agente for uma EC2 instância da Amazon).
- [Use qualquer tipo de endpoint de DataSync serviço, incluindo endpoints públicos, Federal Information Processing Standard \(FIPS\) ou VPC.](#)

Para obter mais informações, consulte [DataSync exemplos de arquitetura e roteamento com AWS Direct Connect](#).

- VPN - Você pode conectar sua rede de armazenamento AWS usando uma VPN (como [AWS Site-to-Site VPN](#)).
- Internet pública - Você pode conectar sua rede de armazenamento diretamente à DataSync Internet usando um endpoint de serviço [público](#) ou [FIPS](#).

Escolher um endpoint de serviço

Seu agente usa um endpoint de serviço para se comunicar com DataSync. Para obter mais informações, consulte [Escolha de um endpoint de serviço para o agente do AWS DataSync](#).

3. Conexão de rede entre o DataSync serviço e o serviço AWS de armazenamento

Para se conectar DataSync a um serviço AWS de armazenamento, você só precisa se certificar de que o DataSync serviço possa acessar seu bucket ou sistema de arquivos do S3. Para obter mais informações, consulte [Requisitos de rede para serviços de armazenamento AWS](#).

Trabalho em rede quando você não precisa de um DataSync agente

Para transferências que [não exigem um DataSync agente](#), basta garantir que o DataSync serviço possa acessar os sistemas de AWS armazenamento entre os quais você está transferindo. Para obter mais informações, consulte [Requisitos de rede para serviços de armazenamento AWS](#).

Como e onde DataSync o tráfego flui pela rede

DataSync tem um plano de dados e um plano de controle de tráfego. Saber como cada um deles flui pela rede é importante se você quiser separar seu DataSync tráfego.

- Tráfego do plano de dados: inclui os dados de arquivos ou objetos que se movem entre os locais de armazenamento. Na maioria dos casos, o tráfego do plano de dados é roteado por meio de [interfaces de rede](#) que DataSync são geradas e gerenciadas automaticamente quando você cria uma tarefa. O local onde essas interfaces de rede são criadas depende do tipo de serviço de AWS armazenamento para ou do qual você está transferindo e do endpoint de serviço que seu DataSync agente usa.
- Controle o tráfego do avião — Inclui atividades de gerenciamento para seus DataSync recursos. Esse tráfego é roteado pelo endpoint de serviço que o agente usa.

Segurança de rede para DataSync

Para obter informações sobre como seus dados de armazenamento (incluindo metadados) são protegidos durante uma transferência, consulte [AWS DataSync criptografia em trânsito](#).

AWS DataSync requisitos de rede

Configurar sua rede é uma etapa importante na configuração do AWS DataSync. A configuração da sua rede depende de vários fatores, como o tipo de sistema de armazenamento com o qual você está trabalhando. Também se baseia no tipo de endpoint de DataSync serviço que você planeja usar.

Requisitos de rede para armazenamento on-premises, autogerenciado, em outra nuvem e a na borda

Os requisitos de rede a seguir podem ser aplicados a sistemas de armazenamento on-premises, autogerenciados, em outra nuvem e na borda. Normalmente, esses são sistemas de armazenamento que você gerencia ou que podem ser gerenciados por outro provedor de nuvem.

Note

Dependendo da sua rede, talvez seja necessário permitir o tráfego em portas diferentes das listadas aqui para que seu DataSync agente se conecte ao seu armazenamento.

De	Para	Protocolo	Port (Porta)	Como é usado por DataSync
DataSync agente	Servidor de arquivos NFS	TCP	2049 (para NFS versão 4.1 e 4.0) 111 e 2049 (para as NFS versão 3.x)	Monta o servidor de arquivos NFS. DataSync suporta as versões 3.x, 4.0 e 4.1 do NFS.
DataSync agente	Servidor de arquivos SMB	TCP	139 or 445	Monta o servidor de arquivos SMB. DataSync oferece suporte às versões 1.0 e posteriores do SMB. Por motivos de segurança, recomendamos usar a versão 3.0.2 ou posterior do SMB. Versões anteriores, como a SMB 1.0, contêm

De	Para	Protocolo	Port (Porta)	Como é usado por DataSync
				vulnerabilidades de segurança conhecidas que os invasores podem explorar para compromet er seus dados.

De	Para	Protocolo	Port (Porta)	Como é usado por DataSync
DataSync agente	Armazenamento de objetos	TCP	443 (HTTPS) ou 80 (HTTP)	Acessa seu armazenam ento de objetos compatível com o Amazon S3 no local ou em outras nuvens.

 **Note**
Depenc o do armaze ento de objetos pode ser necessa o permitir tráfego em portas HTTPS e HTTP não padrão (como 8443 ou 8080).

De	Para	Protocolo	Port (Porta)	Como é usado por DataSync
DataSync agente	Cluster Hadoop	TCP	NameNode porta (o padrão é 8020) Na maioria dos clusters, você pode encontrar esse número de porta no arquivo <code>core-site.xml</code> sob a propriedade <code>fs.default</code> ou <code>fs.default.name</code> (dependendo da distribuição do Hadoop).	Acessa o NameNodes em seu cluster Hadoop. Especifique a porta usada ao criar um local HDFS.

De	Para	Protocolo	Port (Porta)	Como é usado por DataSync
DataSync agente	Cluster Hadoop	TCP	DataNode porta (o padrão é 50010) Na maioria dos clusters, você pode encontrar esse número de porta no arquivo <code>hdfs-site.xml</code> abaixo da propriedade <code>dfs.datanode.address</code>.	Acessa o DataNodes em seu cluster Hadoop. O DataSync agente determina automaticamente a porta a ser usada.
DataSync agente	Servidor de gerenciamento de chaves Hadoop (KMS)	TCP	Porta KMS (o padrão é 9600)	Acessa o KMS do seu cluster Hadoop.
DataSync agente	Servidor Kerberos Key Distribution Center (KDC)	TCP	Porta (o padrão é 88)	É autenticado com o reino Kerberos. Essa porta é usada somente com locais HDFS e SMB que usam a autenticação Kerberos.

De	Para	Protocolo	Port (Porta)	Como é usado por DataSync
DataSync agente	Interface de gerenciamento do sistema de armazenamento	TCP	Depende da sua rede	Conecta-se ao seu sistema de armazenamento.

Requisitos de rede para serviços de armazenamento AWS

As portas de rede necessárias DataSync para se conectar a um serviço AWS de armazenamento durante uma transferência variam.

De	Para	Protocolo	Port (Porta)
DataSync serviço	Amazon EFS	TCP	2049
DataSync serviço	FSx para Windows File Server	Consulte controle de acesso ao sistema de arquivos FSx para Windows File Server .	
DataSync serviço	FSx para Lustre	Consulte controle de acesso ao sistema de arquivos FSx para Lustre .	
DataSync serviço	FSx para OpenZFS	Consulte controle de acesso ao sistema de arquivos FSx para OpenZFS .	
DataSync serviço	FSx para ONTAP	TCP	111, 635 e 2049 (NFS) 445 (SMB)
DataSync serviço	Amazon S3	N/A (DataSync conecta-se aos buckets do S3 em seu nome)	

Requisitos de rede para endpoints de serviço públicos ou FIPS

Seu DataSync agente exige o seguinte acesso à rede ao usar endpoints de serviço público ou FIPS. Se você usar um firewall ou roteador para filtrar ou limitar o tráfego de rede, configure o firewall ou o roteador para permitir esses endpoints de serviço.

De	Para	Protocolo	Port (Porta)	Como é utilizado	Endpoints acessados
Seu navegador da web	DataSync agente	TCP	80 (HTTP)	Permite que seu navegador obtenha a chave de ativação do DataSync agente. Depois de ativado, DataSync fecha a porta 80 do agente. O agente não exige que a porta 80 seja acessível publicamente. O nível necessário de acesso à porta 80 depende da configuração da rede.  Note Você pode	N/D

De	Para	Protocolo	Port (Porta)	Como é utilizado	Endpoints acessados
				obter a chave de ativação sem uma conexão entre o navegador e o agente. Para obter mais informações, consulte Obtenção de uma chave de ativação.	

De	Para	Protocolo	Port (Porta)	Como é utilizado	Endpoints acessados
DataSync agente	Amazon CloudFront	TCP	443 (HTTPS)	Ajuda a inicializar seu DataSync agente antes da ativação.	Regiões da AWS: - d3dvvaliwoko8h.cloudfront.net AWS GovCloud (US) Regiões: - s3.us-gov-west-1.amazonaws.com/fmrse-ndpoints-endpoints-bucket-go4p5gpna6sk
DataSync agente	AWS	TCP	443 (HTTPS)	Ativa seu DataSync agente e o associa ao seu. Conta da AWS É possível bloquear o endpoint público depois da ativação.	activation-region É Região da AWS aqui que você ativa seu DataSync agente. Ativação de endpoint público: - activation.datasyncc.activation-region.amazonaws.com Ativação de endpoint FIPS: - activation.datasyncc-fips.activation-region.amazonaws.com

De	Para	Protocolo	Port (Porta)	Como é utilizado	Endpoints acessados
DataSync agente	AWS	TCP	443 (HTTPS)	Permite a comunicação entre o DataSync agente e o endpoint do DataSync serviço. Para mais informações, consulte Escolha de um endpoint de serviço para o agente do AWS DataSync.	<i>activation-region</i> É Região da AWS aqui que você ativa seu DataSync agente. Dependendo do que você está usando DataSync , talvez não seja necessário permitir o acesso a todos os endpoints listados aqui. DataSync pontos finais do plano de controle: - Endpoint público: cp.datasync.<i>activation-region</i>.amazonaws.com - Endpoint FIPS: cp.datasync-fips.<i>activation-region</i>.amazonaws.com DataSync ponto final do plano de dados (somente para tarefas de transferência): <i>your-task-id</i>.datasync-dp.<i>activation-region</i>.amazonaws.com

De	Para	Protocolo	Port (Porta)	Como é utilizado	Endpoints acessados
Seu cliente	AWS	TCP	443 (HTTPS)	Permite que você faça solicitações de DataSync API.	<i>activation-region</i> É Região da AWS aqui que você ativa seu DataSync agente. Endpoint público: - datasync.<i>activation-region</i>.amazonaws.com Endpoint FIPS: - datasync-fips.<i>activation-region</i>.amazonaws.com
DataSync agente	AWS	TCP	443 (HTTPS)	Permite que o DataSync agente receba atualizações do AWS. Para obter mais informações, consulte Gerencian do seu AWS DataSync agente .	<i>activation-region</i> É Região da AWS aqui que você ativa seu DataSync agente. - amazonlinux.default.amazonaws.com - cdn.amazonlinux.com - amazonlinux-2-repos-<i>activation-region</i>.s3.dualstack.<i>activation-region</i>.amazonaws.com - amazonlinux-2-repos-<i>activation-region</i>.s3.<i>activation-region</i>.amazonaws.com *.s3.<i>activation-region</i>.amazonaws.com

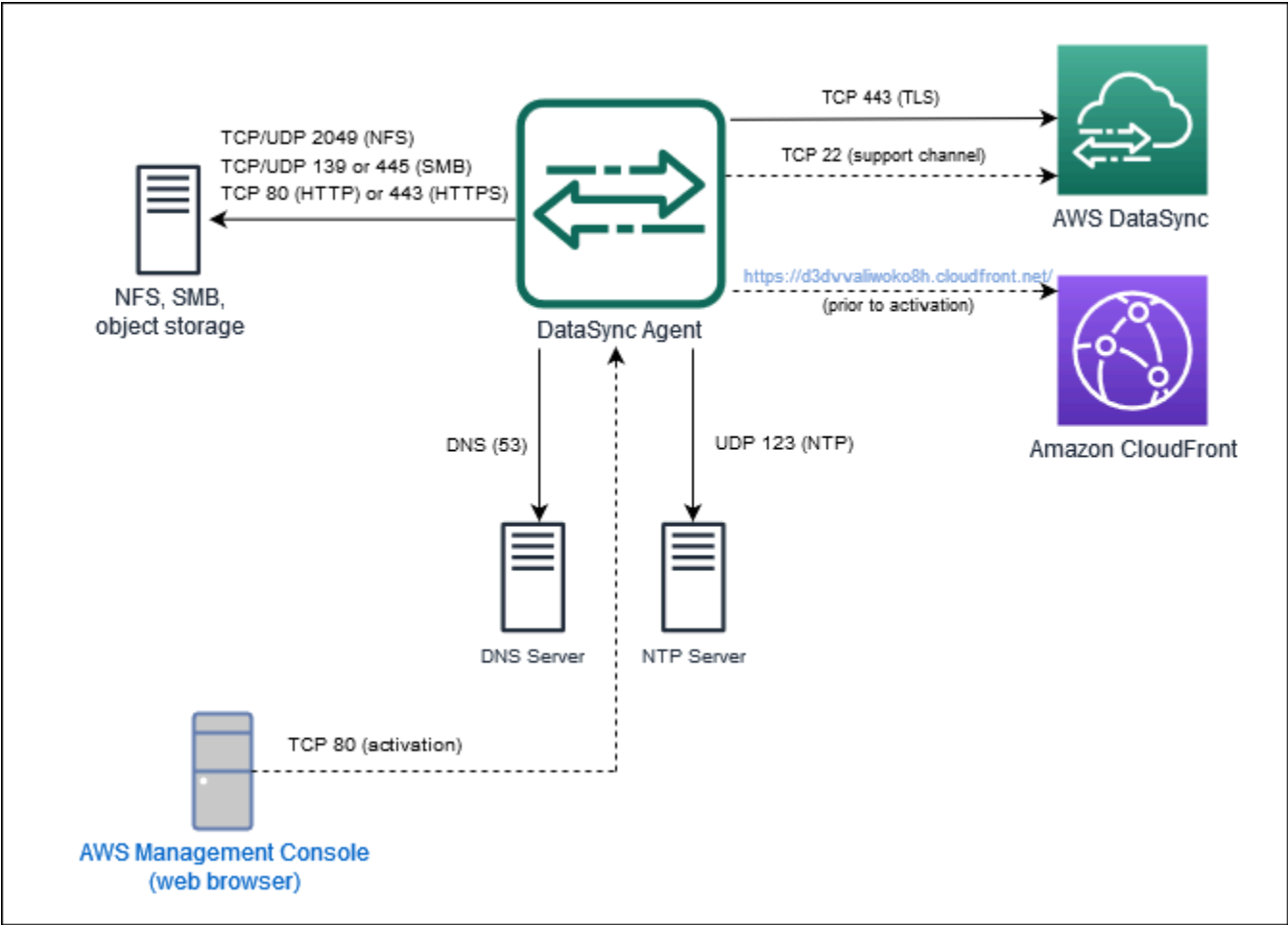
De	Para	Protocolo	Port (Porta)	Como é utilizado	Endpoints acessados
DataSync agente	Servidor Domain Name Service (DNS – Serviço do nome de domínio)	TCP/UDP	53 (DNS)	Permite a comunicação entre o DataSync agente e o servidor DNS.	N/D
DataSync agente	AWS	TCP	22 (Canal de suporte)	Permite AWS Support acessar seu DataSync agente para ajudá-lo a solucionar problemas . Você não precisa dessa porta aberta para operação normal.	AWS Support canal: • 54.201.223.107

De	Para	Protocolo	Port (Porta)	Como é utilizado	Endpoints acessados
DataSync agente	Servidor de Network Time Protocol (NTP)	UDP	123 (NTP)	Permite que sistemas locais sincronizem a hora da VM com a hora do host.	NTP: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org

 **Note**

Se você quiser alterar a configuração NTP padrão do agente do VM para usar um servidor NTP diferente usando o console local, consulte [Sincronizando a hora em seu agente VMware](#).

O diagrama a seguir mostra as portas necessárias DataSync ao usar terminais de serviço público ou FIPS.



Requisitos de rede para endpoints de serviço da VPC

Um endpoint de nuvem privada virtual (VPC) fornece uma conexão privada entre seu agente e AWS que não cruza a Internet nem usa endereços IP públicos. Isso também ajuda a impedir que pacotes entrem ou saiam da rede. Para obter mais informações, consulte [Escolha um endpoint de serviço da VPC](#).

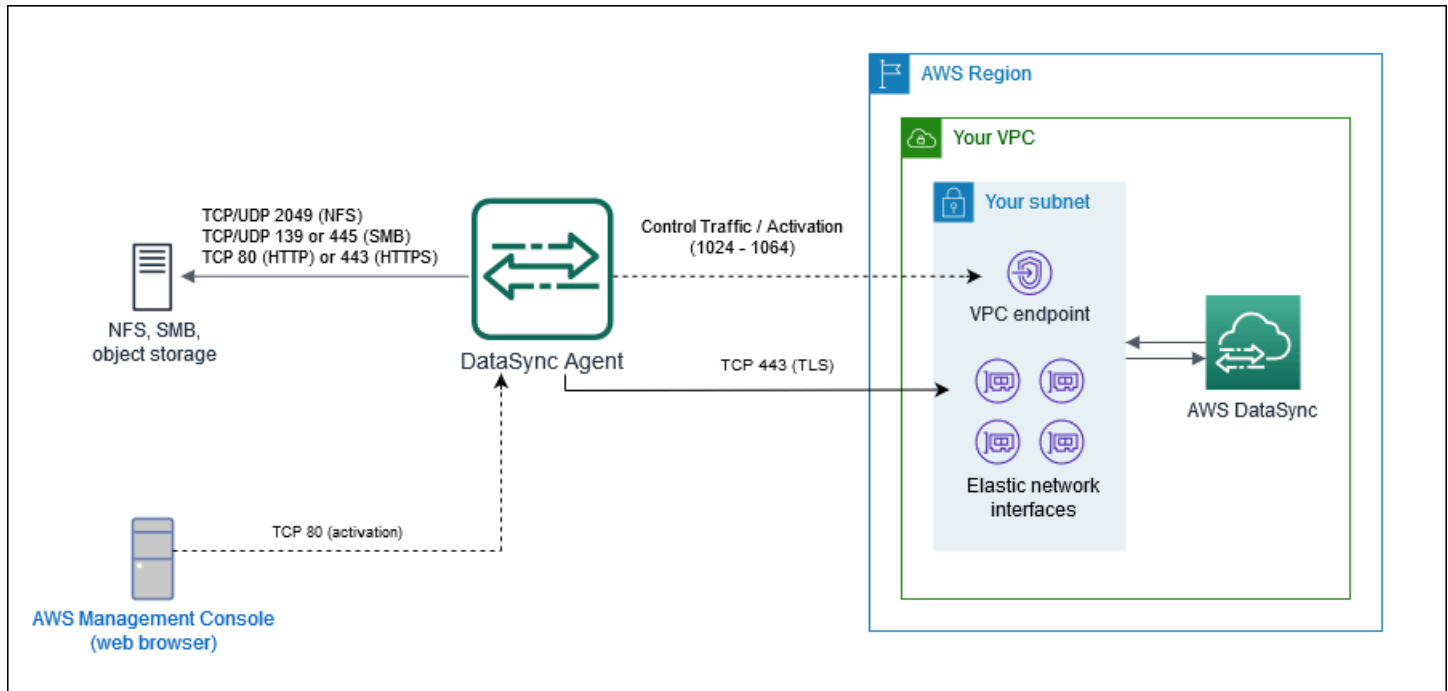
DataSync requer as seguintes portas para que seu agente use um endpoint de serviço VPC.

De	Para	Protocolo	Port (Porta)	Como é utilizado
Seu navegador da web	Seu DataSync agente	TCP	80 (HTTP)	Permite que seu navegador obtenha a chave de ativação do agente. Depois de

De	Para	Protocolo	Port (Porta)	Como é utilizado
				ativado, DataSync fecha a porta 80 do agente. O agente não exige que a porta 80 seja acessível publicamente. O nível necessário de acesso à porta 80 depende da configuração da rede.  Note Você pode obter a chave de ativação sem uma conexão entre o navegador e o agente. Para obter mais informações, consulte Obtenção de uma chave de ativação.

De	Para	Protocolo	Port (Porta)	Como é utilizado
DataSync agente	Seu DataSync endpoint de serviço VPC Para encontrar o endereço IP do endpoint, abra o console da Amazon VPC, escolha Endpoints e selecione seu endpoint de serviço DataSync VPC. Na guia Sub-redes, localize o endereço IP da sub-rede do endpoint de serviço da VPC. Esse é o endereço IP do endpoint.	TCP	1024 a 1064	Para tráfego do ambiente de gerenciamento .
DataSync agente	As interfaces de rede da sua DataSync tarefa Para encontrar os endereços IP dessas interfaces, consulte Visualizar suas interfaces de rede.	TCP	443 (HTTPS)	Para tráfego do plano de dados .
DataSync agente	Seu DataSync endpoint de serviço VPC	TCP	22 (Canal de suporte)	Para permitir AWS Support o acesso ao seu DataSync agente para solução de problemas. Você não precisa dessa porta aberta para operação normal.

O diagrama a seguir mostra as portas necessárias DataSync ao usar os endpoints de serviço VPC.



Interfaces de rede para transferências do AWS DataSync

Para cada tarefa que você cria, gera e gerencia AWS DataSync automaticamente [interfaces de rede](#) para tráfego de transferência de dados. Quantas interfaces de rede são DataSync criadas e onde elas são criadas depende dos seguintes detalhes sobre sua tarefa de transferência:

- Se sua tarefa [requer um DataSync agente](#).
- Seus locais de origem e destino (para onde você está copiando dados de e para onde você está copiando dados).
- O tipo de endpoint de serviço que seu agente usa.

Cada interface de rede usa um único endereço IP em sua sub-rede (quanto mais interfaces de rede houver, mais endereços IP serão necessários). Use as tabelas a seguir para garantir que sua sub-rede tenha endereços IP suficientes para sua tarefa.

Interfaces de rede para transferências com agentes

Em geral, você precisa de um DataSync agente ao copiar dados entre um serviço AWS de armazenamento e um sistema de armazenamento que não esteja AWS.

Local	Interfaces de rede criadas por padrão	Onde as interfaces de rede são criadas ao usar um endpoint público ou FIPS	Onde as interfaces de rede são criadas ao usar um endpoint privado (VPC)
Amazon S3	4	N/D ¹	A sub-rede que você especifica ao ativar seu DataSync agente.
Amazon EFS	4	A sub-rede que você especifica ao criar a localização do Amazon EFS.	
Servidor FSx de arquivos Amazon para Windows	4	A mesma sub-rede do servidor de arquivos preferencial do sistema de arquivos.	
Amazon FSx para Lustre	4	A mesma sub-rede do sistema de arquivos.	
Amazon FSx para OpenZFS	4	A mesma sub-rede do sistema de arquivos.	
Amazon FSx para NetApp ONTAP	4	A mesma sub-rede do sistema de arquivos.	

¹ As interfaces de rede não são necessárias porque o DataSync serviço se comunica diretamente com o bucket do S3.

Interfaces de rede para transferências sem agentes

Você não precisa de um DataSync agente ao copiar dados entre eles Serviços da AWS.

O número total de interfaces de rede depende dos DataSync locais em sua transferência. Por exemplo, a transferência entre o Amazon EFS e os sistemas FSx de arquivos Lustre requer quatro interfaces de rede. Enquanto isso, a transferência entre FSx o Windows File Server e um bucket S3 requer duas interfaces de rede.

Local	Interfaces de rede criadas por padrão	Onde as interfaces de rede são criadas
Amazon S3	N/D ¹	N/D ¹
Amazon EFS	2	A sub-rede que você especifica ao criar a localização do Amazon EFS.
FSx para Windows File Server	2	A mesma sub-rede do servidor de arquivos preferencial para o sistema de arquivos.
FSx para Lustre	2	A mesma sub-rede do sistema de arquivos.
FSx para OpenZFS	2	A mesma sub-rede do sistema de arquivos.
FSx para ONTAP	2	A mesma sub-rede do sistema de arquivos.

¹ As interfaces de rede não são necessárias porque o DataSync serviço se comunica diretamente com o bucket do S3.

Visualizar suas interfaces de rede

Para ver as interfaces de rede alocadas para sua tarefa de DataSync transferência, faça o seguinte:

- Use a operação [DescribeTask](#). A operação retorna SourceNetworkInterfaceArns e DestinationNetworkInterfaceArns com respostas parecidas com estas:

```
arn:aws:ec2:your-region:your-account-id:network-interface/eni-f012345678abcdef0
```

Neste exemplo, o ID da interface de rede é `eni-f012345678abcdef0`.

- No EC2 console da Amazon, pesquise seu ID de tarefa (como `task-f012345678abcdef0`) para encontrar suas interfaces de rede.

DataSync exemplos de arquitetura e roteamento com AWS Direct Connect

Considere as seguintes arquiteturas de rede ao usar o [AWS Direct Connect](#) com as transferências do AWS DataSync .

Tip

Se sua rede usa um gateway de trânsito, recomendamos separar o caminho lógico da DataSync transferência para otimizar os custos (especialmente se você estiver migrando uma grande quantidade de dados).

Por exemplo, se você usa [AWS Transit Gateway](#) para tráfego normal entre suas redes locais e nuvens privadas virtuais (VPCs), você pode configurar sua rede para que o DataSync tráfego ignore o gateway de trânsito e suas cobranças de processamento de dados.

Usando o Direct Connect com um DataSync endpoint de serviço VPC

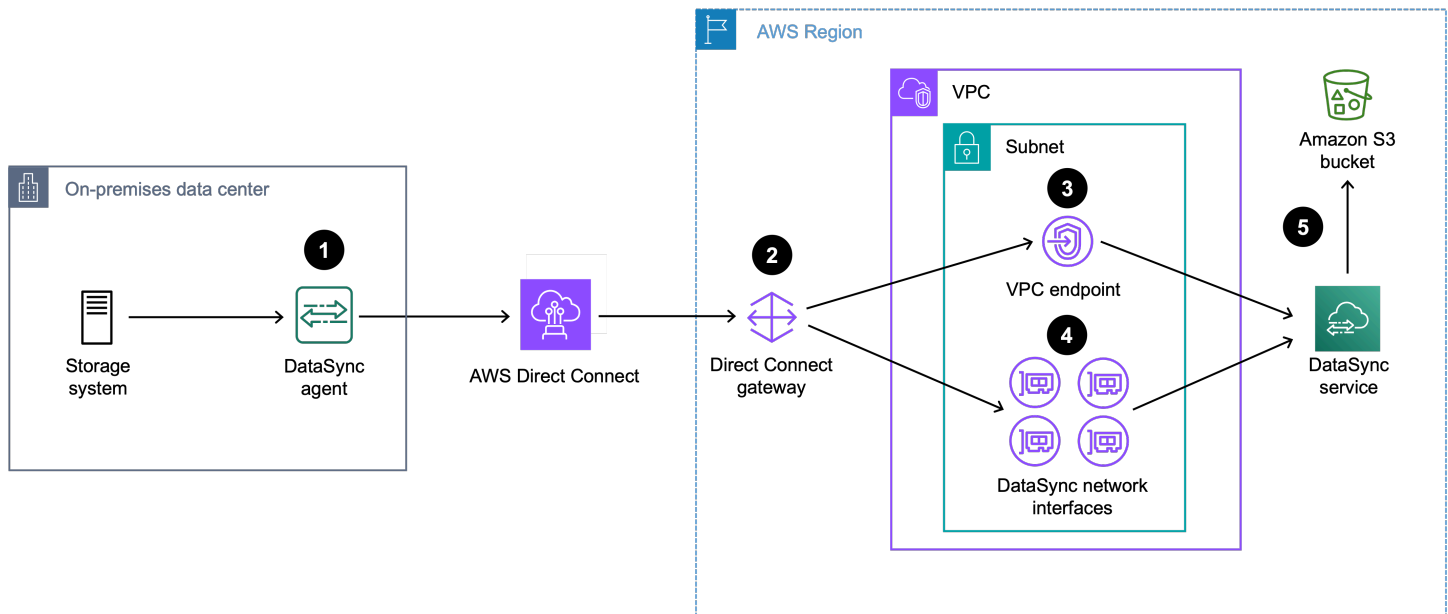
Se seu DataSync agente usa um [endpoint de serviço de VPC](#), você precisa de um [gateway Direct Connect para se conectar](#) à sua VPC.

Sumário

- [Arquitetura do Direct Connect com endpoint da VPC e destino no S3](#)
- [Arquitetura do Direct Connect com endpoint da VPC e destino no sistema de arquivos na mesma sub-rede](#)
- [A arquitetura do Direct Connect com endpoint da VPC e destino no sistema de arquivos em outra sub-rede](#)

Arquitetura do Direct Connect com endpoint da VPC e destino no S3

A arquitetura Direct Connect a seguir mostra uma DataSync transferência de um sistema de armazenamento local para um bucket S3.

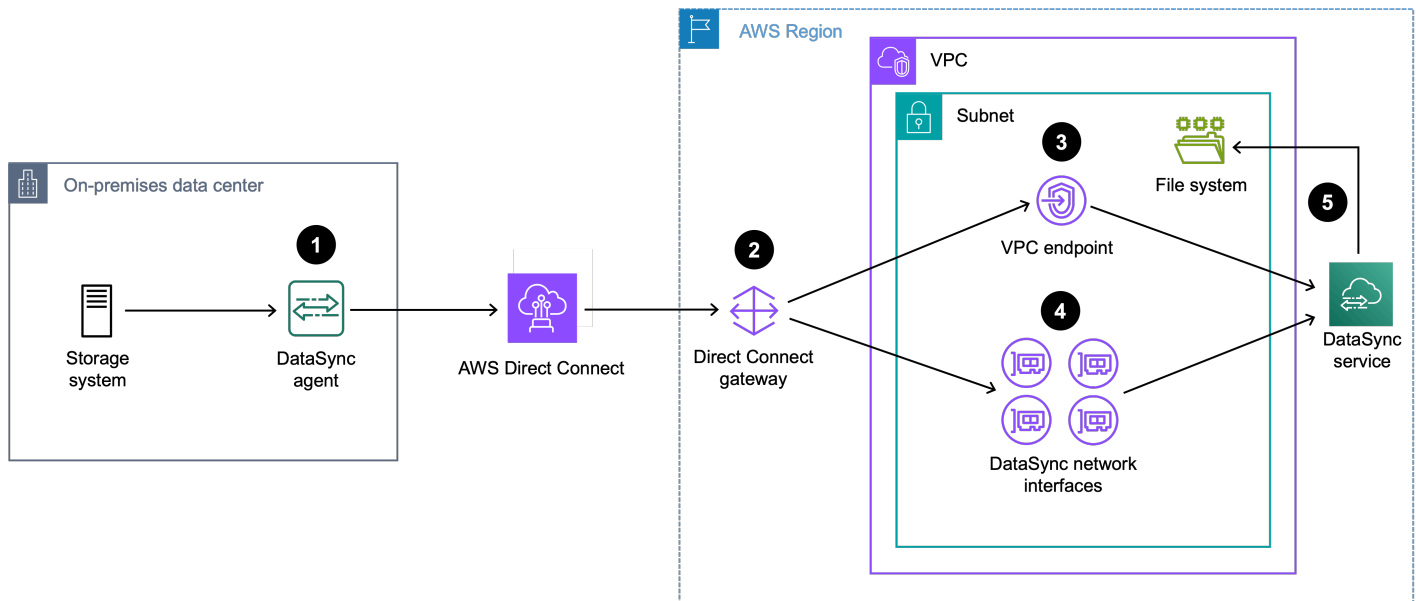


1. O DataSync agente roteia o DataSync tráfego do sistema de armazenamento local (local de origem) para a conexão Direct Connect.
2. DataSync rotas de tráfego para um gateway Direct Connect usado para sua transferência. Para configurar isso, é necessário:
 - a. Associar o gateway do Direct Connect a um [gateway privado virtual](#) para a VPC. [Essa é a VPC em que o DataSync VPC endpoint está localizado e onde a tarefa cria interfaces de rede. DataSync](#)
 - b. Crie uma [interface virtual privada](#) que conecte essa VPC ao gateway do Direct Connect.
3. DataSync rotas de tráfego (plano de controle) pelo DataSync VPC endpoint.
4. DataSync rotas de tráfego (plano de dados) pelas interfaces de DataSync rede na sub-rede que você especifica ao [criar o DataSync agente](#).
5. DataSync rotas de tráfego através do DataSync serviço até o bucket S3 (local de destino).

Arquitetura do Direct Connect com endpoint da VPC e destino no sistema de arquivos na mesma sub-rede

Ao transferir para ou de um sistema de FSx arquivos Amazon EFS ou Amazon, seu sistema de arquivos e o DataSync VPC endpoint podem estar na mesma sub-rede.

A arquitetura Direct Connect a seguir mostra uma DataSync transferência de um sistema de armazenamento local para um Amazon EFS ou sistema de FSx arquivos Amazon.

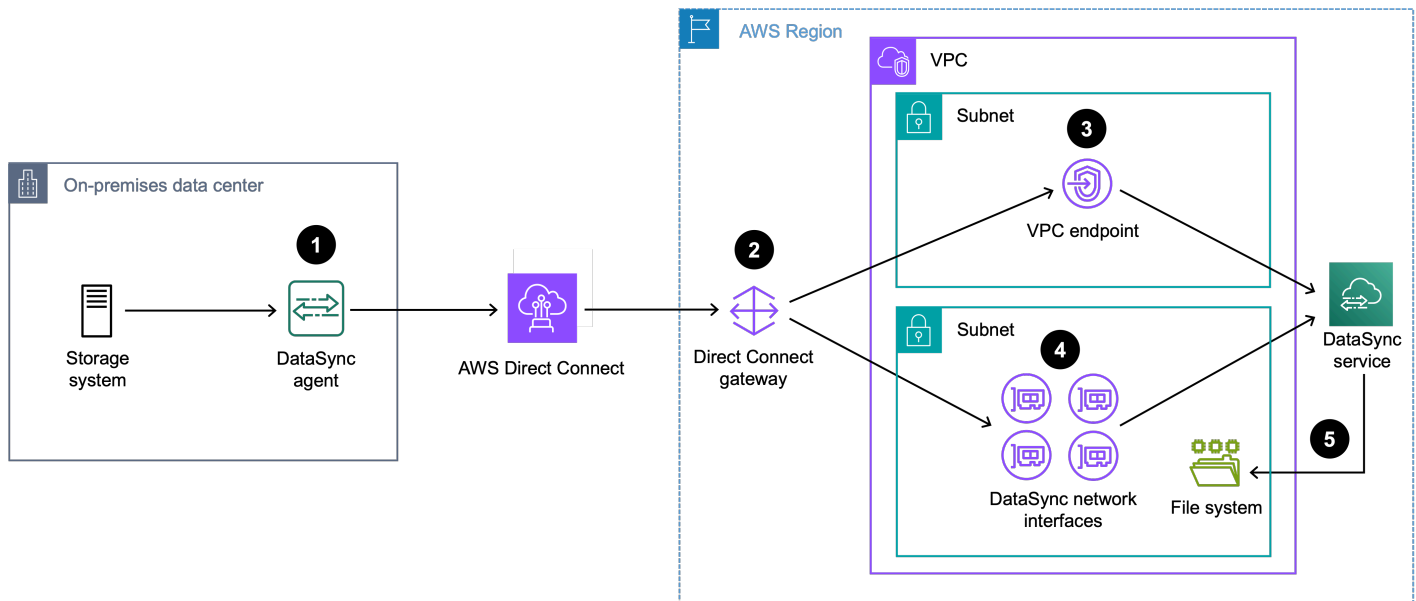


1. O DataSync agente roteia o DataSync tráfego do sistema de armazenamento local (local de origem) para a conexão Direct Connect.
2. DataSync rotas de tráfego para um gateway Direct Connect usado para sua transferência. Para configurar isso, é necessário:
 - a. Associar o gateway do Direct Connect a um [gateway privado virtual](#) para a VPC. Essa é a VPC em que o DataSync VPC endpoint está localizado e onde a DataSync tarefa cria [interfaces de rede](#) para o sistema de arquivos (local de destino).
 - b. Crie uma [interface virtual privada](#) que conecte essa VPC ao gateway do Direct Connect.
3. DataSync rotas de tráfego (plano de controle) pelo DataSync VPC endpoint.
4. DataSync rotas de tráfego (plano de dados) pelas interfaces DataSync de rede na sub-rede do sistema de arquivos. Essa é a mesma sub-rede em que o DataSync VPC endpoint está localizado.
5. DataSync rotas de tráfego através do DataSync serviço para o sistema de arquivos (local de destino).

A arquitetura do Direct Connect com endpoint da VPC e destino no sistema de arquivos em outra sub-rede

Ao transferir para ou de um sistema de FSx arquivos Amazon EFS ou Amazon, seu sistema de arquivos e o DataSync VPC endpoint podem estar em sub-redes diferentes.

A arquitetura Direct Connect a seguir mostra uma DataSync transferência de um sistema de armazenamento local para um Amazon EFS ou sistema de FSx arquivos Amazon.



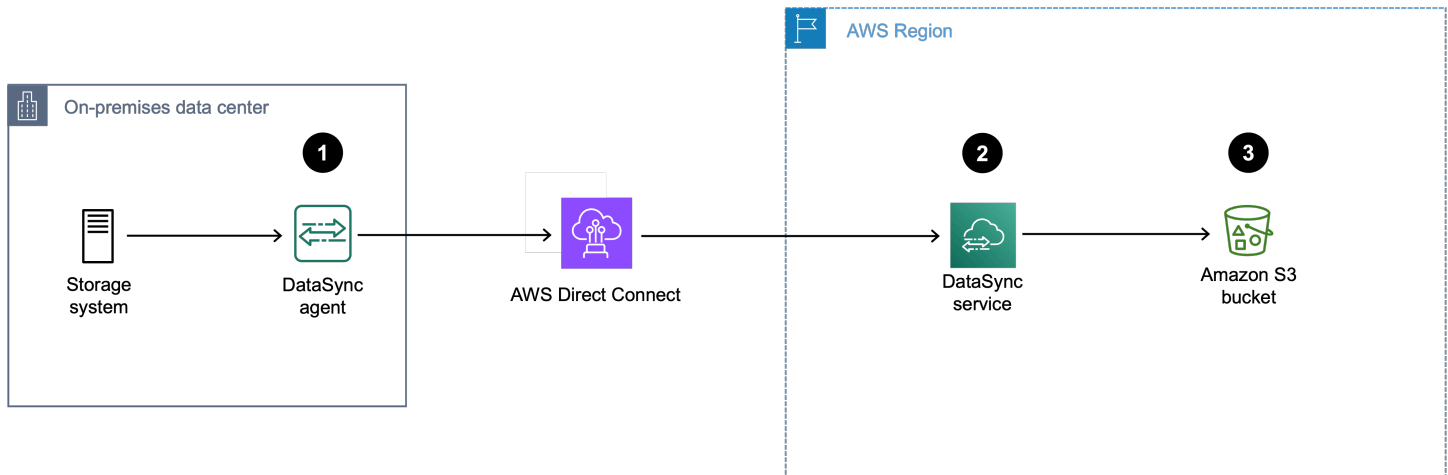
1. O DataSync agente roteia o DataSync tráfego do sistema de armazenamento local (local de origem) para a conexão Direct Connect.
2. DataSync rotas de tráfego para um gateway Direct Connect usado para sua transferência. Para configurar isso, é necessário:
 - a. Associar o gateway do Direct Connect a um [gateway privado virtual](#) para a VPC. Essa é a VPC em que o DataSync VPC endpoint está localizado e onde a DataSync tarefa cria [interfaces de rede](#) para o sistema de arquivos (local de destino).
 - b. Crie uma [interface virtual privada](#) que os conecte VPCs ao gateway Direct Connect.
3. DataSync rotas de tráfego (plano de controle) pelo DataSync VPC endpoint.
4. DataSync rotas de tráfego (plano de dados) pelas interfaces DataSync de rede na sub-rede do sistema de arquivos. Essa é uma sub-rede diferente de onde o DataSync VPC endpoint está localizado.
5. DataSync rotas de tráfego através do DataSync serviço para o sistema de arquivos (local de destino).

Usando o Direct Connect com um DataSync endpoint de serviço público ou FIPS

Se seu DataSync agente usa um endpoint de serviço [público](#) ou [Federal Information Processing Standard \(FIPS\)](#), você pode rotear o tráfego de transferência de dados por meio de uma conexão Direct Connect usando uma interface [virtual pública](#).

Embora o Direct Connect anuncie todos os Região da AWS prefixos locais e remotos por padrão, você pode usar as [tags da comunidade BGP](#) para controlar o escopo (regional ou global) e a preferência de rota do tráfego na interface virtual pública. Você deve anunciar pelo menos um prefixo público para criar seu DataSync agente.

A arquitetura Direct Connect a seguir mostra uma DataSync transferência de um sistema de armazenamento local por meio de um endpoint público ou FIPS para um bucket S3.



1. O DataSync agente roteia o DataSync tráfego do sistema de armazenamento local (local de origem) para a conexão Direct Connect.
2. DataSync rotas de tráfego para o DataSync serviço por meio de uma interface virtual pública.
3. DataSync tráfego para o bucket S3 (local de destino).

Próximas etapas

Se [você precisar de um DataSync agente](#) e ainda não tiver criado um, [implante](#) o agente, [escolha um endpoint de serviço](#) para o agente e, em seguida, [ative](#) o agente.

Depois de criar o agente, você pode [configurar sua rede](#) para DataSync.

Configurando seu AWS DataSync agente para vários NICs

Se você configurar seu AWS DataSync agente para usar vários adaptadores de rede (NICs), o agente poderá ser acessado por mais de um endereço IP. Talvez você queira fazer isso nas seguintes situações:

- Maximização da taxa de transferência: você pode maximizar a taxa de transferência de um agente quando os adaptadores de rede forem um gargalo.
- Isolamento de rede: o Network File System (NFS), Server Message Block (SMB), Sistema de Arquivos Distribuído do Hadoop (HDFS) ou servidor de armazenamento de objetos pode residir em uma LAN virtual (VLAN) que não tem conectividade com a Internet por motivos de segurança.

Em um caso de uso típico de vários adaptadores, um adaptador é configurado como a rota pela qual o agente se comunica AWS (como o agente padrão). Com exceção desse adaptador específico, os locais do NFS, SMB, HDFS ou de Armazenamento de objetos autogerenciados devem estar na mesma sub-rede que o adaptador que se conecta a eles.

Caso contrário, a comunicação com os locais de armazenamento NFS, SMB, HDFS ou de objetos pode não ser possível. Em alguns casos, você pode configurar um local de armazenamento NFS, SMB, HDFS ou de objetos no mesmo adaptador usado para comunicação com AWS. Nesses casos, o tráfego de NFS, SMB, HDFS ou armazenamento de objetos para esse servidor e o AWS tráfego fluem pelo mesmo adaptador.

Em alguns casos, você pode configurar um adaptador para se conectar ao AWS DataSync console e depois adicionar um segundo adaptador. Nesse caso, configura DataSync automaticamente a tabela de rotas para usar o segundo adaptador como a rota preferencial.

Transferência de seus dados com um AWS DataSync

Com AWS DataSync, você pode transferir dados de ou para um armazenamento local AWS, em outras nuvens e na borda.

A configuração de uma DataSync transferência geralmente envolve as seguintes etapas:

1. Determine se DataSync [suporta sua transferência](#).
2. Se [você precisar de um DataSync agente](#) para sua transferência, implante e ative um agente o mais próximo possível de um dos seus sistemas de armazenamento.

Por exemplo, se você fizer uma transferência de um servidor de arquivos Network File System (NFS) on-premises, implante o agente o mais perto possível desse servidor de arquivos.

3. Forneça DataSync acesso ao seu sistema de armazenamento.

DataSync precisa de permissão para ler ou gravar em seu armazenamento (dependendo se o armazenamento é um local de origem ou destino). Por exemplo, saiba como [fornecer DataSync acesso aos servidores de arquivos NFS](#).

4. [Conecte sua rede](#) para obter tráfego entre seu sistema de armazenamento DataSync e.
5. Crie um local para seu sistema de armazenamento usando o DataSync console ou a DataSync API. AWS CLI

Por exemplo, aprenda a [criar um local NFS ou um local do Amazon S3](#).

6. Repita as etapas de 3 a 5 para criar o outro local para a transferência.
7. [Crie e inicie uma tarefa DataSync de transferência](#) que inclua seus locais de origem e destino.

Tópicos

- [Para onde posso transferir meus dados com AWS DataSync?](#)
- [Transferindo de ou para o armazenamento local com AWS DataSync](#)
- [Transferindo de ou para o AWS armazenamento com AWS DataSync](#)
- [Transferindo de ou para outro armazenamento em nuvem com AWS DataSync](#)
- [Transferindo de ou para um armazenamento compatível com S3 no Snowball Edge](#)
- [Criando uma tarefa para transferir seus dados](#)
- [Iniciando uma tarefa para transferir seus dados](#)

Para onde posso transferir meus dados com AWS DataSync?

O local com o qual você pode transferir seus dados AWS DataSync depende dos seguintes fatores:

- [Locais](#) de origem e destino da sua transferência
- Se suas localizações estiverem em locais diferentes Contas da AWS
- Se suas localizações estiverem em locais diferentes Regiões da AWS

Transferências suportadas no mesmo Conta da AWS

DataSync suporta transferências entre os seguintes recursos de armazenamento associados aos mesmos Conta da AWS.

Origem (De)	Destino (Para)
• NFS • SMB • HDFS • Armazenamento de objetos	• Amazon S3 (em Regiões da AWS) • Amazon EFS • Servidor FSx de arquivos Amazon para Windows • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP
• Amazon S3 (em Regiões da AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	• NFS • SMB • HDFS • Armazenamento de objetos
• Google Cloud Storage • Microsoft Azure Blob Storage • Microsoft Azure Files • Wasabi Cloud Storage • DigitalOcean Spaces	• Amazon S3 (em Regiões da AWS) • Amazon EFS • Servidor FSx de arquivos Amazon para Windows • FSx para Lustre • FSx para OpenZFS

Origem (De)	Destino (Para)
• Oracle Cloud Infrastructure Object Storage • Cloudflare R2 Storage • Backblaze B2 Cloud Storage • NAVER Cloud Object Storage • Alibaba Cloud Object Storage Service • IBM Cloud Object Storage • Seagate Lyve Cloud	• FSx para ONTAP
• Amazon S3 (em Regiões da AWS) • Amazon EFS • Servidor FSx de arquivos Amazon para Windows • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	• Google Cloud Storage • Microsoft Azure Blob Storage • Microsoft Azure Files • Wasabi Cloud Storage • DigitalOcean Spaces • Oracle Cloud Infrastructure Object Storage • Cloudflare R2 Storage • Backblaze B2 Cloud Storage • NAVER Cloud Object Storage • Alibaba Cloud Object Storage Service • IBM Cloud Object Storage • Seagate Lyve Cloud
• Armazenamento compatível com Amazon S3 em AWS Snowball Edge	• Amazon S3 (em Regiões da AWS) • Amazon EFS • Servidor FSx de arquivos Amazon para Windows • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP

Origem (De)	Destino (Para)
• Amazon S3 (em Regiões da AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	• Armazenamento compatível com Amazon S3 no Snowball Edge
• Amazon S3 (em Regiões da AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	• Amazon S3 (em Regiões da AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP
• Amazon S3 (em AWS regiões)	• Amazon S3 em AWS Outposts
• Amazon S3 em AWS Outposts	• Amazon S3 (em Regiões da AWS)

Transferências suportadas em Contas da AWS

DataSync suporta algumas transferências entre recursos de armazenamento associados a diferentes Contas da AWS.

Origem (De)	Destino (Para)
• Amazon EFS¹ • FSx para Windows File Server²	• Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP

Origem (De)	Destino (Para)
• Amazon S3 (em Regiões da AWS)	• Amazon S3 (em Regiões da AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP
• Amazon S3 (em Regiões da AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	• Amazon S3 (em Regiões da AWS)
• NFS • SMB • HDFS • Armazenamento de objetos	• Amazon S3 (em Regiões da AWS)

¹ Configurado como um [local NFS](#).

² Configurado como um [local SMB](#).

Transferências suportadas no mesmo Região da AWS

Não há restrições ao transferir dados dentro da mesma Região da AWS (incluindo [regiões de adesão opcional](#)). Para obter mais informações, consulte [Regiões da AWS suportado por DataSync](#).

Transferências compatíveis entre Regiões da AWS

Observe o seguinte ao transferir dados entre os [Regiões da AWS compatíveis com: DataSync](#)

- Ao transferir entre serviços AWS de armazenamento diferentes Regiões da AWS, um dos dois locais deve estar na região em que você está usando DataSync.
- Você não pode transferir entre regiões com um NFS, SMB, HDFS ou um local de armazenamento de objetos. Nessas situações, os dois locais de transferência devem estar na mesma região em que você [ativa seu DataSync agente](#).
- Com AWS GovCloud (US) as Regiões, você pode:
 - Transferência entre as regiões AWS GovCloud (Leste dos EUA) e AWS GovCloud (Oeste dos EUA).
 - Transferência entre uma AWS GovCloud (US) região e uma área comercial Região da AWS, como o Leste dos EUA (Norte da Virgínia). Esse tipo de transferência requer um [agente](#) ao transferir entre o Amazon EFS ou os sistemas de FSx arquivos da Amazon.

Important

Você paga pelos dados transferidos entre Regiões da AWS. Essa transferência é cobrada como transferência de dados para fora, da região de origem para a região de destino. Para obter mais informações, consulte [Preços do AWS DataSync](#).

Determinar se sua transferência requer um DataSync agente

Dependendo do seu cenário de transferência, talvez você precise de um DataSync agente. Para obter mais informações, consulte [Eu preciso de um AWS DataSync agente?](#).

Transferindo de ou para o armazenamento local com AWS DataSync

Com AWS DataSync, você pode transferir arquivos e objetos entre vários sistemas de armazenamento locais ou autogerenciados e os seguintes serviços AWS de armazenamento:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)

- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Tópicos

- [Configurando AWS DataSync transferências com um servidor de arquivos NFS](#)
- [Configurando AWS DataSync transferências com um servidor de arquivos SMB](#)
- [Configurando AWS DataSync transferências com um cluster HDFS](#)
- [Configurando DataSync transferências com um sistema de armazenamento de objetos](#)

Configurando AWS DataSync transferências com um servidor de arquivos NFS

Com AWS DataSync, você pode transferir dados entre o servidor de arquivos do Network File System (NFS) e um dos seguintes serviços de AWS armazenamento:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)
- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Para configurar esse tipo de transferência, você cria um [local](#) para o servidor de arquivos NFS. Você pode usar esse local como origem ou destino de uma transferência.

Fornecendo DataSync acesso aos servidores de arquivos NFS

DataSync Para acessar seu servidor de arquivos NFS, você precisa de um DataSync [agente](#). O agente monta uma exportação em seu servidor de arquivos usando o protocolo NFS.

Tópicos

- [Configurar sua exportação NFS](#)
- [Versões NFS com suporte](#)

Configurar sua exportação NFS

A exportação DataSync necessária para sua transferência depende de seu servidor de arquivos NFS ser um local de origem ou destino e de como as permissões do servidor de arquivos estão configuradas.

Se o seu servidor de arquivos for um local de origem, DataSync basta ler e percorrer seus arquivos e pastas. Se for um local de destino, DataSync precisa de acesso root para gravar no local e definir a propriedade, as permissões e outros metadados nos arquivos e pastas que você está copiando. Você pode usar a opção `no_root_squash` para permitir o acesso raiz para sua exportação.

Os exemplos a seguir descrevem como configurar uma exportação NFS que forneça acesso a DataSync

Quando seu servidor de arquivos NFS é um local de origem (acesso raiz)

Configure sua exportação usando o comando a seguir, que fornece permissões DataSync somente leitura (`ro`) e acesso root (`no_root_squash`):

```
export-path datasync-agent-ip-address(ro,no_root_squash)
```

Quando o servidor de arquivos NFS é um local de destino

Configure sua exportação usando o comando a seguir, que fornece permissões de DataSync gravação (`rw`) e acesso root (`no_root_squash`):

```
export-path datasync-agent-ip-address(rw,no_root_squash)
```

Quando o servidor de arquivos NFS é um local de origem (sem acesso raiz)

Configure sua exportação usando o comando a seguir, que especifica o ID de usuário (UID) e o ID de grupo (GID) do POSIX que você sabe que forneceriam permissões somente de DataSync leitura na exportação:

```
export-path datasync-agent-ip-address(ro,all_squash,anonuid=uid,anongid=gid)
```

Versões NFS com suporte

Por padrão, DataSync usa a versão 4.1 do NFS. DataSync também suporta NFS 4.0 e 3.x.

Configuração da rede para transferências do NFS

Para sua DataSync transferência, você deve configurar o tráfego para algumas conexões de rede:

1. Permita o tráfego nas seguintes portas do seu DataSync agente para o servidor de arquivos NFS:

- Para NFS versão 4.1 e 4.0: porta TCP 2049
- Para NFS versão 3.x: portas TCP 111 e 2049

Outros clientes NFS em sua rede devem ser capazes de montar a exportação NFS que você está usando para transferir dados. A exportação também deve estar acessível sem a autenticação Kerberos.

2. Configure o tráfego para a [conexão de endpoint de serviço](#) (como um endpoint público, FIPS ou da VPC).
3. Permita o tráfego do DataSync serviço para o [serviço AWS de armazenamento](#) para o qual você está transferindo ou do qual você está transferindo.

Criar seu local de transferência de NFS

Antes de começar, verifique o seguinte:

- Você precisa de um servidor de arquivos NFS do qual deseja transferir dados.
- Você precisa de um DataSync agente que possa [acessar seu servidor de arquivos](#).
- DataSync não suporta a cópia de listas de controle de acesso (ACLs) do NFS versão 4.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de localização, escolha Network File System (NFS).
4. Para Agentes, escolha o DataSync agente que pode se conectar ao seu servidor de arquivos NFS.

Você pode escolher mais de um agente. Para obter mais informações, consulte [Usando vários DataSync agentes](#).

5. Para servidor NFS, insira o nome do Sistema de Nomes de Domínio (DNS) ou o endereço IP do servidor de arquivos NFS ao qual seu DataSync agente se conecta.
6. Em Caminho de montagem, insira o caminho de exportação do NFS que você DataSync deseja montar.

Esse caminho (ou um subdiretório do caminho) é onde os dados são DataSync transferidos de ou para. Para obter mais informações, consulte [Configurar sua exportação NFS](#).

7. (Opcional) Expanda Configurações adicionais e escolha uma versão específica do NFS DataSync para usar ao acessar seu servidor de arquivos.

Para obter mais informações, consulte [Versões NFS com suporte](#).

8. (Opcional) Escolha Adicionar tag para marcar sua localização NFS.

As Tags são pares de chave-valor que ajudam você a gerenciar, filtrar e pesquisar seus locais. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

9. Escolha Criar local.

Usando o AWS CLI

- Use o comando a seguir para criar um local do NFS.

```
aws datasync create-location-nfs \
  --server-hostname nfs-server-address \
  --on-prem-config AgentArns=datasync-agent-arns \
  --subdirectory nfs-export-path
```

Para obter mais informações sobre como criar o local, consulte [Fornecendo DataSync acesso aos servidores de arquivos NFS](#).

DataSync escolhe automaticamente a versão do NFS que ele usa para ler de um local do NFS. Para especificar uma versão do NFS, use o parâmetro opcional `Version` na operação de API [NfsMountOptions](#).

Esse comando retornará o nome de recurso da Amazon (ARN) do local de NFS, semelhante ao ARN mostrado a seguir.

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0f01451b140b2af49"
}
```

Para garantir que o diretório possa ser montado, conecte-se a qualquer computador que tenha a mesma configuração de rede que seu agente e execute o comando a seguir.

```
mount -t nfs -o nfsvers=<nfs-server-version> <nfs-server-address>:<nfs-export-path> <test-
folder>
```

Veja a seguir um exemplo do comando .

```
mount -t nfs -o nfsvers=3 198.51.100.123:/path_for_sync_to_read_from /
temp_folder_to_test_mount_on_local_machine
```

Configurando AWS DataSync transferências com um servidor de arquivos SMB

Com AWS DataSync, você pode transferir dados entre o servidor de arquivos do Server Message Block (SMB) e um dos seguintes serviços de AWS armazenamento:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)
- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Para configurar esse tipo de transferência, você cria um [local](#) para o servidor de arquivos SMB. Você pode usar esse local como origem ou destino de uma transferência.

Fornecendo DataSync acesso a servidores de arquivos SMB

DataSync se conecta ao seu servidor de arquivos usando o protocolo SMB e pode se autenticar com NTLM ou Kerberos.

Tópicos

- [Versões compatíveis do SMB](#)
- [Usando a autenticação NTLM](#)
- [Usar a autenticação Kerberos](#)
- [Permissões obrigatórias](#)
- [Namespaces do DFS](#)

Versões compatíveis do SMB

Por padrão, escolhe DataSync automaticamente uma versão do protocolo SMB com base na negociação com seu servidor de arquivos SMB.

Você também pode configurar DataSync para usar uma versão SMB específica, mas recomendamos fazer isso somente se DataSync tiver problemas para negociar com o servidor de arquivos SMB automaticamente. DataSync oferece suporte às versões 1.0 e posteriores do SMB. Por motivos de segurança, recomendamos usar a versão 3.0.2 ou posterior do SMB. Versões anteriores, como a SMB 1.0, contêm vulnerabilidades de segurança conhecidas que os invasores podem explorar para comprometer seus dados.

Consulte a tabela a seguir para ver uma lista de opções no DataSync console e na API:

Opção do console	Opção de API	Descrição
Automatico	AUTOMATIC	DataSync e o servidor de arquivos SMB negociam a versão mais alta do SMB que eles suportam mutuamente entre 2.1 e 3.1.1. Essa é a opção recomendada e também a padrão. Se, em vez disso, você escolher uma versão específica que seu servidor de arquivos não suporta, você pode receber um erro <code>Operation Not Supported</code> .

Opção do console	Opção de API	Descrição
SMB 3.0.2	SMB3	Restringe a negociação do protocolo somente à versão 3.0.2 do SMB.
SMB 2.1	SMB2	Restringe a negociação do protocolo somente à versão 2.1 do SMB.
SMB 2.0	SMB2_0	Restringe a negociação do protocolo somente à versão 2.0 do SMB.
SMB 1.0	SMB1	: restringe a negociação do protocolo somente à versão 3.0.2 do SMB.

Usando a autenticação NTLM

Para usar a autenticação NTLM, você fornece um nome de usuário e uma senha que permitem DataSync acessar o servidor de arquivos SMB para o qual você está transferindo ou de. O usuário pode ser um usuário local em seu servidor de arquivos ou um usuário de domínio em seu Microsoft Active Directory.

Usar a autenticação Kerberos

Para usar a autenticação Kerberos, você fornece um arquivo Kerberos principal, uma tabela de chaves Kerberos (keytab) e um arquivo de configuração Kerberos que permitem acessar o servidor de arquivos SMB que você está transferindo DataSync para ou do qual você está transferindo.

Tópicos

- [Pré-requisitos](#)
- [DataSync opções de configuração para Kerberos](#)

Pré-requisitos

Você precisa criar alguns artefatos Kerberos e configurar sua rede para que DataSync possa acessar seu servidor de arquivos SMB.

- [Crie um arquivo keytab Kerberos usando o utilitário ktpass ou kutil.](#)

O exemplo a seguir cria um arquivo keytab usando `ktpass`. O realm Kerberos que você especifica (`MYDOMAIN.ORG`) deve estar em maiúsculas.

```
ktpass /out C:\YOUR_KEYTAB.keytab /princ HOST/kerberosuser@MYDOMAIN.ORG /mapuser
kerberosuser /pass * /crypto AES256-SHA1 /ptype KRB5_NT_PRINCIPAL
```

- Prepare uma versão simplificada do arquivo de configuração Kerberos (`krb5.conf`). Inclua informações sobre o reino, a localização dos servidores de administração do domínio e mapeamentos de nomes de host em um reino Kerberos.

Verifique se o `krb5.conf` conteúdo está formatado com a combinação correta de maiúsculas e minúsculas para os domínios e os nomes dos domínios. Por exemplo:

```
[libdefaults]
    dns_lookup_realm = true
    dns_lookup_kdc = true
    forwardable = true
    default_realm = MYDOMAIN.ORG

[realms]
    MYDOMAIN.ORG = {
        kdc = mydomain.org
        admin_server = mydomain.org
    }

[domain_realm]
    .mydomain.org = MYDOMAIN.ORG
    mydomain.org = MYDOMAIN.ORG
```

- Em sua configuração de rede, verifique se a porta do servidor Kerberos Key Distribution Center (KDC) está aberta. A porta KDC é normalmente a porta TCP 88.

DataSync opções de configuração para Kerberos

Ao criar um local SMB que usa Kerberos, você configura as seguintes opções.

Opção do console	Opção de API	Descrição
Servidor SMB	<code>ServerHostName</code>	O nome de domínio do servidor de arquivos SMB

Opção do console	Opção de API	Descrição
		que seu DataSync agente montará. Para o Kerberos, você não pode especificar o endereço IP do servidor de arquivos.
Kerberos principal	KerberosPrincipal	Uma identidade em seu realm Kerberos que tem permissão para acessar os arquivos, pastas e metadados de arquivos em seu servidor de arquivos SMB. Talvez seja a aparência de um diretor de Kerberos. <code>HOST/kerberosuser@MYDOMAIN.ORG</code> Os nomes principais diferenciam maiúsculas de minúsculas.
Arquivo Keytab	KerberosKeytab	Um arquivo de tabela de chaves Kerberos (keytab), que inclui mapeamentos entre suas chaves principais e de criptografia do Kerberos.
Arquivo de configuração Kerberos	KerberosKrbConf	Um <code>krb5.conf</code> arquivo que define sua configuração de região Kerberos.

Opção do console	Opção de API	Descrição
Endereços IP DNS (opcional)	DnsIpAddresses	Os IPv4 endereços dos servidores DNS aos quais seu servidor de arquivos SMB pertence. Se você tiver vários domínios em seu ambiente, a configuração garante que ele se DataSync conecte ao servidor de arquivos SMB correto.

Permissões obrigatórias

A identidade que você fornece DataSync deve ter permissão para montar e acessar os arquivos, pastas e metadados de arquivos do seu servidor de arquivos SMB.

Se você fornecer uma identidade no Active Directory, ela deverá ser membro de um grupo do Active Directory com um ou ambos os seguintes direitos de usuário (dependendo dos [metadados que você DataSync deseja copiar](#)):

Direito do usuário	Descrição
Restaurar arquivos e diretórios (SE_RESTORE_NAME)	Permite copiar DataSync a propriedade do objeto, as permissões, os metadados do arquivo e as listas de acesso discricionário do NTFS (. DACLs Esse direito de usuário geralmente é concedido aos membros dos grupos Administradores de domínio e Operadores de backup (ambos grupos padrão do Active Directory).
Gerenciar logs de auditoria e segurança (SE_SECURITY_NAME)	Permite DataSync copiar listas de controle de acesso do sistema NTFS (SACLs).

Direito do usuário	Descrição
	Esse direito de usuário geralmente é concedido aos membros do grupo Administradores de domínio.

Se você quiser copiar o Windows ACLs e estiver fazendo a transferência entre um servidor de arquivos SMB e outro sistema de armazenamento que usa SMB (como Amazon FSx for Windows File Server ou FSx ONTAP), a identidade fornecida DataSync deverá pertencer ao mesmo domínio do Active Directory ou ter uma relação de confiança do Active Directory entre seus domínios.

Namespaces do DFS

DataSync não oferece suporte a namespaces do Microsoft Distributed File System (DFS). Em vez disso, recomendamos especificar um servidor ou compartilhamento de arquivos subjacente ao criar sua DataSync localização.

Criar seu local de transferência do SMB

Antes de começar, é preciso um servidor de arquivos SMB do qual você deseja transferir dados.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de local, escolha Server Message Block (SMB).

Você configurará esse local como origem ou destino posteriormente.

4. Para Agentes, escolha o DataSync agente que pode se conectar ao seu servidor de arquivos SMB.

Você pode escolher mais de um agente. Para obter mais informações, consulte [Usando vários DataSync agentes](#).

5. Para servidor SMB, insira o nome de domínio ou endereço IP do servidor de arquivos SMB que seu DataSync agente montará.

Lembre-se do seguinte com essa configuração:

- Você não pode especificar um endereço IP versão 6 (IPv6).
 - Se você estiver usando a autenticação Kerberos, deverá especificar um nome de domínio.
6. Em Nome do compartilhamento, insira o nome do compartilhamento exportado pelo seu servidor de arquivos SMB onde os dados DataSync serão lidos ou gravados.

Você pode incluir um subdiretório no caminho de compartilhamento (por exemplo, /path/to/subdirectory). Certifique-se de que outros clientes do SMB em sua rede também possam montar este caminho.

Para copiar todos os dados no subdiretório, DataSync deve ser capaz de montar o compartilhamento SMB e acessar todos os seus dados. Para obter mais informações, consulte [Permissões obrigatórias](#).

7. (Opcional) Expanda Configurações adicionais e escolha uma versão SMB DataSync para usar ao acessar seu servidor de arquivos.

Por padrão, escolha DataSync automaticamente uma versão com base na negociação com o servidor de arquivos SMB. Para mais informações, consulte [Versões compatíveis do SMB](#).

8. Em Tipo de autenticação, escolha NTLM ou Kerberos.
9. Siga um dos procedimentos a seguir, dependendo do seu tipo de autenticação:

NTLM

- Em Usuário, insira um nome de usuário que possa montar o servidor de arquivos SMB e tenha permissão para acessar os arquivos e pastas envolvidos na sua transferência.

Para obter mais informações, consulte [Permissões obrigatórias](#).

- Em Senha, especifique a senha do usuário que pode montar o servidor de arquivos do SMB e tem permissão para acessar os arquivos e pastas envolvidos na sua transferência.
- (Opcional) Para Domínio, insira o nome do domínio do Windows ao qual pertence o servidor de arquivos SMB.

Se você tiver vários domínios em seu ambiente, definir essa configuração garante que ele se DataSync conecte ao servidor de arquivos SMB correto.

Kerberos

- Para Kerberos principal, especifique um principal em seu realm Kerberos que tenha permissão para acessar os arquivos, pastas e metadados de arquivos em seu servidor de arquivos SMB.

Talvez seja a aparência de um diretor de Kerberos. HOST/
kerberosuser@MYDOMAIN.ORG

Os nomes principais diferenciam maiúsculas de minúsculas. A execução da DataSync tarefa falhará se o principal que você especificar para essa configuração não corresponder exatamente ao principal usado para criar o arquivo keytab.

- Para o arquivo Keytab, faça upload de um arquivo keytab que inclua mapeamentos entre as chaves principal e de criptografia do Kerberos.
- Para o arquivo de configuração Kerberos, faça upload de um `krb5.conf` arquivo que defina sua configuração de região Kerberos.
- (Opcional) Para endereços IP DNS, especifique até dois IPv4 endereços para os servidores DNS aos quais seu servidor de arquivos SMB pertence.

Se você tiver vários domínios em seu ambiente, a configuração desse parâmetro garante que ele se DataSync conecte ao servidor de arquivos SMB correto.

10. (Opcional) Escolha Adicionar tag para marcar sua localização SMB.

As Tags são pares de chave-valor que ajudam você a gerenciar, filtrar e pesquisar seus locais. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

11. Escolha Criar local.

Usando o AWS CLI

As instruções a seguir descrevem como criar locais SMB com autenticação NTLM ou Kerberos.

NTLM

1. Copie o seguinte comando `create-location-smb`:

```
aws datasync create-location-smb \
  --agent-arns datasync-agent-arns \
```

```
--server-hostname smb-server-address \  
--subdirectory smb-export-path \  
--authentication-type "NTLM" \  
--user user-who-can-mount-share \  
--password user-password \  
--domain windows-domain-of-smb-server
```

2. Para `--agent-arns`, especifique o DataSync agente que pode se conectar ao seu servidor de arquivos SMB.

Você pode escolher mais de um agente. Para obter mais informações, consulte [Usando vários DataSync agentes](#).

3. Para `--server-hostname`, especifique o nome de domínio ou IPv4 endereço do servidor de arquivos SMB que seu DataSync agente montará.
4. Para `--subdirectory`, especifique o nome do compartilhamento exportado pelo seu servidor de arquivos SMB onde DataSync lerá ou gravará dados.

Você pode incluir um subdiretório no caminho de compartilhamento (por exemplo, `/path/to/subdirectory`). Certifique-se de que outros clientes do SMB em sua rede também possam montar este caminho.

Para copiar todos os dados no subdiretório, DataSync deve ser capaz de montar o compartilhamento SMB e acessar todos os seus dados. Para obter mais informações, consulte [Permissões obrigatórias](#).

5. Para `--user`, especifique um nome de usuário que possa montar seu servidor de arquivos SMB e tenha permissão para acessar os arquivos e pastas envolvidos na sua transferência.

Para obter mais informações, consulte [Permissões obrigatórias](#).

6. Para `--password`, especifique a senha do usuário que pode montar seu servidor de arquivos SMB e tem permissão para acessar os arquivos e pastas envolvidos na sua transferência.
7. (Opcional) Para `--domain`, especifique o nome de domínio do Windows ao qual seu servidor de arquivos SMB pertence.

Se você tiver vários domínios em seu ambiente, definir essa configuração garante que ele se DataSync conecte ao servidor de arquivos SMB correto.

8. (Opcional) Adicione a `--version` opção se quiser DataSync usar uma versão SMB específica. Para obter mais informações, consulte [Versões compatíveis do SMB](#).

9. Execute o comando `create-location-smb`.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN do local que você criou. Por exemplo:

```
{
  "arn:aws:datasync:us-east-1:123456789012:location/loc-01234567890example"
}
```

Kerberos

1. Copie o seguinte comando `create-location-smb`:

```
aws datasync create-location-smb \
  --agent-arns datasync-agent-arns \
  --server-hostname smb-server-address \
  --subdirectory smb-export-path \
  --authentication-type "KERBEROS" \
  --kerberos-principal "HOST/kerberosuser@EXAMPLE.COM" \
  --kerberos-keytab "file://path/to/file.keytab" \
  --kerberos-krb5-conf "file://path/to/krb5.conf" \
  --dns-ip-addresses array-of-ipv4-addresses
```

2. Para `--agent-arns`, especifique o DataSync agente que pode se conectar ao seu servidor de arquivos SMB.

Você pode escolher mais de um agente. Para obter mais informações, consulte [Usando vários DataSync agentes](#).

3. Para `--server-hostname`, especifique o nome de domínio do servidor de arquivos SMB que seu DataSync agente montará.

4. Para `--subdirectory`, especifique o nome do compartilhamento exportado pelo seu servidor de arquivos SMB onde DataSync lerá ou gravará dados.

Você pode incluir um subdiretório no caminho de compartilhamento (por exemplo, `/path/to/subdirectory`). Certifique-se de que outros clientes do SMB em sua rede também possam montar este caminho.

Para copiar todos os dados no subdiretório, DataSync deve ser capaz de montar o compartilhamento SMB e acessar todos os seus dados. Para obter mais informações, consulte [Permissões obrigatórias](#).

5. Para as opções do Kerberos, faça o seguinte:

- `--kerberos-principal`: especifique um principal em seu realm Kerberos que tenha permissão para acessar os arquivos, pastas e metadados de arquivos em seu servidor de arquivos SMB.

Talvez seja a aparência de um diretor de Kerberos. `HOST/kerberosuser@MYDOMAIN.ORG`

Os nomes principais diferenciam maiúsculas de minúsculas. A execução da DataSync tarefa falhará se o principal que você especificar para essa opção não corresponder exatamente ao principal usado para criar o arquivo keytab.

- `--kerberos-keytab`: especifique um arquivo keytab que inclua mapeamentos entre as chaves principal e de criptografia do Kerberos.
- `--kerberos-krb5-conf`: especifique um `krb5.conf` arquivo que defina sua configuração de região Kerberos.
- (Opcional) `--dns-ip-addresses`: especifique até dois IPv4 endereços para os servidores DNS aos quais seu servidor de arquivos SMB pertence.

Se você tiver vários domínios em seu ambiente, a configuração desse parâmetro garante que ele se DataSync conecte ao servidor de arquivos SMB correto.

6. (Opcional) Adicione a `--version` opção se quiser DataSync usar uma versão SMB específica. Para obter mais informações, consulte [Versões compatíveis do SMB](#).

7. Execute o comando `create-location-smb`.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN do local que você criou. Por exemplo:

```
{
  "arn:aws:datasync:us-east-1:123456789012:location/loc-01234567890example"
}
```

Configurando AWS DataSync transferências com um cluster HDFS

Com AWS DataSync, você pode transferir dados entre seu cluster Hadoop Distributed File System (HDFS) e um dos seguintes serviços de armazenamento: AWS

- [Amazon S3](#)
- [Amazon EFS](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)
- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Para configurar esse tipo de transferência, você cria um [local](#) para o cluster do HDFS. Você pode usar esse local como origem ou destino de uma transferência.

Fornecendo DataSync acesso aos clusters do HDFS

Para se conectar ao seu cluster HDFS, DataSync use um [agente que você implanta](#) o mais próximo possível do seu cluster HDFS. O DataSync agente atua como um cliente HDFS e se comunica com o NameNodes e DataNodes em seu cluster.

Quando você inicia uma tarefa de transferência, DataSync consulta NameNode os locais dos arquivos e pastas no cluster. Se você configurar a localização do HDFS como uma localização de origem, DataSync lê os dados dos arquivos e pastas do DataNodes seu cluster e copia esses dados para o destino. Se você configurar seu local do HDFS como um local de destino, então DataSync grava arquivos e pastas da origem para o DataNodes em seu cluster.

Autenticação

Ao se conectar a um cluster HDFS, DataSync oferece suporte à autenticação simples ou à autenticação Kerberos. Para usar a autenticação simples, forneça o nome de usuário de um usuário com direitos de leitura e gravação no cluster HDFS. Para usar a autenticação Kerberos, forneça um arquivo de configuração Kerberos, um arquivo de tabela de chaves Kerberos (keytab) e um nome principal Kerberos. As credenciais da entidade principal do Kerberos devem estar no arquivo keytab fornecido.

Criptografia

Ao usar a autenticação Kerberos, DataSync oferece suporte à criptografia de dados à medida que são transmitidos entre o DataSync agente e seu cluster HDFS. Criptografe seus dados usando as configurações de Qualidade de Proteção (QOP) em seu cluster HDFS e especificando as configurações de QOP ao criar sua localização HDFS. A configuração de QOP inclui configurações para proteção de transferência de dados e proteção RPC (Remote Procedure Call).

DataSync suporta os seguintes tipos de criptografia Kerberos:

- `des-cbc-crc`
- `des-cbc-md4`
- `des-cbc-md5`
- `des3-cbc-sha1`
- `arcfour-hmac`
- `arcfour-hmac-exp`
- `aes128-cts-hmac-sha1-96`
- `aes256-cts-hmac-sha1-96`
- `aes128-cts-hmac-sha256-128`
- `aes256-cts-hmac-sha384-192`
- `camellia128-cts-cmac`
- `camellia256-cts-cmac`

Você também pode configurar clusters HDFS para criptografia em repouso usando a Transparent Data Encryption, TDE (Criptografia transparente de dados). Ao usar a autenticação simples, DataSync lê e grava em clusters habilitados para TDE. Se você estiver usando DataSync para copiar dados para um cluster habilitado para TDE, primeiro configure as zonas de criptografia no cluster HDFS. DataSync não cria zonas de criptografia.

Recursos do HDFS não compatíveis

Atualmente, os seguintes recursos do HDFS não são compatíveis com: DataSync

- Transparent Data Encryption (TDE) ao usar a autenticação Kerberos
- Configurando vários NameNodes
- Hadoop HDFS sobre HTTP (HttpFS)

- Listas de controle de acesso POSIX () ACLs
- Atributos estendidos do HDFS (xattrs)
- Clusters HDFS usando Apache HBase

Criar seu local de transferência HDFS

Você pode usar sua localização como origem ou destino para sua DataSync transferência.

Antes de começar: verifique a conectividade de rede entre seu agente e o cluster Hadoop fazendo o seguinte:

- Teste o acesso às portas TCP listadas em [Requisitos de rede para armazenamento on-premises, autogerenciado, em outra nuvem e a na borda](#).
- Teste o acesso entre seu agente local e seu cluster Hadoop. Para obter instruções, consulte [Verificação da conexão do agente com sistema de armazenamento](#).

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de localização, escolha Sistema de arquivos distribuído Hadoop (HDFS).

Você configurará esse local como origem ou destino posteriormente.

4. Em Agentes, escolha o agente do DataSync que pode se conectar ao cluster do HDFS.

Você pode escolher mais de um agente. Para obter mais informações, consulte [Usando vários DataSync agentes](#).

5. Para NameNode, forneça o nome de domínio ou endereço IP do principal NameNode do seu cluster HDFS.
6. Em Pasta, insira uma pasta no cluster HDFS que você deseja usar DataSync para a transferência de dados.

Se a localização do HDFS for uma fonte, DataSync copie os arquivos dessa pasta para o destino. Se sua localização for um destino, DataSync grava arquivos nessa pasta.

7. Para definir o Tamanho do bloco ou o Fator de replicação, escolha Configurações adicionais.

O tamanho de bloco padrão é 128 MiB. O tamanho fornecido deve ser um múltiplo de 512 bytes.

O fator de replicação padrão é três DataNodes ao transferir para o cluster HDFS.

8. Na seção Segurança, escolha o Tipo de autenticação usado no cluster HDFS.

- Simples: em Usuário, especifique o nome do usuário com as seguintes permissões no cluster HDFS (dependendo do seu caso de uso):
 - Se você planeja usar esse local como local de origem, especifique um usuário que tenha apenas permissões de leitura.
 - Se você planeja usar esse local como local de destino, especifique um usuário que tenha apenas permissões de leitura e gravação.

Opcionalmente, especifique o URI do Key Management Server (KMS) do cluster do HDFS.

- Kerberos: especifique o Kerberos Principal com acesso ao cluster HDFS. Em seguida, forneça o KeyTabarquivo que contém o principal Kerberos fornecido. Depois, forneça o arquivo de configuração do Kerberos. Por fim, especifique o tipo de criptografia na proteção de trânsito nas listas suspensas Proteção RPC e Proteção de transferência de dados.

9. (Opcional) Escolha Adicionar tag para marcar sua localização HDFS.

As Tags são pares de chave-valor que ajudam você a gerenciar, filtrar e pesquisar seus locais. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

10. Escolha Criar local.

Usando o AWS CLI

1. Copie o seguinte comando `create-location-hdfs`:

```
aws datasync create-location-hdfs --name-nodes [{"Hostname":"host1", "Port": 8020}] \
  --authentication-type "SIMPLE|KERBEROS" \
  --agent-arns [arn:aws:datasync:us-east-1:123456789012:agent/  
agent-01234567890example] \
  --subdirectory "/path/to/my/data"
```

2. Para o `--name-nodes` parâmetro, especifique o nome do host ou endereço IP do seu cluster HDFS primário NameNode e a porta TCP na qual ele NameNode está escutando.

3. No parâmetro `--authentication-type`, especifique o tipo de autenticação a ser usada ao se conectar ao cluster do Hadoop. É possível especificar `SIMPLE` ou `KERBEROS`.

Se você usa a autenticação `SIMPLE`, use o parâmetro `--simple-user` para especificar o nome de usuário do usuário. Se você usa a autenticação `KERBEROS`, use os parâmetros `--kerberos-principal`, `--kerberos-keytab` e `--kerberos-krb5-conf`. Para obter mais informações, consulte [create-location-hdfs](#).

4. Para o `--agent-arns` parâmetro, especifique o ARN do DataSync agente que pode se conectar ao seu cluster HDFS.

Você pode escolher mais de um agente. Para obter mais informações, consulte [Usando vários DataSync agentes](#).

5. (Opcional) Para o `--subdirectory` parâmetro, especifique uma pasta no cluster HDFS que você deseja usar DataSync para a transferência de dados.

Se a localização do HDFS for uma fonte, DataSync copie os arquivos dessa pasta para o destino. Se sua localização for um destino, DataSync grava arquivos nessa pasta.

6. Execute o comando `create-location-hdfs`.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN do local que você criou. Por exemplo:

```
{
  "arn:aws:datasync:us-east-1:123456789012:location/loc-01234567890example"
}
```

Configurando DataSync transferências com um sistema de armazenamento de objetos

Com AWS DataSync, você pode transferir dados entre seu sistema de armazenamento de objetos e um dos seguintes serviços AWS de armazenamento:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)

- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Para configurar esse tipo de transferência, você cria um [local](#) para o sistema de armazenamento de objetos. Você pode usar esse local como origem ou destino de uma transferência. A transferência de dados para ou do seu armazenamento de objetos local requer um DataSync agente.

Pré-requisitos

Seu sistema de armazenamento de objetos deve ser compatível com as seguintes [operações de API do Amazon S3](#) para se conectar DataSync a ele:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- DeleteObjectTagging
- GetBucketLocation
- GetObject
- GetObjectTagging
- HeadBucket
- HeadObject
- ListObjectsV2
- PutObject
- PutObjectTagging
- UploadPart

Criar o local de transferência de armazenamento de objetos

Antes de começar, você precisa de um sistema de armazenamento de objetos do qual e para o qual você planeja transferir dados.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de localização, escolha Armazenamento de objetos.

Você configurará esse local como origem ou destino posteriormente.

4. Em Servidor, forneça o nome do domínio ou o endereço IP do servidor de armazenamento de objetos.
5. Especifica o Nome do bucket de armazenamento de objetos envolvido na transferência.
6. Em Pasta, insira um prefixo de objeto.

DataSync copia somente objetos com esse prefixo.

7. Se sua transferência exigir um agente, escolha Usar agentes e, em seguida, escolha o DataSync agente que se conecta ao seu sistema de armazenamento de objetos.

Algumas transferências não exigem agentes. Em outros cenários, talvez você queira usar mais de um agente. Para obter mais informações, consulte [Situações em que você não precisa de um DataSync agente](#) e [Usando vários DataSync agentes](#).

8. Para configurar a conexão com o servidor de armazenamento de objetos, expanda Configurações adicionais e faça o seguinte:
 - a. Em Protocolo de servidor, escolha HTTP ou HTTPS.
 - b. Em Porta do servidor, use uma porta padrão (80 para HTTP ou 443 para HTTPS) ou especifique uma porta personalizada, se necessário.
 - c. Em Certificado, se o sistema de armazenamento de objetos usar uma autoridade de certificação (CA) privada ou autoassinada, selecione Escolher arquivo e especifique um único arquivo .pem com uma cadeia de certificados completa.

A cadeia de certificados pode incluir:

- O certificado do sistema de armazenamento de objetos
- Todos os certificados intermediários (se for o caso)
- O certificado-raiz da CA assinante

Você pode concatenar os certificados em um arquivo `.pem` (que pode ter até 32.768 bytes antes da codificação base64). O exemplo de comando `cat` a seguir cria um arquivo `object_storage_certificates.pem` que inclui três certificados:

```
cat object_server_certificate.pem intermediate_certificate.pem ca_root_certificate.pem  
> object_storage_certificates.pem
```

9. Se o servidor de armazenamento de objetos exigir credenciais para acesso, selecione **Requer credenciais** e insira a chave de acesso que você usa para acessar o bucket. Em seguida, insira a chave secreta diretamente ou especifique um AWS Secrets Manager segredo que contenha a chave. Para obter mais informações, consulte [Fornecimento de credenciais para locais de armazenamento](#).

A chave de acesso e a chave secreta podem ser um nome de usuário e uma senha, respectivamente.

10. (Opcional) Escolha **Adicionar tag** para marcar o local de armazenamento do objeto.

As Tags são pares de chave-valor que ajudam você a gerenciar, filtrar e pesquisar seus locais. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

11. Escolha **Criar local**.

Usando o AWS CLI

1. Copie o seguinte comando `create-location-object-storage`:

```
aws datasync create-location-object-storage \
  --server-hostname object-storage-server.example.com \
  --bucket-name your-bucket \
  --agent-arns arn:aws:datasync:us-east-1:123456789012:agent/
agent-01234567890deadfb
```

2. Especifique os parâmetros exigidos a seguir no comando:
 - `--server-hostname`: especifica o nome do domínio ou o endereço IP do seu servidor de armazenamento de objetos.
 - `--bucket-name`: especifica o nome do bucket no servidor de armazenamento de objetos para o qual você está transferindo ou do qual você está transferindo.

3. (Opcional) Adicione qualquer um dos seguintes parâmetros ao comando:

- `--agent-arns`— Especifique os DataSync agentes que você deseja conectar ao seu servidor de armazenamento de objetos.
- `--server-port`: especifica a porta em que o servidor de armazenamento de objetos aceita o tráfego de rede de entrada (por exemplo, a porta 443).
- `--server-protocol`: especifica o protocolo (HTTP ou HTTPS) que o servidor de armazenamento de objetos utiliza para se comunicar.
- `--access-key`: especifica a chave de acesso (por exemplo, um nome de usuário) se as credenciais forem necessárias para autenticação no servidor de armazenamento de objetos.
- `--secret-key`: especifica a chave secreta (por exemplo, uma senha) se as credenciais forem necessárias para autenticação no servidor de armazenamento de objetos.

Você também pode fornecer parâmetros adicionais para proteger suas chaves usando AWS Secrets Manager. Para obter mais informações, consulte [Fornecimento de credenciais para locais de armazenamento](#).

- `--server-certificate`— Especifica uma cadeia de certificados DataSync para autenticação em seu sistema de armazenamento de objetos se o sistema usar uma autoridade de certificação (CA) privada ou autoassinada. Você deve especificar um único arquivo `.pem` com uma cadeia de certificados completa (por exemplo, `file:///home/user/.ssh/object_storage_certificates.pem`).

A cadeia de certificados pode incluir:

- O certificado do sistema de armazenamento de objetos
- Todos os certificados intermediários (se for o caso)
- O certificado-raiz da CA assinante

Você pode concatenar os certificados em um arquivo `.pem` (que pode ter até 32.768 bytes antes da codificação base64). O exemplo de comando `cat` a seguir cria um arquivo `object_storage_certificates.pem` que inclui três certificados:

```
cat object_server_certificate.pem intermediate_certificate.pem ca_root_certificate.pem  
> object_storage_certificates.pem
```

- `--subdirectory`: especifica o prefixo de objeto do servidor de armazenamento de objetos.

DataSync copia somente objetos com esse prefixo.

- `--tags`: especifica o par de chave-valor que representa uma etiqueta que você deseja adicionar ao recurso do local.

Tags ajudam a gerenciar, filtrar e procurar recursos. Recomendamos criar uma etiqueta de nome para a sua localização.

4. Execute o comando `create-location-object-storage`.

Você recebe uma resposta que mostra o ARN do local que você acabou de criar.

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-01234567890abcdef"
}
```

Transferindo de ou para o AWS armazenamento com AWS DataSync

Com AWS DataSync, você pode transferir dados de ou para vários serviços de AWS armazenamento. Para obter mais informações, consulte [Com onde posso transferir meus dados DataSync?](#)

Tópicos

- [Configurando AWS DataSync transferências com o Amazon S3](#)
- [Configurando AWS DataSync transferências com o Amazon EFS](#)
- [Configurando transferências com o FSx Windows File Server](#)
- [Configurando DataSync transferências com FSx for Lustre](#)
- [Configurando DataSync transferências com a Amazon FSx para OpenZFS](#)
- [Configurando transferências com a Amazon FSx para ONTAP NetApp](#)

Configurando AWS DataSync transferências com o Amazon S3

Para transferir dados para ou do seu bucket do Amazon S3, você cria um local de AWS DataSync transferência. DataSync pode usar esse local como origem ou destino para transferir dados.

Fornecendo DataSync acesso aos buckets do S3

DataSync precisa acessar o bucket do S3 para o qual você está transferindo ou do qual você está transferindo. Para fazer isso, você deve criar uma função AWS Identity and Access Management (IAM) que DataSync assuma as permissões necessárias para acessar o bucket. Em seguida, você especifica essa função ao [criar sua localização no Amazon S3](#) para DataSync

Sumário

- [Permissões obrigatórias](#)
- [Criação de uma função do IAM DataSync para acessar sua localização no Amazon S3](#)
- [Acessar buckets do S3 usando criptografia no lado do servidor](#)
- [Acesso aos buckets restritos do S3](#)
- [Acesso aos buckets do S3 com acesso restrito à VPC](#)

Permissões obrigatórias

As permissões que sua função do IAM precisa podem depender se o bucket é um local de DataSync origem ou destino. O Amazon S3 no Outposts requer um conjunto diferente de permissões.

Amazon S3 (source location)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
```

```

        "s3:ListMultipartUploadParts"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
  ]
}

```

Amazon S3 (destination location)

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {

```

```

        "aws:ResourceAccount": "123456789012"
      }
    }
  ]
}

```

Amazon S3 on Outposts

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "s3-outposts:ListBucket",
      "s3-outposts:ListBucketMultipartUploads"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3-outposts:region:account-id:outpost/outpost-id/bucket/amzn-s3-demo-bucket",
      "arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/bucket-access-point-name"
    ]
  },
  {
    "Action": [
      "s3-outposts:AbortMultipartUpload",
      "s3-outposts>DeleteObject",
      "s3-outposts:GetObject",
      "s3-outposts:GetObjectTagging",
      "s3-outposts:GetObjectVersion",
      "s3-outposts:GetObjectVersionTagging",
      "s3-outposts:ListMultipartUploadParts",
      "s3-outposts:PutObject",
      "s3-outposts:PutObjectTagging"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3-outposts:region:account-id:outpost/outpost-id/bucket/amzn-s3-demo-bucket/*",
      "arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/bucket-access-point-name/*"
    ]
  }
]
}

```

```
    },  
    {  
      "Action": "s3-outposts:GetAccessPoint",  
      "Effect": "Allow",  
      "Resource": "arn:aws:s3-outposts:region:account-  
id:outpost/outpost-id/accesspoint/bucket-access-point-name"  
    }  
  ]  
}
```

Criação de uma função do IAM DataSync para acessar sua localização no Amazon S3

Ao [criar sua localização do Amazon S3](#) no console, DataSync você pode criar e assumir automaticamente uma função do IAM que normalmente tem as permissões certas para acessar seu bucket do S3.

Em algumas situações, talvez seja necessário criar essa função manualmente (por exemplo, acessar buckets com camadas extras de segurança ou transferir para ou de um bucket em outro Contas da AWS).

Criação manual de uma função do IAM para DataSync

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação esquerdo, em Gerenciamento de acesso, escolha Perfis e, em seguida, escolha Criar perfil.
3. Na página Selecionar entidade confiável, para Tipo de entidade confiável, escolha AWS service (Serviço da AWS).
4. Em Caso de uso, escolha DataSyncna lista suspensa e selecione. DataSync Escolha Próximo.
5. Na página Adicionar permissões, escolha Próximo. Forneça um nome ao perfil e escolha Criar perfil.
6. Na página Perfis, procure o perfil que você acabou de criar e escolha seu nome.
7. Na página do perfil, escolha a guia Permissões. Selecione Adicionar permissões e, em seguida, Criar política em linha.
8. Escolha a guia JSON e [adicione as permissões necessárias](#) para acessar o bucket no editor de políticas.
9. Escolha Próximo. Digite um nome para a política e escolha Criar política.
10. (Recomendado) Para evitar o [problema “confused deputy” entre serviços](#), faça o seguinte:

- a. Na página Detalhes do perfil, escolha a guia Relações de confiança. Escolha Editar política de confiança.
- b. Atualize a política de confiança usando o exemplo a seguir, que inclui as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount`:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": "datasync.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      },
      "StringLike": {
        "aws:SourceArn": "arn:aws:datasync:region:account-id:*"
      }
    }
  }]
}
```

- c. Escolha Atualizar política.

Você pode especificar esse perfil ao criar seu local no Amazon S3.

Acessar buckets do S3 usando criptografia no lado do servidor

DataSync pode transferir dados de ou para [buckets do S3 que usam criptografia do lado do servidor](#). O tipo de chave de criptografia que um bucket usa pode determinar se você precisa de uma política personalizada que DataSync permita acessar o bucket.

Ao usar DataSync com buckets S3 que usam criptografia do lado do servidor, lembre-se do seguinte:

- Se seu bucket do S3 estiver criptografado com uma chave AWS gerenciada, DataSync poderá acessar os objetos do bucket por padrão se todos os seus recursos estiverem no mesmo Conta da AWS lugar.
- Se seu bucket do S3 estiver criptografado com uma chave gerenciada pelo cliente AWS Key Management Service (AWS KMS) (SSE-KMS), a [política da chave](#) deve incluir a função do IAM DataSync usada para acessar o bucket.
- Se seu bucket do S3 estiver criptografado com uma chave SSE-KMS gerenciada pelo cliente e em uma chave diferente Conta da AWS, DataSync precisará de permissão para acessar o bucket no outro. Conta da AWS Para isso, você pode configurar fazendo o seguinte:
 - Na função do IAM DataSync usada, você deve especificar a chave SSE-KMS do bucket entre contas usando o Amazon Resource Name (ARN) totalmente qualificado da chave. Esse é o mesmo ARN da chave que você usa para configurar a criptografia [padrão](#) do bucket. Você não pode especificar um ID de chave, um nome alias ou um ARN alias nessa situação.

Aqui está um exemplo de ARN de chave:

```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Para obter mais informações sobre a especificação de chaves do KMS em instruções de política do IAM, consulte o [Guia do desenvolvedor do AWS Key Management Service](#).

- Na política de chaves SSE-KMS, [especifique a função do IAM usada](#) por. DataSync
- Se seu bucket do S3 for criptografado com uma AWS KMS chave gerenciada pelo cliente (DSSE-KMS) para criptografia de camada dupla no lado do servidor, a [política da chave deve incluir a função do IAM usada](#) para acessar o bucket. DataSync (Lembre-se de que o DSSE-KMS não é compatível com [chaves de bucket do S3](#), o que pode reduzir AWS KMS os custos da solicitação.)
- Se seu bucket do S3 estiver criptografado com uma chave de criptografia fornecida pelo cliente (SSE-C), não é DataSync possível acessar esse bucket.

Exemplo: política de chaves SSE-KMS para DataSync

O exemplo a seguir é uma [política de chave](#) para uma chave SSE-KMS gerenciada pelo cliente. A política está associada a um bucket do S3 que usa criptografia no lado do servidor.

Se você desejar usar esse exemplo, substitua os valores a seguir pelos seus:

- ***account-id***— Seu Conta da AWS.

- *admin-role-name*— O nome da função do IAM que pode administrar a chave.
- *datasync-role-name*— O nome da função do IAM que permite DataSync usar a chave ao acessar o bucket.

JSON

```
{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access for Key Administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:role/admin-role-name"
      },
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms>Delete*",
        "kms:TagResource",
        "kms:UntagResource",
        "kms:ScheduleKeyDeletion",
        "kms:CancelKeyDeletion"
      ]
    }
  ],
}
```

```

        "Resource": "*"
    },
    {
        "Sid": "Allow use of the key",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::account-id:role/datasync-role-name"
        },
        "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*"
        ],
        "Resource": "*"
    }
]
}

```

Acesso aos buckets restritos do S3

Se você precisar transferir para ou de um bucket do S3 que normalmente nega todo o acesso, você pode editar a política do bucket para que DataSync possa acessar o bucket somente para sua transferência.

Exemplo: permissão de acesso com base nos perfis do IAM

1. Copie a política de bucket do S3 a seguir.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "Deny-access-to-bucket",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": [
            "arn:aws:s3::amzn-s3-demo-bucket",
            "arn:aws:s3::amzn-s3-demo-bucket/*"
        ]
    }]
}

```



```

    ],
    "Condition": {
      "StringNotLike": {
        "aws:userid": [
          "datasync-iam-role-id:*",
          "your-iam-role-id"
        ]
      }
    }
  }
}

```

2. Na política, substitua os seguintes valores:

- *amzn-s3-demo-bucket*: especifique o nome do bucket restrito do S3.
- *datasync-iam-role-id*— Especifique o ID da [função do IAM DataSync usada](#) para acessar o bucket.

Execute o AWS CLI comando a seguir para obter o ID da função do IAM:

```
aws iam get-role --role-name datasync-iam-role-name
```

Na saída, procure o valor RoleId:

```
"RoleId": "ANPAJ2UCCR6DPCEXAMPLE"
```

- *your-iam-role-id*— Especifique o ID da função do IAM que você usa para criar sua DataSync localização para o bucket.

Execute o comando a seguir para criar a ID do perfil do IAM:

```
aws iam get-role --role-name your-iam-role-name
```

Na saída, procure o valor RoleId:

```
"RoleId": "AIDACKCEVSQ6C2EXAMPLE"
```

3. [Adicione essa política](#) à política do bucket do S3.

4. Quando você terminar de usar DataSync o bucket restrito, remova as condições para ambas as funções do IAM da política do bucket.

Acesso aos buckets do S3 com acesso restrito à VPC

Um bucket do Amazon S3 que [limita o acesso a endpoints específicos de nuvem privada virtual \(VPC\) ou VPCs negará a transferência DataSync de ou](#) para esse bucket. Para permitir transferências nessas situações, você pode atualizar a política do bucket para incluir a função do IAM que você [especifica com sua DataSync localização](#).

Option 1: Allowing access based on DataSync location role ARN

Na política de bucket do S3, você pode especificar o Amazon Resource Name (ARN) da DataSync sua função de localização do IAM.

O exemplo a seguir é uma política de bucket do S3 que nega o acesso de todos, exceto dois VPCs (vpc-1234567890abcdef0evpc-abcdef01234567890). No entanto, a política também inclui a [ArnNotLikeIfExists](#) condição e a chave de PrincipalArn condição [aws:](#), que permitem que o ARN de uma função de DataSync localização acesse o bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCs-only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceVpc": [
            "vpc-1234567890abcdef0",
            "vpc-abcdef01234567890"
          ]
        },
        "ArnNotLikeIfExists": {
          "aws:PrincipalArn": [
            "arn:aws:iam::account-id:role/datasync-location-role-  
name"
          ]
        }
      }
    }
  ]
}
```

```
}
```

Option 2: Allowing access based on DataSync location role tag

Na política de bucket do S3, você pode especificar uma tag anexada à sua função de DataSync localização do IAM.

O exemplo a seguir é uma política de bucket do S3 que nega o acesso de todos, exceto dois VPCs (`vpc-1234567890abcdef0` e `vpc-abcdef01234567890`). No entanto, a política também inclui a [StringNotEqualsIfExists](#) condição e [aws: PrincipalTag](#) condition key, que permitem um principal com a chave `exclude-from-vpc-restriction` e o valor da tag `true`. Você pode tentar uma abordagem semelhante em sua política de bucket especificando uma tag anexada à sua função de DataSync localização.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCs-only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringNotEqualsIfExists": {
          "aws:SourceVpc": [
            "vpc-1234567890abcdef0",
            "vpc-abcdef01234567890"
          ],
          "aws:PrincipalTag/exclude-from-vpc-restriction": "true"
        }
      }
    }
  ]
}
```

Considerações sobre as classes de armazenamento com transferências do Amazon S3

Quando o Amazon S3 é seu local de destino, DataSync você pode transferir seus dados diretamente para uma classe de armazenamento específica do [Amazon S3](#).

Algumas classes de armazenamento têm comportamentos que podem afetar os custos de armazenamento do Amazon S3. Ao usar classes de armazenamento que podem gerar custos adicionais por substituição, exclusão ou recuperação de objetos, as alterações em dados ou metadados de objetos resultam nesses custos. Para obter mais informações, consulte [Preço do Amazon S3](#).

Important

Novos objetos transferidos para o local de destino no Amazon S3 são armazenados usando a classe de armazenamento que você especifica ao [criar o local](#).

Por padrão, DataSync preserva a classe de armazenamento dos objetos existentes em seu local de destino, a menos que você configure sua tarefa para [transferir todos os dados](#). Nessas situações, a classe de armazenamento que você especifica ao criar sua localização é usada para todos os objetos.

Classe de armazenamento do Amazon S3	Considerações
S3 Standard	Selecione S3 Standard (Padrão) para armazenar seus arquivos acessados com frequência de forma redundante em várias zonas de disponibilidade separadas geograficamente. Esse será o padrão se você não especificar uma classe de armazenamento.
S3 Intelligent-Tiering	Escolha S3 Intelligent-Tiering para otimizar os custos de armazenamento movendo automaticamente os dados para o nível de acesso de armazenamento mais econômico. Você paga uma taxa mensal por objeto armazenado na classe de armazenamento S3 Intelligent-Tiering. Essa cobrança do Amazon S3 inclui o monitoramento de padrões de acesso a dados e a movimentação de objetos entre níveis.

Classe de armazenamento do Amazon S3	Considerações
S3 Standard – IA	Selecione S3 Standard-IA para armazenar seus objetos raramente acessados de forma redundante em várias zonas de disponibilidade separadas geograficamente. Os objetos armazenados na classe de armazenamento S3 Standard-IA podem incorrer em cobranças adicionais pela substituição, exclusão ou recuperação. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Alterações nos dados ou metadados do objeto equivalem a excluir um objeto e criar um novo para substituí-lo. Isso resulta em cobranças adicionais para objetos armazenados na classe de armazenamento S3 Standard-IA. Objetos com menos de 128 KB são menores que a cobrança de capacidade mínima por objeto na classe de armazenamento S3 Standard-IA. Esses objetos são armazenados na classe de armazenamento S3 Standard.
S3 One Zone-IA	Selecione S3 One Zone-IA para armazenar seus objetos raramente acessados em uma única zona de disponibilidade. Os objetos armazenados na classe de armazenamento S3 One Zone-IA podem incorrer em cobranças adicionais pela substituição, exclusão ou recuperação. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Alterações nos dados ou metadados do objeto equivalem a excluir um objeto e criar um novo para substituí-lo. Isso resulta em cobranças adicionais para objetos armazenados na classe de armazenamento S3 One Zone-IA. Objetos com menos de 128 KB são menores que a cobrança de capacidade mínima por objeto na classe de armazenamento S3 One Zone-IA. Esses objetos são armazenados na classe de armazenamento S3 Standard.

Classe de armazenamento do Amazon S3	Considerações
S3 Glacier Instant Retrieval	Escolha o S3 Glacier Instant Retrieval para arquivar objetos que raramente são acessados, mas que precisam ser recuperados em milissegundos. Os dados armazenados na classe de armazenamento S3 Glacier Instant Retrieval oferecem economia de custos em comparação à classe de armazenamento S3 Standard – IA, com a mesma latência e performance do throughput. Contudo, os custos de acesso a dados do S3 Glacier Instant Retrieval são mais altos que os do S3 Standard-IA. Os objetos armazenados no S3 Glacier Instant Retrieval podem incorrer em cobranças adicionais pela substituição, exclusão ou recuperação. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Alterações nos dados ou metadados do objeto equivalem a excluir um objeto e criar um novo para substituí-lo. Isso resulta em cobranças adicionais para objetos armazenados na classe de armazenamento S3 Glacier Instant Retrieval. Objetos com menos de 128 KB são menores que a cobrança mínima de capacidade por objeto na classe de armazenamento S3 Glacier Instant Retrieval. Esses objetos são armazenados na classe de armazenamento S3 Standard.

Classe de armazenamento do Amazon S3	Considerações
S3 Glacier Flexible Retrieval	Escolha S3 Glacier Flexible Retrieval para arquivos mais ativos. Os objetos armazenados na classe S3 Glacier Flexible Retrieval podem incorrer em cobranças adicionais pela substituição, exclusão ou recuperação. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Alterações nos dados ou metadados do objeto equivalem a excluir um objeto e criar um novo para substituí-lo. Isso resulta em cobranças adicionais para objetos armazenados na classe de armazenamento S3 Glacier Flexible Retrieval. A classe de armazenamento S3 Glacier Flexible Retrieval exige 40 KB de metadados adicionais para cada objeto arquivado. DataSync coloca objetos com menos de 40 KB na classe de armazenamento S3 Standard. Você deve restaurar objetos arquivados nessa classe de armazenamento antes de DataSync poder lê-los. Para obter mais informações, consulte Trabalhar com objetos arquivados no Guia do usuário do Amazon S3. Ao usar o S3 Glacier Flexible Retrieval, escolha a opção de tarefa Verificar somente os dados transferidos para comparar somas de verificação de dados e metadados no final da transferência. Você não pode usar a opção Verificar todos os dados no destino para essa classe de armazenamento, pois requer a recuperação de todos os objetos existentes do destino.

Classe de armazenamento do Amazon S3	Considerações
S3 Glacier Deep Archive	Escolha S3 Glacier Deep Archive para arquivar seus objetos para retenção de dados de longo prazo e preservação digital, no caso em que os dados são acessados uma ou duas vezes por ano. Os objetos armazenados no S3 Glacier Deep Archive podem incorrer em cobranças adicionais pela substituição, exclusão ou recuperação. Considere a frequência com que esses objetos mudam, por quanto tempo você planeja manter esses objetos e com que frequência você precisa acessá-los. Alterações nos dados ou metadados do objeto equivalem a excluir um objeto e criar um novo para substituí-lo. Isso resulta em cobranças adicionais para objetos armazenados na classe de armazenamento S3 Glacier Deep Archive. A classe de armazenamento S3 Glacier Deep Archive exige 40 KB de metadados adicionais para cada objeto arquivado. DataSync coloca objetos com menos de 40 KB na classe de armazenamento S3 Standard. Você deve restaurar objetos arquivados nessa classe de armazenamento antes de DataSync poder lê-los. Para obter mais informações, consulte Trabalhar com objetos arquivados no Guia do usuário do Amazon S3. Ao usar o S3 Glacier Deep Archive, escolha a opção de tarefa Verificar somente os dados transferidos para comparar somas de verificação de dados e metadados no final da transferência. Você não pode usar a opção Verificar todos os dados no destino para essa classe de armazenamento, pois requer a recuperação de todos os objetos existentes do destino.
S3 Outposts	Classe de armazenamento para o Amazon S3 no Outposts.

Avaliando os custos de solicitação do S3 ao usar DataSync

Com os locais do Amazon S3, você incorre em custos relacionados às solicitações de API do S3 feitas por DataSync. Esta seção pode ajudá-lo a entender como DataSync usa essas solicitações e como elas podem afetar seus custos do [Amazon S3](#).

Tópicos

- [Solicitações do S3 feitas por DataSync](#)
- [Considerações sobre custos](#)

Solicitações do S3 feitas por DataSync

A tabela a seguir descreve as solicitações do S3 que você DataSync pode fazer quando você está copiando dados de ou para um local do Amazon S3.

Solicitação do S3	Como DataSync o usa
ListObjectV2	DataSync faz pelo menos uma LIST solicitação para cada objeto que termina em uma barra (/) para listar os objetos que começam com esse prefixo. Essa solicitação é chamada durante a fase de preparação de uma tarefa.
HeadObject	DataSync faz HEAD solicitações para recuperar metadados do objeto durante as fases de preparação e verificação de uma tarefa. Pode haver várias HEAD solicitações por objeto, dependendo de como você DataSync deseja verificar a integridade dos dados que ele transfere .
GetObject	DataSync faz GET solicitações para ler dados de um objeto durante a fase de transferência de uma tarefa. Pode haver várias solicitações de GET para objetos grandes.
GetObjectTagging	Se você configurar sua tarefa para copiar tags de objeto , DataSync faça essas GET solicitações

Solicitação do S3	Como DataSync o usa
	ões para verificar as tags de objeto durante as fases de preparação e transferência da tarefa.
PutObject	DataSync faz PUT solicitações para criar objetos e prefixos em um bucket do S3 de destino durante a fase de transferência de uma tarefa. Como DataSync usa o recurso de upload de várias partes do Amazon S3 , pode haver várias PUT solicitações para objetos grandes. Para ajudar a minimizar os custos de armazenamento, recomendamos o uso de uma configuração de ciclo de vida para impedir uploads incompletos de várias partes.
PutObjectTagging	Se seus objetos de origem tiverem tags e você configurar sua tarefa para copiar tags de objetos , DataSync faça essas PUT solicitações ao transferir essas tags.
CopyObject	DataSync faz uma COPY solicitação para criar uma cópia de um objeto somente se os metadados desse objeto mudarem. Isso pode acontecer se você copiou originalmente os dados para o bucket do S3 usando outro serviço ou ferramenta que não transferiu seus metadados.

Considerações sobre custos

DataSync faz solicitações do S3 nos buckets do S3 toda vez que você executa sua tarefa. Isso pode fazer com que as cobranças aumentem em determinadas situações. Por exemplo:

- Você está frequentemente transferindo objetos para ou de um bucket do S3.
- Talvez você não esteja transferindo muitos dados, mas o bucket do S3 contém muitos objetos. Você ainda pode ver altas cobranças nesse cenário porque DataSync faz solicitações do S3 em cada um dos objetos do bucket.

- Você está transferindo entre buckets do S3, assim DataSync como fazendo solicitações do S3 na origem e no destino.

Para ajudar a minimizar os custos de solicitação do S3 relacionados a DataSync, considere o seguinte:

Tópicos

- [Quais classes de armazenamento do S3 eu estou usando?](#)
- [Com que frequência preciso transferir meus dados?](#)

Quais classes de armazenamento do S3 eu estou usando?

As taxas de solicitação do S3 podem variar de acordo com a classe de armazenamento do Amazon S3 que os objetos estão usando, principalmente para classes que arquivam objetos (como S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive).

Aqui estão alguns cenários nos quais as classes de armazenamento podem afetar suas cobranças de solicitação do S3 durante o uso DataSync:

- Sempre que você executa uma tarefa, DataSync faz HEAD solicitações para recuperar metadados do objeto. Essas solicitações resultam em cobranças mesmo se você não estiver movendo nenhum objeto. O quanto essas solicitações afetam sua fatura depende da classe de armazenamento que seus objetos estão usando, juntamente com o número de objetos DataSync digitalizados.
- Se você moveu objetos para a classe de armazenamento S3 Glacier Instant Retrieval (diretamente ou por meio de uma configuração de ciclo de vida do bucket), as solicitações de objetos dessa classe são mais caras do que de outras classes de armazenamento.
- Se você configurar sua DataSync tarefa para [verificar se os locais de origem e destino estão totalmente sincronizados](#), haverá GET solicitações para cada objeto em todas as classes de armazenamento (exceto S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive).
- Além das solicitações de GET, você incorre em custos de recuperação de dados para objetos nas classes de armazenamento S3 Standard-IA, S3 One Zone-IA ou S3 Glacier Instant Retrieval.

Para obter mais informações, consulte [Definição de preço do Amazon S3](#).

Com que frequência preciso transferir meus dados?

Se você precisar mover dados de forma recorrente, pense em um [cronograma](#) que não execute mais tarefas do que o necessário.

Você também pode considerar limitar o escopo de suas transferências. Por exemplo, você pode configurar DataSync para focar em objetos em determinados prefixos ou [filtrar quais dados são transferidos](#). Essas opções podem ajudar a reduzir o número de solicitações do S3 feitas sempre que você executa sua DataSync tarefa.

Outras considerações sobre transferências do Amazon S3

- Se você estiver transferindo de um bucket S3, use a [Lente de Armazenamento do S3](#) para descobrir quantos objetos você está movendo.
- [Ao fazer a transferência entre buckets do S3, recomendamos usar o modo de tarefa aprimorado porque você não está sujeito às DataSync cotas de tarefas.](#)
- DataSync talvez não transfira um objeto com caracteres não padrão em seu nome. Para obter mais informações, consulte [Diretrizes de nomeação de chave de objeto](#) no Guia do usuário do Amazon S3.
- Ao usar DataSync com um bucket do S3 que usa controle de [versão, lembre-se do](#) seguinte:
 - Ao transferir para um bucket do S3, DataSync cria uma nova versão de um objeto se esse objeto for modificado na origem. Isso resulta em custos adicionais.
 - Um objeto tem uma versão diferente IDs nos buckets de origem e destino.
- Depois de transferir inicialmente os dados de um bucket do S3 para um sistema de arquivos (por exemplo, NFS ou Amazon FSx), as execuções subsequentes da mesma DataSync tarefa não incluirão objetos que foram modificados, mas têm o mesmo tamanho da primeira transferência.

Criando seu local de transferência para um bucket de uso geral do Amazon S3

Para criar um local para sua transferência, você precisa de um bucket S3 de uso geral existente. Se você não tiver um, consulte o Guia do [usuário do Amazon S3](#).

Important

Antes de criar seu local, leia as seguintes seções:

- [Considerações sobre as classes de armazenamento com transferências do Amazon S3](#)

- [Avaliando os custos de solicitação do S3 ao usar DataSync](#)

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de localização, escolha Amazon S3 e, em seguida, escolha Balde de uso geral.
4. Para URI do S3, insira ou escolha o bucket e o prefixo que você deseja usar para sua localização.

Warning

DataSync não é possível transferir objetos com um prefixo que comece com uma barra (/) ou inclua ///./, ou /../ padrões. Por exemplo:

- /photos
- photos//2006/January
- photos/./2006/February
- photos/././2006/March

5. Para a classe de armazenamento S3 quando usada como destino, escolha uma classe de armazenamento que você deseja que seus objetos usem quando o Amazon S3 for um destino de transferência.

Para obter mais informações, consulte [Considerações sobre a classes de armazenamento com transferências do Amazon S3](#).

6. Em Perfil do IAM, siga um destes procedimentos:
 - Escolha Autogenerate DataSync para criar automaticamente uma função do IAM com as permissões necessárias para acessar o bucket do S3.

Se uma função do IAM foi criada DataSync anteriormente para esse bucket do S3, essa função é escolhida por padrão.

 - Escolha um perfil do IAM personalizado que você criou. Para obter mais informações, consulte [Criação de uma função do IAM DataSync para acessar sua localização no Amazon S3](#).

7. (Opcional) Escolha Adicionar nova tag para marcar sua localização no Amazon S3.

Tags ajudam a gerenciar, filtrar e procurar recursos. Recomendamos criar uma etiqueta de nome para a sua localização.

8. Escolha Criar local.

Usando o AWS CLI

1. Copie o seguinte comando `create-location-s3`:

```
aws datasync create-location-s3 \
  --s3-bucket-arn 'arn:aws:s3:::amzn-s3-demo-bucket' \
  --s3-storage-class 'your-S3-storage-class' \
  --s3-config 'BucketAccessRoleArn=arn:aws:iam::account-id:role/role-allowing-  
datasync-operations' \
  --subdirectory /your-prefix-name
```

2. Em `--s3-bucket-arn`, especifique o ARN do bucket do S3 que você deseja usar como um local.
3. Em `--s3-storage-class`, especifique uma classe de armazenamento que você deseja que os objetos usem quando o Amazon S3 for um destino de transferência.
4. Para `--s3-config`, especifique o ARN da função do IAM que DataSync precisa acessar seu bucket.

Para obter mais informações, consulte [Criação de uma função do IAM DataSync para acessar sua localização no Amazon S3](#).

5. Para `--subdirectory`, especifique um prefixo no bucket do S3 que DataSync leia ou grave (dependendo se o bucket é um local de origem ou destino).

Warning

DataSync não é possível transferir objetos com um prefixo que comece com uma barra (/) ou inclua `///./`, ou `/. ./` padrões. Por exemplo:

- `/photos`
- `photos//2006/January`
- `photos/./2006/February`

- `photos/./2006/March`

6. Execute o comando `create-location-s3`.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN do local que você criou. Por exemplo:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0b3017fc4ba4a2d8d"
}
```

Você pode usar esse local como origem ou destino para sua DataSync tarefa.

Criando seu local de transferência para um bucket do S3 on Outposts

Para criar um local para sua transferência, você precisa de um bucket existente do Amazon S3 on Outposts. Se você não tiver um, consulte o Guia do usuário do [Amazon S3 on Outposts](#).

Você também precisa de um DataSync agente. Para obter mais informações, consulte [Implantando seu agente em AWS Outposts](#).

Ao transferir de um prefixo de bucket do S3 on Outposts que contém um grande conjunto de dados (como centenas de milhares ou milhões de objetos), sua tarefa pode atingir o tempo limite. DataSync Para evitar isso, considere usar um [DataSync manifesto](#), que permite especificar os objetos exatos que você precisa transferir.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Para Tipo de localização, escolha Amazon S3 e, em seguida, escolha Outposts bucket.
4. Para o bucket do S3, escolha um ponto de acesso do Amazon S3 que possa acessar seu bucket do S3 on Outposts.

Para obter mais informações, consulte o [Guia do usuário do Amazon S3](#).

5. Para a classe de armazenamento S3 quando usada como destino, escolha uma classe de armazenamento que você deseja que seus objetos usem quando o Amazon S3 for um destino de transferência.

Para obter mais informações, consulte [Considerações sobre a classes de armazenamento com transferências do Amazon S3](#). DataSync por padrão, usa a classe de armazenamento S3 Outposts para Amazon S3 on Outposts.

6. Para agentes, especifique o Amazon Resource Name (ARN) do DataSync agente em seu Outpost.
7. Em Pasta, insira um prefixo no bucket do S3 que DataSync lê ou grava (dependendo se o bucket é um local de origem ou destino).

 Warning

DataSync não é possível transferir objetos com um prefixo que comece com uma barra (/) ou inclua ///./, ou /../ padrões. Por exemplo:

- /photos
- photos//2006/January
- photos/./2006/February
- photos/../2006/March

8. Em Perfil do IAM, siga um destes procedimentos:
 - Escolha Autogenerate DataSync para criar automaticamente uma função do IAM com as permissões necessárias para acessar o bucket do S3.

Se uma função do IAM foi criada DataSync anteriormente para esse bucket do S3, essa função é escolhida por padrão.

 - Escolha um perfil do IAM personalizado que você criou. Para obter mais informações, consulte [Criação de uma função do IAM DataSync para acessar sua localização no Amazon S3](#).
9. (Opcional) Escolha Adicionar nova tag para marcar sua localização no Amazon S3.

Tags ajudam a gerenciar, filtrar e procurar recursos. Recomendamos criar uma etiqueta de nome para a sua localização.

10. Escolha Criar local.

Usando o AWS CLI

1. Copie o seguinte comando `create-location-s3`:

```
aws datasync create-location-s3 \
  --s3-bucket-arn 'bucket-access-point' \
  --s3-storage-class 'your-S3-storage-class' \
  --s3-config 'BucketAccessRoleArn=arn:aws:iam::account-id:role/role-allowing-  
datasync-operations' \
  --subdirectory /your-folder \
  --agent-arns 'arn:aws:datasync:your-region:account-id:agent/agent-agent-id'
```

2. Para `--s3-bucket-arn`, especifique o ARN de um ponto de acesso Amazon S3 que pode acessar seu bucket do S3 no Outposts.

Para obter mais informações, consulte o [Guia do usuário do Amazon S3](#).

3. Em `--s3-storage-class`, especifique uma classe de armazenamento que você deseja que os objetos usem quando o Amazon S3 for um destino de transferência.

Para obter mais informações, consulte [Considerações sobre a classes de armazenamento com transferências do Amazon S3](#). DataSync por padrão, usa a classe de armazenamento S3 Outposts para S3 on Outposts.

4. Para `--s3-config`, especifique o ARN da função do IAM que DataSync precisa acessar seu bucket.

Para obter mais informações, consulte [Criação de uma função do IAM DataSync para acessar sua localização no Amazon S3](#).

5. Para `--subdirectory`, especifique um prefixo no bucket do S3 que DataSync leia ou grave (dependendo se o bucket é um local de origem ou destino).

Warning

DataSync não é possível transferir objetos com um prefixo que comece com uma barra (/) ou inclua `///./`, ou `/./` padrões. Por exemplo:

- `/photos`
- `photos//2006/January`
- `photos/./2006/February`

- `photos/./2006/March`

6. Para `--agent-arns`, especifique o ARN do DataSync agente em seu Posto Avançado.
7. Execute o comando `create-location-s3`.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN do local que você criou. Por exemplo:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0b3017fc4ba4a2d8d"
}
```

Você pode usar esse local como origem ou destino para sua DataSync tarefa.

Transferências do Amazon S3 entre Contas da AWS

[Com DataSync, você pode mover dados de ou para buckets do S3 em diferentes. Contas da AWS](#)

Para obter mais informações, consulte os seguintes tutoriais:

- [Transferência de dados do armazenamento local para o Amazon S3 em Contas da AWS](#)
- [Transferência de dados do Amazon S3 para o Amazon S3 em Contas da AWS](#)

Transferências do Amazon S3 entre regiões comerciais e AWS GovCloud (US) Regions

Por padrão, DataSync não é transferido entre buckets S3 em ambientes comerciais e. AWS GovCloud (US) Regions Porém, você ainda pode configurar esse tipo de transferência criando um local de armazenamento de objetos para um dos buckets do S3 da transferência. Você pode realizar esse tipo de transferência com ou sem um agente. Se você usa um agente, sua tarefa deve ser configurada para o modo Básico. Para transferir sem um agente, você deve usar o modo Avançado.

Antes de começar: certifique-se de que compreende as implicações de custos de transferir entre regiões. Para obter mais informações, consulte [Preços do AWS DataSync](#).

Sumário

- [Fornecendo DataSync acesso ao bucket do seu local de armazenamento de objetos](#)

- [Criando seu DataSync agente \(opcional\)](#)
- [Criação de um local de armazenamento de objetos para o bucket do S3](#)

Fornecendo DataSync acesso ao bucket do seu local de armazenamento de objetos

Ao criar o local de armazenamento de objetos para essa transferência, você deve fornecer DataSync as credenciais de um usuário do IAM com permissão para acessar o bucket S3 do local. Para obter mais informações, consulte [Permissões obrigatórias](#).

 Warning

Os usuários do IAM têm credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários.

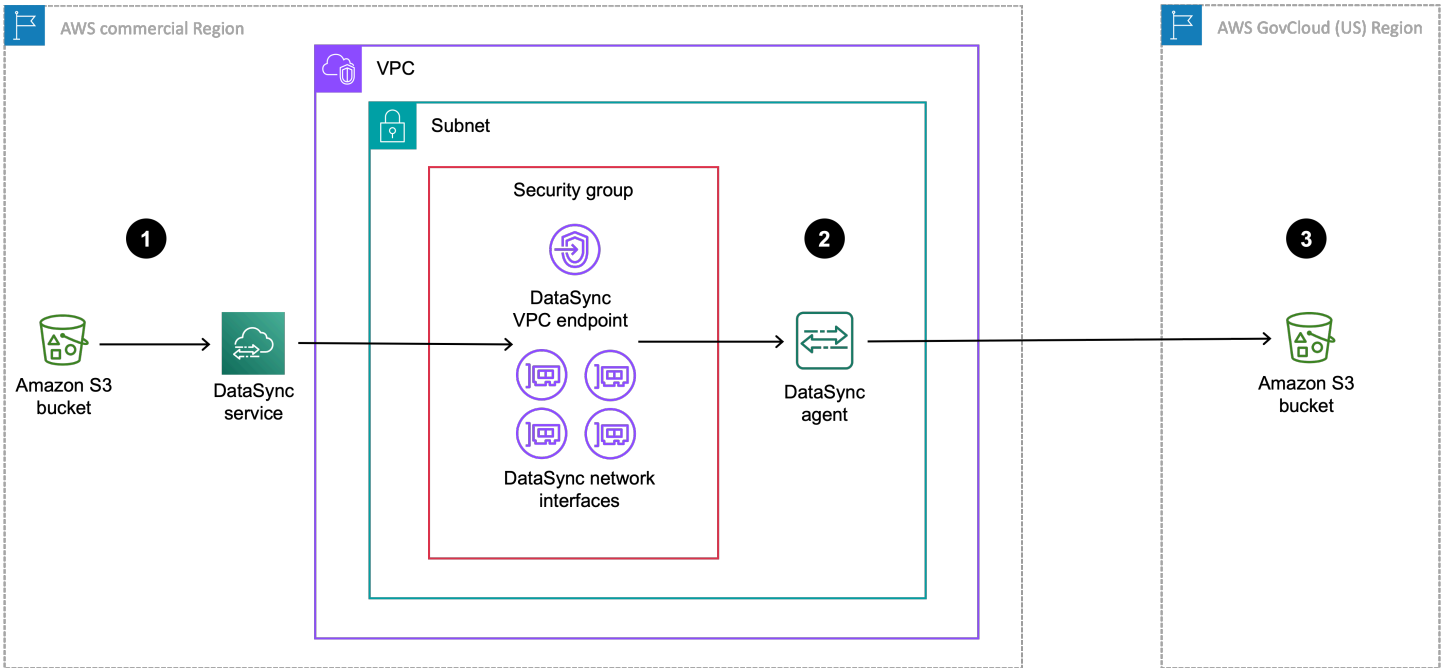
Criando seu DataSync agente (opcional)

Se você quiser executar sua transferência usando o modo Básico, precisará usar um agente. Como você está se transferindo entre um comercial e um AWS GovCloud (US) Region, você implanta seu DataSync agente como uma EC2 instância da Amazon em uma das regiões. Recomendamos que o agente use um endpoint de serviço da VPC para evitar custos de transferência de dados para a Internet pública. Para obter mais informações, consulte os [preços do Amazon EC2 Data Transfer](#).

Escolha um dos cenários a seguir que descrevem como criar um agente com base na região em que você planeja executar sua DataSync tarefa.

Ao executar uma DataSync tarefa em uma região comercial

O diagrama a seguir mostra uma transferência em que sua DataSync tarefa e seu agente estão na região comercial.



Referência	Descrição
1	Na região comercial em que você está executando uma DataSync tarefa, os dados são transferidos do bucket S3 de origem. O bucket de origem é configurado como um local no Amazon S3 na região comercial.
2	Transferências de dados por meio do DataSync agente, que está na mesma VPC e sub-rede em que o endpoint do serviço VPC e as interfaces de rede estão localizados.
3	Transferências de dados para o bucket do S3 de destino na AWS GovCloud (US) Region. O bucket de destino é configura do como um local de armazenamento de objetos na região comercial.

Você também pode usar essa mesma configuração para transferir a direção oposta da AWS GovCloud (US) Region para a região comercial.

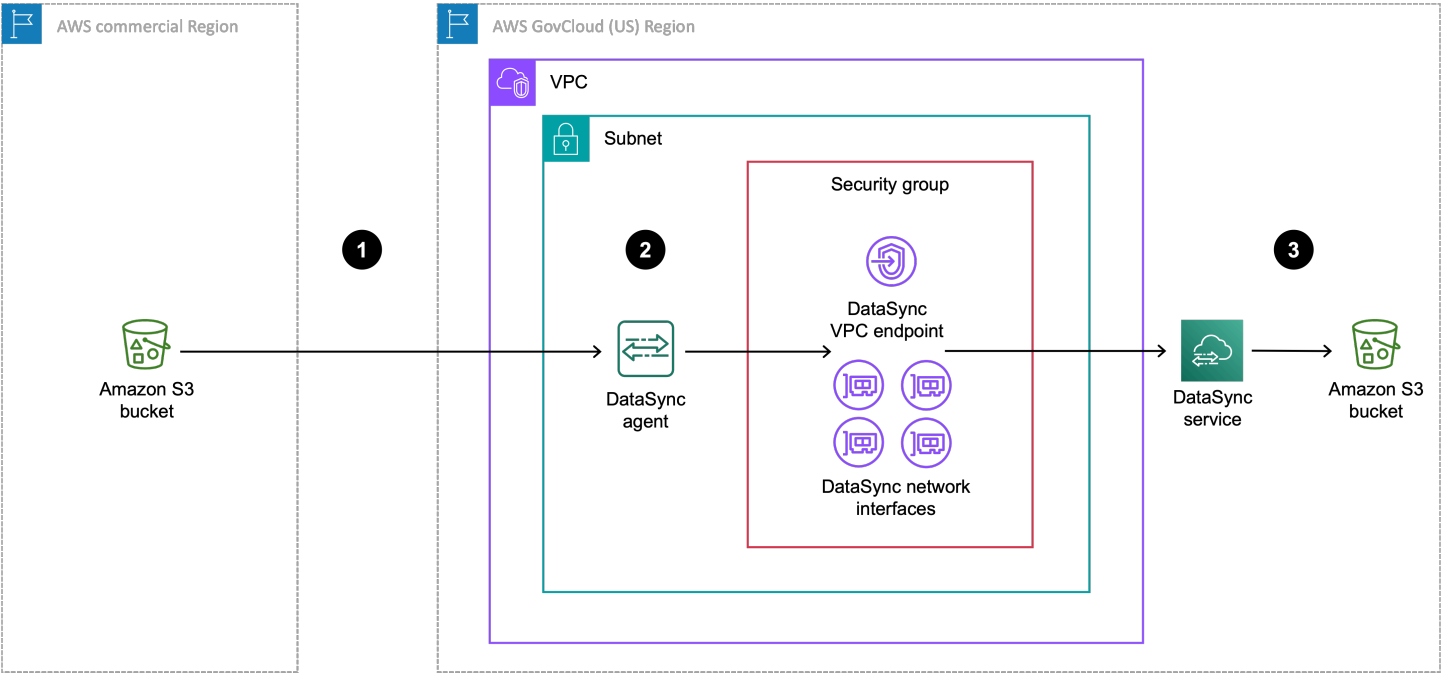
Para criar seu DataSync agente

1. [Implante um EC2 agente da Amazon](#) em sua região comercial.

2. Configure o agente para usar um [endpoint de serviço da VPC](#).
3. [Ative o agente](#).

Ao executar uma DataSync tarefa em uma região GovCloud (EUA)

O diagrama a seguir mostra uma transferência em que sua DataSync tarefa e seu agente estão no AWS GovCloud (US) Region.



Referência	Descrição
1	Transferências de dados do bucket S3 de origem na região comercial para o AWS GovCloud (US) Region local em que você está executando uma DataSync tarefa. O bucket de origem é configurado como um local de armazenamento de objetos na AWS GovCloud (US) Region.
2	No AWS GovCloud (US) Region, os dados são transferidos por meio do DataSync agente na mesma VPC e sub-rede em que o endpoint do serviço VPC e as interfaces de rede estão localizados.

Referência	Descrição
3	Transferências de dados para o bucket do S3 de destino na AWS GovCloud (US) Region. O bucket de destino é configurado como um local do Amazon S3 na AWS GovCloud (US) Region.

Você também pode usar essa mesma configuração para transferir a direção oposta da AWS GovCloud (US) Region para a região comercial.

Para criar seu DataSync agente

1. [Implante um EC2 agente da Amazon](#) em seu AWS GovCloud (US) Region.
2. Configure o agente para usar um [endpoint de serviço da VPC](#).
3. [Ative o agente](#).

Se o conjunto de dados for altamente compactável, você poderá ter uma redução de custos se criar o agente em uma região comercial enquanto executa uma tarefa em uma AWS GovCloud (US) Region. Há necessidade de mais configuração do que o normal para criar esse agente, incluindo preparar o agente para uso em uma região comercial. Para obter informações sobre como criar um agente para essa configuração, consulte o AWS DataSync blog [Mover dados para dentro e para fora AWS GovCloud \(US\) com](#).

Criação de um local de armazenamento de objetos para o bucket do S3

Você precisa de um local de armazenamento de objetos para o bucket do S3 que esteja na região em que você não está executando sua DataSync tarefa.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. Verifique se você está na mesma região em que planeja executar a tarefa.
3. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
4. Em Tipo de localização, escolha Armazenamento de objetos.
5. Para Agentes, escolha o DataSync agente que você criou para essa transferência.

6. Em Servidor, insira um endpoint do Amazon S3 para o bucket usando um dos seguintes formatos:

- Bucket de região comercial: `s3.your-region.amazonaws.com`
- Bucket de AWS GovCloud (US) Region : `s3.your-gov-region.amazonaws.com`

Para obter uma lista dos endpoints do Amazon S3, consulte [Referência geral da AWS](#).

7. Em nome do bucket, insira o nome do bucket do S3.
8. Em Pasta, insira um prefixo no bucket do S3 que DataSync lê ou grava (dependendo se o bucket é um local de origem ou destino).

 Warning

DataSync não é possível transferir objetos com um prefixo que comece com uma barra (/) ou inclua `///.`, ou `/. ./` padrões. Por exemplo:

- `/photos`
- `photos//2006/January`
- `photos/. /2006/February`
- `photos/. ./2006/March`

9. Selecione Exige credenciais e faça o seguinte:
- Em Chave de acesso, insira a chave de acesso de um [usuário do IAM](#) que possa acessar o bucket.
 - Em Chave secreta, insira a mesma chave secreta do usuário do IAM.
10. (Opcional) Escolha Adicionar tag para marcar sua localização.

Tags ajudam a gerenciar, filtrar e procurar recursos. Recomendamos criar uma etiqueta de nome para a sua localização.

11. Escolha Criar local.

Como usar o AWS CLI

1. Copie o seguinte comando `create-location-object-storage`:

```
aws datasync create-location-object-storage \
  --server-hostname s3-endpoint \
  --bucket-name amzn-s3-demo-bucket \
  --agent-arns arn:aws:datasync:your-region:123456789012:agent/
agent-01234567890deadfb
```

2. No parâmetro `--server-hostname`, especifique um endpoint do Amazon S3 para o bucket usando um dos seguintes formatos:

- Bucket de região comercial: `s3.your-region.amazonaws.com`
- Bucket de AWS GovCloud (US) Region : `s3.your-gov-region.amazonaws.com`

Para a região no endpoint, certifique-se de especificar a mesma região em que você planeja executar a tarefa.

Para obter uma lista dos endpoints do Amazon S3, consulte [Referência geral da AWS](#).

3. No parâmetro `--bucket-name`, especifique o nome do bucket do S3.
4. Para o `--agent-arns` parâmetro, especifique o DataSync agente que você criou para essa transferência.
5. No parâmetro `--access-key`, especifique a chave de acesso para um [usuário do IAM](#) que possa acessar o bucket.
6. No parâmetro `--secret-key`, insira a mesma chave secreta do usuário do IAM.
7. (Opcional) Para o `--subdirectory` parâmetro, especifique um prefixo no bucket do S3 que DataSync lê ou grava (dependendo se o bucket é um local de origem ou destino).

Warning

DataSync não é possível transferir objetos com um prefixo que comece com uma barra (/) ou inclua `///./`, ou `/../` padrões. Por exemplo:

- `/photos`
- `photos//2006/January`
- `photos/./2006/February`
- `photos/../2006/March`

8. (Opcional) No parâmetro `--tags`, especifique os pares chave-valor que representam as tags para o recurso do local.

Tags ajudam a gerenciar, filtrar e procurar recursos. Recomendamos criar uma etiqueta de nome para a sua localização.

9. Execute o comando `create-location-object-storage`.

Você recebe uma resposta que mostra o ARN do local que você acabou de criar.

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-01234567890abcdef"
}
```

Você pode usar esse local como origem ou destino para sua DataSync tarefa. Para o outro bucket do S3 nessa transferência, [crie um local do Amazon S3](#).

Próximas etapas

Algumas das próximas etapas possíveis incluem:

1. Se necessário, crie outro local. Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).
2. [Defina as configurações da DataSync tarefa](#), como quais arquivos transferir, como lidar com metadados, entre outras opções.
3. [Defina um cronograma](#) para sua DataSync tarefa.
4. [Configure o monitoramento](#) para sua DataSync tarefa.
5. [Inicie](#) a tarefa.

Configurando AWS DataSync transferências com o Amazon EFS

Para transferir dados para ou do seu sistema de arquivos Amazon EFS, você deve criar um local AWS DataSync de transferência. DataSync pode usar esse local como origem ou destino para transferir dados.

Fornecendo DataSync acesso aos sistemas de arquivos do Amazon EFS

[Criar um local](#) envolve entender como DataSync acessar seu armazenamento. Para o Amazon EFS, DataSync monta seu sistema de arquivos como usuário raiz a partir da sua nuvem privada virtual (VPC) [usando](#) interfaces de rede.

Sumário

- [Determinar a sub-rede e os grupos de segurança do destino de montagem](#)
- [Acesso a sistemas de arquivos restritos](#)
 - [Criação de uma função DataSync do IAM para acesso ao sistema de arquivos](#)
 - [Exemplo de política de sistema de arquivos que permite DataSync acesso](#)

Determinar a sub-rede e os grupos de segurança do destino de montagem

Ao criar sua localização, você especifica a sub-rede e os grupos de segurança que permitem DataSync a conexão com um dos [destinos de montagem](#) do seu sistema de arquivos Amazon EFS.

A sub-rede especificada deve estar localizada:

- Na mesma VPC que o sistema de arquivos.
- Na mesma zona de disponibilidade que pelo menos um destino de montagem do sistema de arquivos.

Note

Você não precisa especificar uma sub-rede que inclua um destino de montagem do sistema de arquivos.

Os grupos de segurança que você especificar devem permitir tráfego de entrada na porta NFS 2049. Para obter informações sobre a criação e a atualização de grupos de segurança para seus destinos de montagem, consulte o [Amazon EFS User Guide](#).

Especificação de grupos de segurança associados a um destino de montagem

Você pode especificar um grupo de segurança associado a um dos destinos de montagem do sistema de arquivos. Recomendamos essa abordagem do ponto de vista do gerenciamento de rede.

Especificação de grupos de segurança não associados a um destino de montagem

Você pode especificar um grupo de segurança que não esteja associado a um dos destinos de montagem do sistema de arquivos. Porém, esse grupo de segurança deve ser capaz de se comunicar com o grupo de segurança de um destino de montagem.

Por exemplo, veja como você pode criar uma relação entre o grupo de segurança D (para DataSync) e o grupo de segurança M (para o destino de montagem):

- O grupo de segurança D, que você especifica ao criar o local, deve ter uma regra que permita conexões de saída na porta NFS 2049 com o grupo de segurança M.
- O grupo de segurança M, que você associa ao destino de montagem, deve permitir acesso de entrada na porta NFS 2049 do grupo de segurança D.

Para encontrar o grupo de segurança de um destino de montagem

As instruções a seguir podem ajudá-lo a identificar o grupo de segurança de um destino de montagem do sistema de arquivos Amazon EFS que você deseja usar DataSync para sua transferência.

1. No AWS CLI, execute o `describe-mount-targets` comando a seguir.

```
aws efs describe-mount-targets \
  --region file-system-region \
  --file-system-id file-system-id
```

Esse comando retorna informações sobre os destinos de montagem do sistema de arquivos (semelhante ao exemplo de saída a seguir).

```
{
  "MountTargets": [
    {
      "OwnerId": "111222333444",
      "MountTargetId": "fsmt-22334a10",
      "FileSystemId": "fs-123456ab",
      "SubnetId": "subnet-f12a0e34",
      "LifecycleState": "available",
      "IpAddress": "11.222.0.123",
      "NetworkInterfaceId": "eni-1234a044"
    }
  ]
}
```

```
}
```

2. Anote o valor de `MountTargetId` que você deseja usar.
3. Execute o comando `describe-mount-target-security-groups` a seguir usando o `MountTargetId` para ver o grupo de segurança do destino de montagem.

```
aws efs describe-mount-target-security-groups \  
  --region file-system-region \  
  --mount-target-id mount-target-id
```

Você pode especificar um grupo de segurança ao [criar o local](#).

Acesso a sistemas de arquivos restritos

DataSync podem ser transferidos de ou para sistemas de arquivos do Amazon EFS que restringem o acesso por meio de [pontos de acesso](#) e [políticas do IAM](#).

Note

Se DataSync acessar um sistema de arquivos de destino por meio de um ponto de acesso que impõe a identidade do usuário, o usuário e o grupo POSIX IDs para seus dados de origem não serão preservados se você configurar sua DataSync tarefa para copiar a propriedade. Em vez disso, os arquivos e pastas transferidos são definidos para o usuário e o grupo do ponto de acesso IDs. Quando isso acontece, a verificação da tarefa falha porque DataSync detecta uma incompatibilidade entre os metadados nos locais de origem e destino.

Sumário

- [Criação de uma função DataSync do IAM para acesso ao sistema de arquivos](#)
- [Exemplo de política de sistema de arquivos que permite DataSync acesso](#)

Criação de uma função DataSync do IAM para acesso ao sistema de arquivos

Se você tiver um sistema de arquivos Amazon EFS que restringe o acesso por meio de uma política do IAM, você pode criar uma função do IAM que forneça DataSync permissão para ler ou gravar dados no sistema de arquivos. Depois, talvez seja necessário especificar esse perfil na [política do sistema de arquivos](#).

Para criar a função DataSync do IAM

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação esquerdo, em Gerenciamento de acesso, escolha Perfis e, em seguida, escolha Criar perfil.
3. Na página Selecionar entidade confiável, em Tipo de entidade confiável, escolha Política de confiança personalizada.
4. Cole o JSON a seguir no editor de política:

JSON

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

5. Escolha Próximo. Na página Adicionar permissões, escolha Próximo.
6. Forneça um nome ao perfil e escolha Criar perfil.

Você pode especificar esse perfil ao [criar o local](#).

Exemplo de política de sistema de arquivos que permite DataSync acesso

O exemplo de política de sistema de arquivos a seguir mostra como o acesso a um sistema de arquivos do Amazon EFS (identificado na política como `fs-1234567890abcdef0`) é restrito, mas ainda permite o acesso DataSync por meio de uma função do IAM chamada `MyDataSyncRole`:

JSON

```
{
  "Version": "2012-10-17",
  "Id": "ExampleEFSFileSystemPolicy",
```

```

    "Statement": [{
      "Sid": "AccessEFSFileSystem",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyDataSyncRole"
      },
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite",
        "elasticfilesystem:ClientRootAccess"
      ],
      "Resource": "arn:aws:elasticfilesystem:us-east-1:111122223333:file-
system/fs-1234567890abcdef0",
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "true"
        },
        "StringEquals": {
          "elasticfilesystem:AccessPointArn":
            "arn:aws:elasticfilesystem:us-east-1:111122223333:access-point/
fsap-abcdef01234567890"
        }
      }
    }]
  }
}

```

- **Principal**— Especifica uma [função do IAM](#) que dá DataSync permissão para acessar o sistema de arquivos.
- **Action**— Fornece acesso DataSync root e permite que ele leia e grave no sistema de arquivos.
- **aws:SecureTransport**: exige que clientes do NFS usem TLS ao se conectar ao sistema de arquivos.
- **elasticfilesystem:AccessPointArn**: permite o acesso ao sistema de arquivos somente por um ponto de acesso específico.

Considerações de rede com transferências do Amazon EFS

VPCs que você usa com DataSync deve ter locação padrão. VPCs com locação dedicada não são suportadas.

Considerações de performance com transferências do Amazon EFS

O modo de throughput do sistema de arquivos Amazon EFS pode afetar a duração da transferência e a performance do sistema de arquivos durante a transferência. Considere o seguinte:

- Para obter melhores resultados, recomendamos o uso do modo de throughput elástico. Se você não usar o modo de throughput elástico, a transferência pode demorar mais.
- Se você usar o modo de taxa de transferência intermitente, o desempenho dos aplicativos do seu sistema de arquivos poderá ser afetado porque DataSync consome créditos de intermitência do sistema de arquivos.
- A forma como você [configura DataSync para verificar os dados transferidos](#) pode afetar o desempenho do sistema de arquivos e os custos de acesso aos dados.

Para obter mais informações, consulte [Amazon EFS performance](#) no Amazon Elastic File System User Guide e a página [Amazon EFS Pricing](#).

Criar seu local de transferência do Amazon EFS

Para criar o local de transferência, você precisa de um sistema de arquivos do Amazon EFS. Se você não tiver um, consulte [Introdução ao Amazon Elastic File System](#) no Guia do usuário do Amazon Elastic File System.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de localização, escolha Sistema de arquivos Amazon EFS.

Você configurará esse local como origem ou destino posteriormente.

4. Para Sistema de arquivos, escolha o sistema de arquivos do Amazon EFS que você deseja usar como um local.
5. Em Caminho da montagem, digite o caminho de montagem para o sistema de arquivos Amazon EFS.

Isso especifica onde DataSync lê ou grava dados (dependendo se esse é um local de origem ou destino) no seu sistema de arquivos.

Por padrão, DataSync usa o diretório raiz (ou [ponto de acesso](#), se você fornecer um para a configuração do ponto de acesso EFS). Você também pode especificar subdiretórios usando barras (por exemplo,). `/path/to/directory`

6. Em Sub-rede, escolha uma sub-rede na qual você deseja DataSync criar as [interfaces de rede](#) para gerenciar seu tráfego de transferência de dados.

A sub-rede deve estar localizada:

- Na mesma VPC que o sistema de arquivos.
- Na mesma zona de disponibilidade que pelo menos um destino de montagem.

 Note

Você não precisa especificar uma sub-rede que inclua um destino de montagem do sistema de arquivos.

7. Em Grupos de segurança, escolha o grupo de segurança associado ao destino de montagem do sistema de arquivos Amazon EFS. Você pode escolher mais de um grupo de segurança.

 Note

O grupo de segurança que você especificar deve permitir tráfego de entrada na porta NFS 2049. Para obter mais informações, consulte [Determinar a sub-rede e os grupos de segurança do destino de montagem](#).

8. Para criptografia em trânsito, escolha se você deseja usar DataSync a criptografia TLS (Transport Layer Security) ao transferir dados para ou do seu sistema de arquivos.

 Note

Você deve habilitar essa configuração para configurar um ponto de acesso, um perfil do IAM ou ambos com o local do Amazon EFS.

9. (Opcional) Para o ponto de acesso EFS, escolha um ponto de acesso que DataSync possa ser usado para montar seu sistema de arquivos.

Para obter mais informações, consulte [Acesso a sistemas de arquivos restritos](#).

10. (Opcional) Para a função do IAM, especifique uma função que DataSync permita acessar seu sistema de arquivos.

Para obter informações sobre como criar essa função, consulte [Criação de uma função DataSync do IAM para acesso ao sistema de arquivos](#).

11. (Opcional) Selecione Adicionar tag para marcar o sistema de arquivos.

Uma tag é um par de chave-valor que ajuda você a gerenciar, filtrar e pesquisar seus locais.

12. Escolha Criar local.

Usando o AWS CLI

1. Copie o seguinte comando create-location-efs:

```
aws datasync create-location-efs \
  --efs-filesystem-arn 'arn:aws:elasticfilesystem:region:account-id:file-
system/file-system-id' \
  --subdirectory /path/to/your/subdirectory \
  --ec2-config SecurityGroupArns='arn:aws:ec2:region:account-id:security-
group/security-group-id',SubnetArn='arn:aws:ec2:region:account-id:subnet/subnet-id' \
  --in-transit-encryption TLS1_2 \
  --access-point-arn 'arn:aws:elasticfilesystem:region:account-id:access-
point/access-point-id' \
  --file-system-access-role-arn 'arn:aws:iam::account-id:role/datasync-efs-
access-role'
```

2. Em --efs-filesystem-arn, especifique o nome do recurso da Amazon (ARN) do sistema de arquivos Amazon EFS que você está transferindo de ou para.
3. Em --subdirectory, especifique um caminho de montagem para o sistema de arquivos.

É aqui que DataSync lê ou grava dados (dependendo se esse é um local de origem ou destino) no seu sistema de arquivos.

Por padrão, DataSync usa o diretório raiz (ou [ponto de acesso](#), se você fornecer um --access-point-arn). Você também pode especificar subdiretórios usando barras (por exemplo), /path/to/directory

4. Para --ec2-config, faça o seguinte:

- Em `SecurityGroupArns`, especifique o ARN do grupo de segurança associado ao destino de montagem do sistema de arquivos. Você pode especificar mais de um grupo de segurança.

 Note

O grupo de segurança que você especificar deve permitir tráfego de entrada na porta NFS 2049. Para obter mais informações, consulte [Determinar a sub-rede e os grupos de segurança do destino de montagem](#).

- Para `SubnetArn`, especifique o ARN da sub-rede em que você deseja criar as [interfaces de rede DataSync](#) para gerenciar seu tráfego de transferência de dados.

A sub-rede deve estar localizada:

- Na mesma VPC que o sistema de arquivos.
- Na mesma zona de disponibilidade que pelo menos um destino de montagem.

 Note

Você não precisa especificar uma sub-rede que inclua um destino de montagem do sistema de arquivos.

5. Para `--in-transit-encryption`, especifique se você deseja usar DataSync a criptografia TLS (Transport Layer Security) ao transferir dados para ou do seu sistema de arquivos.

 Note

Você deve definir isso como `TLS1_2` para configurar um ponto de acesso, um perfil do IAM ou ambos com o local do Amazon EFS.

6. (Opcional) Para `--access-point-arn`, especifique o ARN de um ponto de acesso que DataSync pode ser usado para montar seu sistema de arquivos.

Para obter mais informações, consulte [Acesso a sistemas de arquivos restritos](#).

7. (Opcional) Para `--file-system-access-role-arn`, especifique o ARN de uma função do IAM que permite DataSync acessar seu sistema de arquivos.

Para obter informações sobre como criar essa função, consulte [Criação de uma função DataSync do IAM para acesso ao sistema de arquivos](#).

8. Execute o comando `create-location-efs`.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN do local que você criou. Por exemplo:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0b3017fc4ba4a2d8d"
}
```

Configurando transferências com o FSx Windows File Server

Para transferir dados para ou do seu sistema de arquivos Amazon FSx for Windows File Server, você deve criar um local AWS DataSync de transferência. DataSync pode usar esse local como origem ou destino para transferir dados.

Fornecendo DataSync acesso aos sistemas FSx de arquivos do Windows File Server

DataSync [se conecta ao seu sistema FSx de arquivos do Windows File Server com o protocolo Server Message Block \(SMB\) e o monta a partir da sua nuvem privada virtual \(VPC\) usando interfaces de rede.](#)

Note

VPCs que você usa com DataSync deve ter locação padrão. VPCs com locação dedicada não são suportadas.

Tópicos

- [Permissões obrigatórias](#)
- [Protocolos de autenticação necessários](#)
- [Namespaces do DFS](#)

Permissões obrigatórias

Você deve fornecer DataSync ao usuário os direitos necessários para montar e acessar seus FSx arquivos, pastas e metadados de arquivos do Windows File Server.

Recomendamos que esse usuário pertença a um grupo do Microsoft Active Directory para administrar o sistema de arquivos. As especificidades desse grupo dependem da configuração do Active Directory:

- Se você estiver usando AWS Directory Service for Microsoft Active Directory com FSx o Windows File Server, o usuário deverá ser membro do grupo FSx Administradores AWS Delegados.
- Se você estiver usando o Active Directory FSx autogerenciado com o Windows File Server, o usuário deverá ser membro de um dos dois grupos:
 - O grupo Administradores de domínio, que é o grupo padrão dos administradores delegados.
 - Um grupo personalizado de administradores delegados com direitos de usuário que permitem DataSync copiar permissões de propriedade de objetos e listas de controle de acesso do Windows (ACLs).

 Important

Você não pode alterar o grupo de administradores delegados depois que o sistema de arquivos foi implantado. Você deve reimplantar o sistema de arquivos ou restaurá-lo a partir de um backup para usar o grupo personalizado de administradores delegados com os seguintes direitos de usuário que DataSync precisam copiar metadados.

Direito do usuário	Descrição
Restaurar arquivos e diretórios (SE_RESTORE_NAME)	Permite copiar DataSync a propriedade do objeto, as permissões, os metadados do arquivo e as listas de acesso discricionário do NTFS (ACLs). Esse direito de usuário geralmente é concedido aos membros dos grupos Administradores de domínio e Operadores de backup (ambos grupos padrão do Active Directory).
Gerenciar logs de auditoria e segurança (SE_SECURITY_NAME)	Permite DataSync copiar listas de controle de acesso do sistema NTFS (SACLs).

Direito do usuário	Descrição
	Esse direito de usuário geralmente é concedido aos membros do grupo Administradores de domínio.

- Se você quiser copiar o Windows ACLs e estiver transferindo entre um servidor de arquivos SMB e FSx para o sistema de arquivos Windows File Server ou entre FSx sistemas de arquivos Windows File Server, os usuários fornecidos DataSync devem pertencer ao mesmo domínio do Active Directory ou ter uma relação de confiança do Active Directory entre seus domínios.

Warning

Seu FSx usuário do sistema de arquivos do Windows File Server deve ter permissões de controle total em todas as pastas do seu sistema de arquivos. Não altere as permissões de NTFS ACL para esse usuário em suas pastas. Se você fizer isso, DataSync poderá alterar as permissões do sistema de arquivos de uma forma que torne seu compartilhamento de arquivos inacessível e impeça que os backups do sistema de arquivos sejam utilizáveis. Para obter mais informações sobre o acesso em nível de arquivo e pasta, consulte o [Guia do usuário do Amazon FSx para Windows File Server](#).

Protocolos de autenticação necessários

Seu servidor de arquivos FSx para Windows deve usar a autenticação NTLM DataSync para acessá-lo. DataSync não consegue acessar um servidor de arquivos que usa a autenticação Kerberos.

Namespaces do DFS

DataSync não oferece suporte a namespaces do Microsoft Distributed File System (DFS). Em vez disso, recomendamos especificar um servidor ou compartilhamento de arquivos subjacente ao criar sua DataSync localização.

Para obter mais informações, consulte [Agrupando vários sistemas de arquivos com namespaces DFS no Guia do usuário](#) do Amazon FSx para Windows File Server.

Criando seu local de transferência FSx para o Windows File Server

Antes de começar, verifique se você tem um servidor FSx de arquivos do Windows existente no seu Região da AWS. Para obter mais informações, consulte [Introdução à Amazon FSx](#) no Guia do usuário do Amazon FSx para Windows File Server.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Para Tipo de localização, escolha Amazon FSx.
4. Para sistema de FSx arquivos, escolha o FSx sistema de arquivos do Windows File Server que você deseja usar como local.
5. Em Nome do compartilhamento, insira um caminho de montagem FSx para o Windows File Server usando barras.

Isso especifica o caminho onde DataSync lê ou grava dados (dependendo se esse é um local de origem ou destino).

Você também pode incluir subdiretórios (por exemplo, `/path/to/directory`).

6. Para grupos de segurança, escolha até cinco grupos de EC2 segurança da Amazon que fornecem acesso à sub-rede preferencial do seu sistema de arquivos.

Os grupos de segurança que você escolher devem ser capazes de se comunicar com os grupos de segurança do sistema de arquivos. Para obter informações sobre a configuração de grupos de segurança para acesso ao sistema de arquivos, consulte o [Guia do usuário do Amazon FSx para Windows File Server](#).

Note

Se você escolher um grupo de segurança que não permite conexões de dentro de si mesmo, siga um destes procedimentos:

- Configure o grupo de segurança para permitir que ele se comunique dentro de si próprio.

- Escolha outro grupo de segurança diferente que possa se comunicar com o grupo de segurança do destino de montagem.

7. Em Usuário, insira o nome de um usuário que pode acessar o seu FSx para o Windows File Server.

Para obter mais informações, consulte [Permissões obrigatórias](#).

8. Para Senha, insira a senha do nome de usuário.
9. (Opcional) Em Domínio, insira o nome do domínio do Windows ao qual seu sistema FSx de arquivos do Windows File Server pertence.

Se você tiver vários domínios do Active Directory em seu ambiente, definir essa configuração garante que ele DataSync se conecte ao sistema de arquivos correto.

10. (Opcional) Insira valores para os campos Chave e Valor para marcar o FSx Windows File Server.

As tags ajudam você a gerenciar, filtrar e pesquisar seus AWS recursos. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

11. Escolha Criar local.

Usando o AWS CLI

Para criar um local FSx para o Windows File Server usando o AWS CLI

- Use o comando a seguir para criar uma FSx localização na Amazon.

```
aws datasync create-location-fsx-windows \
  --fsx-filesystem-arn arn:aws:fsx:region:account-id:file-system/filesystem-id \
  --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id \
  --user smb-user --password password
```

No comando `create-location-fsx-windows`, faça o seguinte:

- `fsx-filesystem-arn`: especifique o nome do recurso da Amazon (ARN) do sistema de arquivos para o qual ou do qual deseja transferir.
- `security-group-arns`— Especifique até cinco grupos ARNs de EC2 segurança da Amazon que fornecem acesso à sub-rede preferencial do seu sistema de arquivos.

Os grupos de segurança que você especificar devem ser capazes de se comunicar com os grupos de segurança do seu sistema de arquivos. Para obter informações sobre a configuração de grupos de segurança para acesso ao sistema de arquivos, consulte o [Guia do usuário do Amazon FSx para Windows File Server](#).

 Note

Se você escolher um grupo de segurança que não permite conexões de dentro de si mesmo, siga um destes procedimentos:

- Configure o grupo de segurança para permitir que ele se comunique dentro de si próprio.
 - Escolha outro grupo de segurança diferente que possa se comunicar com o grupo de segurança do destino de montagem.
- A Região da AWS — A região que você especifica é aquela em que seu sistema de FSx arquivos da Amazon de destino está localizado.

O comando anterior retorna um ARN do local semelhante ao exibido a seguir.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07db7abfc326c50fb"
}
```

Configurando DataSync transferências com FSx for Lustre

Para transferir dados para ou do seu sistema de arquivos Amazon FSx for Lustre, você deve criar um local de AWS DataSync transferência. DataSync pode usar esse local como origem ou destino para transferir dados.

Fornecendo DataSync acesso aos FSx sistemas de arquivos Lustre

DataSync acessa seu sistema de arquivos FSx for Lustre usando o cliente Lustre. DataSync requer acesso a todos os dados em seu sistema de arquivos FSx for Lustre. Para ter esse nível de acesso, DataSync monta seu sistema de arquivos como usuário raiz usando um ID de usuário (UID) e um ID de grupo (GID) do. 0

DataSync monta seu sistema de arquivos a partir da sua nuvem privada virtual (VPC) [usando](#) interfaces de rede. DataSync gerencia totalmente a criação, o uso e a exclusão dessas interfaces de rede em seu nome.

 Note

VPCs que você usa com DataSync deve ter localização padrão. VPCs com localização dedicada não são suportadas.

Criando seu local FSx de transferência para Lustre

Para criar o local de transferência, você precisa de um sistema de arquivos existente FSx para o Lustre. Para obter mais informações, consulte [Introdução ao Amazon FSx for Lustre no Guia](#) do usuário do Amazon FSx for Lustre.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Para Tipo de localização, escolha Amazon FSx.

Você configurará esse local como origem ou destino posteriormente.

4. Para sistema de FSx arquivos, escolha o FSx sistema de arquivos Lustre que você deseja usar como local.
5. Em Mount path, insira o caminho de montagem do seu sistema de arquivos FSx for Lustre.

O caminho pode incluir um subdiretório. Quando o local é usado como fonte, DataSync lê os dados do caminho de montagem. Quando o local é usado como destino, DataSync grava todos os dados no caminho de montagem. Se um subdiretório não for fornecido, DataSync usa o diretório raiz (/).

6. Para grupos de segurança, escolha até cinco grupos de segurança que fornecem acesso ao seu sistema de arquivos FSx for Lustre.

Os grupos de segurança devem conseguir acessar as portas do sistema de arquivos. O sistema de arquivos também deve permitir o acesso a partir dos grupos de segurança.

Para obter mais informações sobre grupos de segurança, consulte [Controle de acesso ao sistema de arquivos com Amazon VPC no Guia](#) do usuário do Amazon FSx for Lustre.

7. (Opcional) Insira valores nos campos Chave e Valor para marcar o FSx sistema de arquivos do Lustre.

As tags ajudam você a gerenciar, filtrar e pesquisar seus AWS recursos. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

8. Escolha Criar local.

Usando o AWS CLI

Para criar um local FSx para o Lustre usando o AWS CLI

- Use o comando a seguir para criar um local FSx para o Lustre.

```
aws datasync create-location-fsx-lustre \
  --fsx-filesystem-arn arn:aws:fsx:region:account-id:file-system:filesystem-id \
  --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id
```

Os parâmetros a seguir são obrigatórios no comandos create-location-fsx-lustre.

- fsx-filesystem-arn: o nome do recurso da Amazon (ARN) totalmente qualificado do sistema de arquivos no qual deseja ler ou gravar.
- security-group-arns— O ARN de um grupo de EC2 segurança da Amazon a ser aplicado às [interfaces de rede da sub-rede](#) preferencial do sistema de arquivos.

O comando anterior retorna um ARN do local semelhante ao seguir.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07sb7abfc326c50fb"
}
```

Configurando DataSync transferências com a Amazon FSx para OpenZFS

Para transferir dados para ou do seu sistema de arquivos Amazon FSx for OpenZFS, você deve criar um local de AWS DataSync transferência. DataSync pode usar esse local como origem ou destino para transferir dados.

Fornecendo DataSync acesso a FSx sistemas de arquivos OpenZFS

DataSync [monta seu sistema de arquivos FSx para OpenZFS a partir de sua nuvem privada virtual \(VPC\) usando interfaces de rede](#). DataSync gerencia totalmente a criação, o uso e a exclusão dessas interfaces de rede em seu nome.

Note

VPCs que você usa com DataSync deve ter locação padrão. VPCs com locação dedicada não são suportadas.

Configurando a autorização do FSx sistema de arquivos OpenZFS

DataSync acessa seu sistema de arquivos FSx para OpenZFS como um cliente NFS, montando o sistema de arquivos como um usuário root com um ID de usuário (UID) e ID de grupo (GID) de 0.

DataSync Para copiar todos os metadados do arquivo, você deve definir as configurações de exportação de NFS nos volumes do sistema de arquivos usando `no_root_squash`. No entanto, você pode limitar esse nível de acesso somente a uma DataSync tarefa específica.

Para obter mais informações, consulte [Propriedades de volume](#) no Guia do usuário do Amazon FSx for OpenZFS.

Configurando exportações NFS específicas para DataSync (recomendado)

Você pode configurar uma exportação NFS específica para cada volume acessado somente pela sua DataSync tarefa. Faça isso para o volume ancestral mais recente do caminho de montagem que você especificou ao criar sua localização FSx para OpenZFS.

Para configurar uma exportação NFS específica para DataSync

1. Crie sua [DataSync tarefa](#).

Isso cria as interfaces de rede da tarefa que você especifica nas configurações de exportação do NFS.

2. Localize os endereços IP privados das interfaces de rede da tarefa usando o EC2 console da Amazon ou AWS CLI.
3. FSx Para o volume do sistema de arquivos OpenZFS, defina as seguintes configurações de exportação NFS para cada uma das interfaces de rede da tarefa:
 - Endereço do cliente: insira o endereço IP privado da interface de rede (por exemplo, **10.24.34.0**).
 - Opções de NFS: insira `rw,no_root_squash`.

Configurar exportações do NFS para todos os clientes

Você pode especificar uma exportação do NFS que permita acesso à raiz a todos os clientes.

Configurar uma exportação NFS para todos os clientes

- FSx Para o volume do sistema de arquivos OpenZFS, defina as seguintes configurações de exportação de NFS:
 - Endereço do cliente: insira `*`.
 - Opções de NFS: insira `rw,no_root_squash`.

Criando seu local FSx de transferência para o OpenZFS

Para criar o local, você precisa de um sistema de arquivos existente FSx para OpenZFS. Se você não tiver um, consulte [Introdução ao Amazon FSx for OpenZFS](#) no Guia do usuário do Amazon FSx for OpenZFS.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação à esquerda, escolha Locais e, em seguida, Criar local.
3. Para Tipo de localização, escolha Amazon FSx.

Você configurará esse local como origem ou destino posteriormente.

4. Para sistema de FSx arquivos, escolha o FSx sistema de arquivos OpenZFS que você deseja usar como local.
5. Em Mount path, insira o caminho de montagem do seu sistema de arquivos FSx para OpenZFS.

O caminho deve começar com `/fsx` e pode ser qualquer caminho de diretório existente no sistema de arquivos. Quando o local é usado como fonte, DataSync lê os dados do caminho de montagem. Quando o local é usado como destino, DataSync grava todos os dados no caminho de montagem. Se um subdiretório não for fornecido, DataSync usa o diretório do volume raiz (por exemplo, `/fsx`).

6. Para grupos de segurança, escolha até cinco grupos de segurança que fornecem acesso de rede ao seu sistema de arquivos FSx para OpenZFS.

Os grupos de segurança devem fornecer acesso às portas de rede que são usadas pelo sistema de arquivos FSx for OpenZFS. O sistema de arquivos deve permitir o acesso à rede dos grupos de segurança.

Para obter mais informações sobre grupos de segurança, consulte [Controle de acesso ao sistema de arquivos com o Amazon VPC no Guia](#) do usuário do Amazon FSx for OpenZFS.

7. (Opcional) Expanda Configurações adicionais e, para a versão NFS, escolha a versão NFS que DataSync usa para acessar seu sistema de arquivos.

Por padrão, DataSync usa a versão 4.1 do NFS.

8. (Opcional) Insira valores para os campos Chave e Valor para marcar o sistema FSx de arquivos OpenZFS.

Tags ajudam a gerenciar, filtrar e procurar seu local. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

9. Escolha Criar local.

Usando o AWS CLI

Para criar um local FSx para o OpenZFS usando o AWS CLI

1. Copie o seguinte comando `create-location-fsx-open-zfs`:

```
aws datasync create-location-fsx-open-zfs \
  --fsx-filesystem-arn arn:aws:fsx:region:account-id:file-system/filesystem-id \
  --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id \
```

```
--protocol NFS={}
```

2. Especifique os parâmetros exigidos a seguir no comando:

- Para `fsx-filesystem-arn`, especifique o Nome do recursos da Amazon (ARN) totalmente qualificado do sistema de arquivos de localização. Isso inclui o Região da AWS local em que seu sistema de arquivos reside Conta da AWS, seu e o ID do sistema de arquivos.
- Para `security-group-arns`, especifique o ARN do grupo de EC2 segurança da Amazon que fornece acesso às [interfaces de rede de sua sub-rede](#) FSx preferencial do sistema de arquivos OpenZFS. Isso inclui o Região da AWS local em que sua EC2 instância da Amazon reside Conta da AWS, seu e o ID do grupo de segurança.

Para obter mais informações sobre grupos de segurança, consulte [Controle de acesso ao sistema de arquivos com Amazon VPC no Guia](#) do usuário do Amazon FSx for OpenZFS.

- Para `protocol`, especifique o protocolo DataSync usado para acessar seu sistema de arquivos. (DataSync atualmente suporta somente NFS.)

3. Execute o comando. Você recebe uma resposta que mostra o local que você acabou de criar.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
abcdef01234567890"
}
```

Configurando transferências com a Amazon FSx para ONTAP NetApp

Para transferir dados para ou do seu sistema de arquivos Amazon FSx for NetApp ONTAP, você deve criar um local de AWS DataSync transferência. DataSync pode usar esse local como origem ou destino para transferir dados.

Fornecendo DataSync acesso aos FSx sistemas de arquivos ONTAP

Para acessar um sistema de arquivos FSx for ONTAP, DataSync monta uma máquina virtual de armazenamento (SVM) em seu sistema de arquivos usando [interfaces de rede](#) em sua nuvem privada virtual (VPC). DataSync cria essas interfaces de rede na sub-rede preferencial do seu sistema de arquivos somente quando você cria uma tarefa que inclui sua localização FSx para ONTAP.

 Note

VPCs que você usa com DataSync deve ter localização padrão. VPCs com localização dedicada não são suportadas.

DataSync pode se conectar a um FSx SVM do sistema de arquivos ONTAP e copiar dados usando o protocolo Network File System (NFS) ou Server Message Block (SMB).

Tópicos

- [Usar o protocolo NFS](#)
- [Usar o protocolo SMB](#)
- [Protocolos incompatíveis](#)
- [Escolhendo o protocolo certo](#)
- [Acessando SnapLock volumes](#)

Usar o protocolo NFS

Com o protocolo NFS, DataSync usa o mecanismo de AUTH_SYS segurança com um ID de usuário (UID) e ID de grupo (GID) 0 para se autenticar com sua SVM.

 Note

DataSync atualmente só oferece suporte ao NFS versão 3 com quatro localizações FSx ONTAP.

Usar o protocolo SMB

Com o protocolo SMB, DataSync usa as credenciais que você fornece para se autenticar com seu SVM.

Versões compatíveis do SMB

Por padrão, escolhe DataSync automaticamente uma versão do protocolo SMB com base na negociação com seu servidor de arquivos SMB. Você também pode configurar DataSync para usar uma versão específica, mas recomendamos fazer isso somente se DataSync tiver

problemas para negociar com o servidor de arquivos SMB automaticamente. Por motivos de segurança, recomendamos usar a versão 3.0.2 ou posterior do SMB.

Consulte a tabela a seguir para obter uma lista de opções no DataSync console e na API para configurar uma versão SMB com sua localização FSx para ONTAP:

Opção do console	Opção de API	Descrição
Automatico	AUTOMATIC	DataSync e o servidor de arquivos SMB negociam a versão mais alta do SMB que eles suportam mutuamente entre 2.1 e 3.1.1. Essa é a opção recomendada e também a padrão. Se, em vez disso, você escolher uma versão específica que seu servidor de arquivos não suporta, você pode receber um erro <code>Operation Not Supported</code> .
SMB 3.0.2	SMB3	Restringe a negociação do protocolo somente à versão 3.0.2 do SMB.
SMB 2.1	SMB2	Restringe a negociação do protocolo somente à versão 2.1 do SMB.
SMB 2.0	SMB2_0	Restringe a negociação do protocolo somente à versão 2.0 do SMB.

Permissões obrigatórias

Você deve fornecer a DataSync um usuário local em seu SVM ou a um usuário de domínio em seu Microsoft Active Directory os direitos necessários para montar e acessar seus arquivos, pastas e metadados de arquivos.

Se você fornecer um usuário no Active Directory, observe o seguinte:

- Se você estiver usando AWS Directory Service for Microsoft Active Directory, o usuário deverá ser membro do grupo `FSxAdministradores AWS Delegados`.
- Se você estiver usando um Microsoft Active Directory autogerenciado, o usuário deverá ser membro de um de dois grupos:

- O grupo Administradores de domínio, que é o grupo padrão dos administradores delegados.
- Um grupo personalizado de administradores delegados com direitos de usuário que permitem DataSync copiar permissões de propriedade de objetos e listas de controle de acesso do Windows (ACLs).

 Important

Você não pode alterar o grupo de administradores delegados depois que o sistema de arquivos foi implantado. Você deve reimplantar o sistema de arquivos ou restaurá-lo a partir de um backup para usar o grupo personalizado de administradores delegados com os seguintes direitos de usuário que DataSync precisam copiar metadados.

Direito do usuário	Descrição
Atuar como parte do sistema operacional (SE_TCB_NAME)	Permite copiar DataSync a propriedade do objeto, as permissões, os metadados do arquivo e as listas de acesso discricionário do NTFS (DACLs). Esse direito de usuário geralmente é concedido aos membros dos grupos Administradores de domínio e Operadores de backup (ambos grupos padrão do Active Directory).
Gerenciar logs de auditoria e segurança (SE_SECURITY_NAME)	Permite DataSync copiar listas de controle de acesso do sistema NTFS (SACLs). Esse direito de usuário geralmente é concedido aos membros do grupo Administradores de domínio.

- Se você quiser copiar o Windows ACLs e estiver fazendo transferências FSx para sistemas de arquivos ONTAP usando SMB (ou outros tipos de sistemas de arquivos usando SMB), os

usuários fornecidos DataSync devem pertencer ao mesmo domínio do Active Directory ou ter uma relação de confiança do Active Directory entre seus domínios.

Protocolos de autenticação necessários

DataSync Para acessar seu compartilhamento SMB, seu FSx sistema de arquivos do ONTAP deve usar a autenticação NTLM. DataSync não consegue acessar os sistemas FSx de arquivos ONTAP que usam a autenticação Kerberos.

Namespaces do DFS

DataSync não oferece suporte a namespaces do Microsoft Distributed File System (DFS). Em vez disso, recomendamos especificar um servidor ou compartilhamento de arquivos subjacente ao criar sua DataSync localização.

Protocolos incompatíveis

DataSync não consegue acessar os sistemas FSx de arquivos ONTAP usando o protocolo iSCSI (Internet Small Computer Systems Interface).

Escolhendo o protocolo certo

Para preservar os metadados do arquivo nas FSx migrações do ONTAP, configure seus locais de DataSync origem e destino para usar o mesmo protocolo. Entre os protocolos compatíveis, o SMB preserva os metadados com a mais alta fidelidade (consulte [Entendendo como DataSync manipula metadados de arquivos e objetos](#) para obter detalhes).

Ao migrar de um servidor Unix (Linux) ou compartilhamento de armazenamento conectado à rede (NAS) que atenda aos usuários por meio do NFS, faça o seguinte:

1. [Crie um local NFS](#) para o servidor Unix (Linux) ou compartilhamento NAS. (Esse será seu local de origem.)
2. Configure o volume ONTAP FSx para o qual você está transferindo dados com o estilo de segurança [Unix](#).
3. Crie um local para o seu FSx sistema de arquivos do ONTAP que esteja configurado para NFS. (Esse será seu local de destino.)

Ao migrar de um servidor Windows ou compartilhamento NAS que atende usuários por meio de SMB, faça o seguinte:

1. [Crie um local SMB](#) para o servidor Windows ou compartilhamento NAS. (Esse será seu local de origem.)
2. Configure o volume ONTAP FSx para o qual você está transferindo dados com o estilo de segurança [NTFS](#).
3. Crie um local para o seu FSx sistema de arquivos do ONTAP que esteja configurado para SMB. (Esse será seu local de destino.)

Se o seu ambiente FSx for ONTAP usa vários protocolos, recomendamos trabalhar com um especialista em AWS armazenamento. Para saber mais sobre as melhores práticas para acesso multiprotocolo, consulte [Habilitando cargas de trabalho multiprotocolo com a Amazon FSx](#) para ONTAP. NetApp

Acessando SnapLock volumes

Se você estiver transferindo dados para um [SnapLock volume](#) em um sistema de arquivos FSx para ONTAP, certifique-se de que as SnapLock configurações Confirmação automática e Modo de acréscimo de volume estejam desativadas no volume durante a transferência. É possível reabilitar essas configurações quando terminar de transferir dados.

Criando seu local FSx de transferência para o ONTAP

Para criar o local, você precisa de um sistema de arquivos existente FSx para ONTAP. Se você não tiver um, consulte [Introdução ao Amazon FSx for NetApp ONTAP](#) no Guia do usuário do Amazon FSx for NetApp ONTAP.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Para Tipo de localização, escolha Amazon FSx.

Você configurará esse local como origem ou destino posteriormente.

4. Para sistema de FSx arquivos, escolha o FSx sistema de arquivos ONTAP que você deseja usar como local.
5. Em Máquina virtual de armazenamento, escolha uma máquina virtual de armazenamento (SVM) no sistema de arquivos para o qual e do qual você copia dados.

6. Em Montar caminho, especifique um caminho para o compartilhamento de arquivos no SVM no qual que você copiará os dados.

Você pode especificar um caminho de união (também conhecido como ponto de montagem), caminho qtree (para compartilhamentos de arquivos NFS) ou nome de compartilhamento (para compartilhamentos de arquivos SMB). Por exemplo, seu caminho de montagem pode ser /vol1, /vol1/tree1 ou /share1.

 Tip

Não especifique um caminho no volume raiz do SVM. Para obter mais informações, consulte [Gerenciamento FSx de máquinas virtuais de armazenamento ONTAP no Guia do usuário do Amazon FSx for NetApp ONTAP](#).

7. Para grupos de segurança, escolha até cinco grupos de EC2 segurança da Amazon que fornecem acesso à sub-rede preferencial do seu sistema de arquivos.

Os grupos de segurança devem permitir tráfego de saída nas seguintes portas (dependendo do protocolo em uso):

- NFS: portas TCP 111, 635 e 2049
- SMB: porta TCP 445

Os grupos de segurança do seu sistema de arquivos também devem permitir tráfego de entrada na mesma porta.

8. Em Protocolo, escolha o protocolo de transferência de dados DataSync usado para acessar o SVM do seu sistema de arquivos.

Para obter mais informações, consulte [Escolhendo o protocolo certo](#).

NFS

DataSync usa o NFS versão 3.

SMB

Configure uma versão do SMB, o nome de usuário, a senha e o nome de domínio do Active Directory (se necessário) para acessar a SVM.

- (Opcional) Expanda Configurações adicionais e escolha uma versão SMB DataSync para usar ao acessar seu SVM.

Por padrão, escolha DataSync automaticamente uma versão com base na negociação com o servidor de arquivos SMB. Para obter mais informações, consulte [Usar o protocolo SMB](#).

- Em Usuário, especifique um nome de usuário que possa montar e acessar os arquivos, as pastas e os metadados que você deseja transferir na SVM.

Para obter mais informações, consulte [Usar o protocolo SMB](#).

- Em Senha, insira a senha do usuário que você especificou e que pode acessar a SVM.
- (Opcional) Em nome de domínio do Active Directory, insira o nome de domínio totalmente qualificado (FQDN) do Active Directory ao qual a SVM pertence.

Se você tiver vários domínios em seu ambiente, definir essa configuração garante que ele se DataSync conecte ao SVM correto.

9. (Opcional) Insira valores para os campos Chave e Valor para marcar o FSx sistema de arquivos ONTAP.

As tags ajudam você a gerenciar, filtrar e pesquisar seus AWS recursos. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

10. Escolha Criar local.

Usando o AWS CLI

Para criar um local FSx para ONTAP usando o AWS CLI

1. Copie o seguinte comando `create-location-fsx-ontap`:

```
aws datasync create-location-fsx-ontap \
  --storage-virtual-machine-arn arn:aws:fsx:region:account-id:storage-virtual-
machine/fs-file-system-id \
  --security-group-arns arn:aws:ec2:region:account-id:security-group/group-id \
  --protocol data-transfer-protocol={}
```

2. Especifique os parâmetros exigidos a seguir no comando:

- Para `storage-virtual-machine-arn`, especifique o Nome do recursos da Amazon (ARN) de uma máquina virtual de armazenamento (SVM) no seu sistema de arquivos para o qual ou do qual você copie dados.

Esse ARN inclui o Região da AWS local em que seu sistema de arquivos reside Conta da AWS, seu e o sistema de arquivos e a SVM. IDs

- Para `security-group-arns`, especifique os grupos ARNs de EC2 segurança da Amazon que fornecem acesso às [interfaces de rede](#) da sub-rede preferencial do seu sistema de arquivos.

Isso inclui Região da AWS onde sua EC2 instância da Amazon reside Conta da AWS, você e seu grupo IDs de segurança. Você pode especificar até cinco grupos de segurança ARNs.

Para obter mais informações sobre grupos de segurança, consulte [Controle de acesso ao sistema de arquivos com Amazon VPC no Guia](#) do usuário do Amazon FSx for NetApp ONTAP.

- Para `protocol`, configure o protocolo DataSync usado para acessar o SVM do seu sistema de arquivos.

- Para NFS, você pode usar a configuração padrão:

```
--protocol NFS={}
```

- Para SMB, você deve especificar um nome de usuário e uma senha que possam acessar a SVM:

```
--protocol SMB={User=smb-user, Password=smb-password}
```

3. Execute o comando .

Você recebe uma resposta que mostra o local que você acabou de criar.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
abcdef01234567890"
}
```

Transferindo de ou para outro armazenamento em nuvem com AWS DataSync

Com AWS DataSync, você pode transferir dados entre alguns outros provedores de nuvem e serviços AWS de armazenamento. Para obter mais informações, consulte [Com onde posso transferir meus dados DataSync?](#)

Tópicos

- [Planejando transferências de ou para sistemas de armazenamento em nuvem de terceiros](#)
- [Configurando AWS DataSync transferências com o Google Cloud Storage](#)
- [Configurar transferências com o Microsoft Azure Blob Storage](#)
- [Configurando AWS DataSync transferências com Microsoft Azure Files Ações de pequenas e médias empresas](#)
- [Configurar transferências de com outro armazenamento de objetos na nuvem](#)

Planejando transferências de ou para sistemas de armazenamento em nuvem de terceiros

Ao planejar transferências de dados entre nuvens, considere o seguinte:

- Usando um agente: um agente só precisa acessar o armazenamento em outras nuvens ao usar tarefas do modo Básico. [As tarefas do modo aprimorado](#) não exigem um agente. Se você decidir usar um agente, poderá implantá-lo como uma [EC2instância da Amazon](#) ao transferir do armazenamento de objetos compatível com S3 de um provedor de nuvem ou como uma máquina virtual do Google Compute Engine ou Azure para transferências desses serviços de armazenamento específicos, respectivamente. Ao transferir de sistemas de arquivos no Google e no Azure, recomendamos implantar o agente como uma VM do Google ou do Azure para que o agente fique o mais próximo possível do sistema de arquivos. Além disso, DataSync comprime os dados do agente para AWS, o que pode ajudar a reduzir os custos de saída. DataSync fornece uma lista de [locais de nuvem validados](#) que fornecem a compatibilidade necessária com a [API Amazon S3](#).
- O endpoint de armazenamento de objetos da outra nuvem: o endpoint de armazenamento de um provedor de nuvem terceirizado geralmente é específico da região ou da conta. O endpoint regional é usado como servidor no local de armazenamento de DataSync objetos, junto com um nome de bucket especificado.

- Classes de armazenamento dos objetos de origem: como o Amazon S3, alguns provedores de nuvem oferecem suporte a um nível de arquivamento que requer uma restauração antes de poder acessar os objetos arquivados. Por exemplo, objetos na camada de arquivamento Azure Blob devem ser recuperados para acesso padrão antes de uma transferência de dados. Os objetos na camada de arquivamento do Google Cloud Storage podem ser acessados imediatamente e não precisam ser restaurados, mas há custos de recuperação associados ao acesso direto à camada de arquivamento. Revise a documentação da classe de armazenamento em nuvem para determinar os requisitos de acesso e as taxas de recuperação antes de iniciar a transferência de dados. Para obter mais informações sobre como restaurar objetos arquivados no Amazon S3, [consulte Restauração de um objeto arquivado](#) no Guia do usuário do Amazon Simple Storage Service.
- Acesso ao armazenamento de objetos: a transferência de dados entre provedores de nuvem terceirizados requer acesso ao armazenamento de objetos da outra nuvem na forma de chaves de autenticação. Por exemplo, para fornecer acesso ao Google Cloud Storage, você configura um local de armazenamento de DataSync objetos que se conecta à [API XML do Google Cloud Storage](#) e se autentica usando uma [chave de código de autenticação de mensagem \(HMAC\) baseada em hash](#) para sua conta de serviço. [Para o armazenamento do Azure Blob, você configura um DataSync local dedicado do Azure Blob que se autentica usando tokens SAS.](#) DataSync usa AWS Secrets Manager para armazenar com segurança suas credenciais de armazenamento de objetos. Para obter mais informações, consulte [Protegendo as credenciais do local de armazenamento](#).
- Suporte para tags de objetos:
 - Diferentemente do Amazon S3, nem todos os provedores de nuvem oferecem suporte a tags de [objetos](#). DataSync as tarefas podem falhar ao tentar ler tags do local de origem se o provedor de nuvem não oferecer suporte a tags de objetos por meio da API do Amazon S3 ou se as credenciais fornecidas forem insuficientes para recuperar as tags. DataSync fornece uma opção de tarefa para desativar a [leitura e a cópia de tags de objeto](#) durante uma transferência se as tags de objeto não forem suportadas ou se você não quiser reter as tags. Revise a documentação do seu provedor de nuvem para determinar se as tags de objeto são suportadas e verifique as configurações da tag de objeto da sua tarefa de transferência antes de iniciar a transferência.
 - Você pode usar a API do Amazon S3 para verificar se um provedor de nuvem retornará uma `get-object-tagging` solicitação. Para obter mais informações, consulte [get-object-tagging](#) na Referência de comandos da AWS CLI .

Um provedor de nuvem que ofereça suporte a tags de objetos retornará uma resposta semelhante ao exemplo a seguir:

```
aws s3api get-object-tagging --bucket BUCKET_NAME --endpoint-url=https://
BUCKET_ENDPOINT --key prefix/file1

{
    "TagSet": []
}
```

Um provedor de nuvem que não oferece suporte `get-object-tagging` retornará a seguinte mensagem:

```
aws s3api get-object-tagging --bucket BUCKET_NAME --endpoint-url=https://
BUCKET_ENDPOINT --key prefix/file1

An error occurred (OperationNotSupported) when calling the GetObjectTagging
operation: The operation is not supported for this resource
```

- Custos associados às solicitações e à saída de dados: a transferência de dados do armazenamento de objetos na nuvem tem [custos de solicitação e saída](#) associados à leitura e à transferência de dados para fora. As cobranças de solicitação variam entre os provedores de nuvem e entre as classes de armazenamento, quando aplicável. Consulte a documentação do seu provedor de nuvem sobre os custos específicos das solicitações relacionadas à classe de armazenamento que você planeja ler. [Para obter uma visão geral das cobranças de solicitações que DataSync envolvem as transferências de dados, consulte Avaliação dos custos de solicitação do S3 ao usar DataSync e AWS DataSync preços.](#) A transferência de dados de provedores de nuvem específicos resulta em cobranças de saída. Os custos de transferência de dados variam entre os provedores de nuvem e também dependem da região em que os dados são armazenados.
- Taxas de solicitação de armazenamento de objetos: os provedores de nuvem têm várias características de desempenho e taxa de solicitação para suas plataformas de armazenamento de objetos. Analise as taxas de solicitação de seu outro provedor de nuvem e determine onde os limites de solicitação são aplicados. Planeje com antecedência transferências altamente paralelizadas que consistem em vários agentes, onde possam ser necessários particionamentos específicos ou aumentos de desempenho.

O Amazon S3 documentou taxas de solicitação com base nas quais você pode criar sua solução. As taxas de solicitação do Amazon S3 são por prefixo particionado e são escaláveis em vários prefixos. Para obter mais informações, consulte [Padrões de design de melhores práticas: otimização do desempenho do Amazon S3](#) no Guia do usuário do Amazon Simple Storage Service.

Configurando AWS DataSync transferências com o Google Cloud Storage

O tutorial a seguir mostra como você pode usar AWS DataSync para migrar objetos de um bucket do Google Cloud Storage (GCS) para um bucket do Amazon S3.

Visão geral

DataSync usa a [API XML do Google Cloud Storage](#) para transferências de dados. Essa API fornece uma interface compatível com o Amazon S3 para leitura e gravação de dados com buckets do GCS.

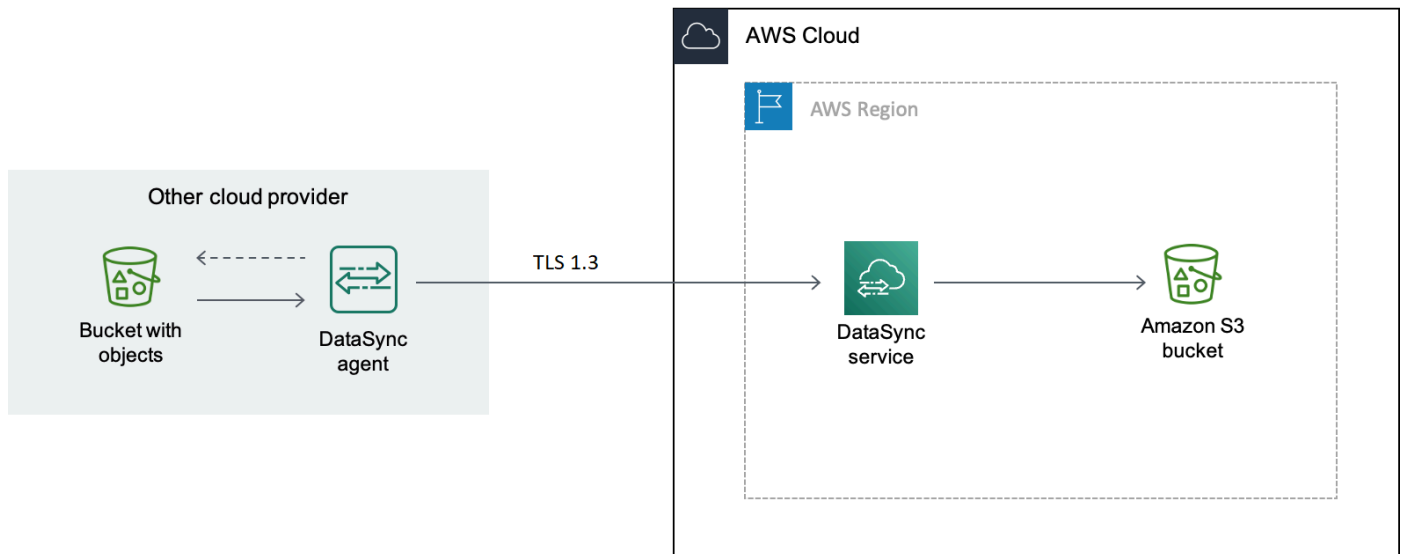
DataSync suporta transferências entre o GCS e os serviços AWS de armazenamento. Ao copiar entre o GCS e o Amazon EFS ou a Amazon FSx, é necessário um agente e sua tarefa deve usar o modo Básico. Ao copiar entre o GCS e o Amazon S3, um agente só é necessário ao usar o modo Básico.

Se você usar um agente para sua transferência, poderá implantar o agente no Google Cloud ou na sua Amazon VPC.

Agent in Google Cloud

1. Você implanta um DataSync agente em seu ambiente do Google Cloud.
2. O agente lê seu bucket do Google Cloud Storage usando uma chave de código de autenticação de mensagens por hash (HMAC).
3. Os objetos do seu bucket do Google Cloud Storage são transferidos com segurança por meio do TLS 1.3 para o Nuvem AWS usando um endpoint público.
4. O DataSync serviço grava os dados no seu bucket do S3.

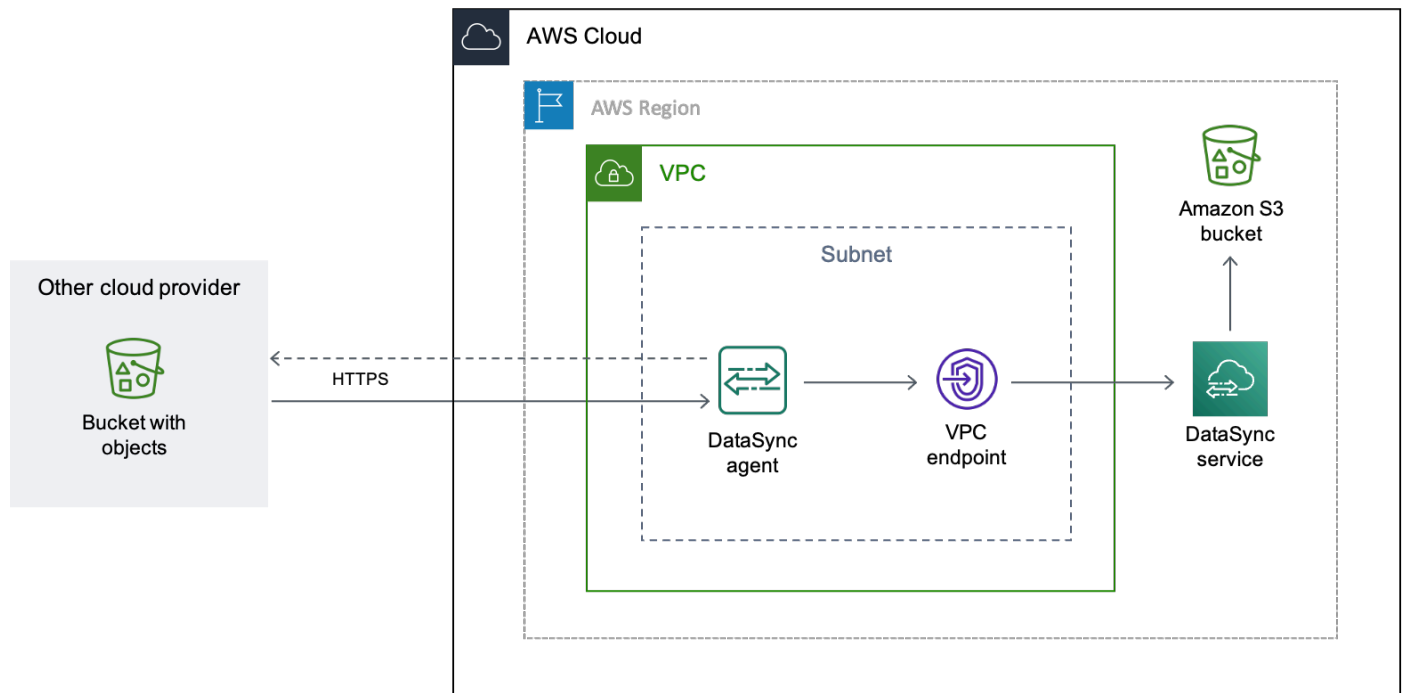
O diagrama a seguir ilustra a transferência.



Agent in your VPC

1. Você implanta um DataSync agente em uma nuvem privada virtual (VPC) em seu AWS ambiente.
2. O agente lê seu bucket do Google Cloud Storage usando uma chave de código de autenticação de mensagens por hash (HMAC).
3. Os objetos do seu bucket do Google Cloud Storage são transferidos com segurança por meio do TLS 1.3 para o Nuvem AWS usando um VPC endpoint privado.
4. O DataSync serviço grava os dados no seu bucket do S3.

O diagrama a seguir ilustra a transferência.



Custos

As taxas associadas a essa migração podem incluir:

- Executar uma instância de máquina virtual (VM) do Google [Compute Engine](#) (se você implantar seu DataSync agente no Google Cloud)
- Executando uma EC2 instância [da Amazon](#) (se você implantar seu DataSync agente em uma VPC interna) AWS
- Transferir os dados usando [DataSync](#), incluindo cobranças de solicitação relacionadas ao [Google Cloud Storage](#) e ao [Amazon S3](#) (se o S3 for um dos seus locais de transferência)
- Transferindo dados para fora do [Google Cloud Storage](#)
- Armazenando dados no [Amazon S3](#)

Pré-requisitos

Antes de começar, faça o seguinte, se já não o tiver feito:

- [Crie um bucket do Google Cloud Storage](#) com os objetos para os quais você quer transferir AWS.
- [Cadastre-se em uma Conta da AWS](#).
- [Crie um bucket do Amazon S3](#) para armazenar seus objetos depois que eles entrarem no AWS.

Criar uma chave HMAC para seu bucket do Google Cloud Storage

DataSync usa uma chave HMAC associada à sua conta de serviço do Google para se autenticar e ler o bucket do qual você está transferindo dados. (Para obter instruções detalhadas sobre como criar chaves HMAC, consulte a [Documentação do Google Cloud Storage](#).)

Para criar uma chave HMAC

1. Crie uma chave HMAC para sua conta de serviço do Google.
2. Certifique-se de que sua conta de serviço do Google tenha pelo menos Storage Object Viewer permissões.
3. Salve o ID da chave de acesso HMAC e o segredo em um local seguro.

Posteriormente, você precisará desses itens para configurar sua localização DataSync de origem.

Etapa 2: configure sua rede

A configuração de rede é necessária somente ao usar um DataSync agente com sua transferência. Os requisitos de rede para essa migração dependem de onde você escolher implantar seu agente.

Para um DataSync agente no Google Cloud

Se você quiser hospedar seu DataSync agente no Google Cloud, configure sua rede para [permitir DataSync transferências por meio de um endpoint público](#).

Para um DataSync agente em sua VPC

Se você quiser hospedar seu agente em AWS, precisará de uma VPC com um endpoint de interface. DataSync usa o VPC endpoint para facilitar a transferência.

Para configurar sua rede para um endpoint da VPC

1. Se você não tiver uma, [crie uma VPC](#) igual ao Região da AWS seu bucket do S3.
2. [Crie uma sub-rede privada para sua VPC](#).
3. [Crie um endpoint de serviço VPC para](#) DataSync
4. Configure sua rede para [permitir DataSync transferências por meio de um endpoint de serviço VPC](#).

Para fazer isso, modifique o [grupo de segurança](#) associado com seu endpoint de serviço da VPC.

Etapa 3: criar um DataSync agente (opcional)

Um DataSync agente só é necessário ao usar tarefas do modo Básico. Se você estiver usando o modo Avançado para transferir entre o Google Cloud Storage (GCS) e o Amazon S3, nenhum agente será necessário. Se você quiser usar o modo Básico, precisará de um DataSync agente que possa acessar seu bucket do GCS.

Para Google Cloud

Nesse cenário, o DataSync agente é executado em seu ambiente do Google Cloud.

Antes de começar: [instale a CLI do Google Cloud](#).

Para criar o agente para o Google Cloud

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação à esquerda, escolha Agents e Create agent.
3. Para Hypervisor, escolha e VMware ESXi, em seguida, escolha Baixar a imagem para baixar um .zip arquivo que contém o agente.
4. Abra um terminal do . Descompacte a imagem executando o seguinte comando:

```
unzip AWS-DataSync-Agent-VMWare.zip
```

5. Extraia o conteúdo do arquivo .ova do agente, começando com aws-datasync, executando o seguinte comando:

```
tar -xvf aws-datasync-2.0.1655755445.1-x86_64.xfs.gpt.ova
```

6. Importe o arquivo .vmdk do agente para o Google Cloud executando o seguinte comando da CLI do Google Cloud:

```
gcloud compute images import aws-datasync-2-test \  
  --source-file INCOMPLETE-aws-datasync-2.0.1655755445.1-x86_64.xfs.gpt-disk1.vmdk \  
  --os centos-7
```

 Note

A importação do arquivo .vmdk pode levar até duas horas.

7. Crie e inicie uma instância de VM para a imagem do agente que você acabou de importar.

A instância precisa das seguintes configurações para seu agente. (Para obter instruções detalhadas sobre como criar uma instância, consulte a [Documentação do Google Cloud Compute Engine](#)).

- Em Machine type (Tipo de máquina), selecione uma das seguintes opções:
 - e2-standard-8 — Para execuções de DataSync tarefas trabalhando com até 20 milhões de objetos.
 - e2-standard-16 — Para execuções de DataSync tarefas trabalhando com mais de 20 milhões de objetos.
- Para as configurações de inicialização do disco, acesse a seção de imagens personalizadas. Em seguida, escolha a imagem do DataSync agente que você acabou de importar.
- Para a configuração da conta de serviço, escolha sua conta de serviço do Google (a mesma conta que você usou na [Etapa 1](#)).
- Para a configuração do firewall, escolha a opção para permitir o tráfego HTTP (porta 80).

Para ativar seu DataSync agente, a porta 80 deve estar aberta no agente. A porta não precisa ser acessível publicamente. Depois de ativado, DataSync fecha a porta.

8. Depois que a instância de VM estiver em execução, anote seu endereço IP público.

Você precisará desse endereço IP para ativar o agente.

9. Volte para o DataSync console. Na tela Criar agente, na qual você baixou a imagem do agente, faça o seguinte para ativar seu agente:
 - Para Tipo de endpoint, escolha a opção de endpoints de serviço público (por exemplo, Endpoints de serviço público no leste dos EUA em Ohio).
 - Em Chave de ativação, escolha Obter a chave de ativação com o seu agente automaticamente.
 - Em Endereço do agente, insira o endereço IP público da instância de VM do agente que você acabou de criar.
 - Escolha Obter chave.

10. Dê um nome ao seu agente e, em seguida, escolha Criar agente.

O agente está online e pronto para transferir dados.

Para sua VPC

Nesse cenário, o agente é executado como uma EC2 instância da Amazon em uma VPC associada à sua. Conta da AWS

Antes de começar: [configure o AWS Command Line Interface \(AWS CLI\)](#).

Para criar o agente para sua VPC

1. Abra um terminal. Certifique-se de configurar seu AWS CLI perfil para usar a conta associada ao seu bucket do S3.
2. Copie o seguinte comando : Substitua *vpc-region* pelo Região da AWS onde sua VPC reside (por exemplo, us-east-1).

```
aws ssm get-parameter --name /aws/service/datasync/ami --region vpc-region
```

3. Execute o comando . Examine o resultado e anote a propriedade "Value".

Esse valor é o ID da DataSync Amazon Machine Image (AMI) da região que você especificou. Por exemplo, uma ID de AMI pode ser semelhante a `ami-1234567890abcdef0`.

4. Copie o seguinte URL. Novamente, substitua *vpc-region* pelo Região da AWS onde sua VPC reside. Depois, substitua *ami-id* pelo ID da AMI que você anotou na etapa anterior.

```
https://console.aws.amazon.com/ec2/v2/home?region=vpc-region#LaunchInstanceWizard:ami=ami-id
```

5. Cole o URL no navegador.

A página de lançamento da EC2 instância da Amazon é AWS Management Console exibida.

6. Em Tipo de instância, escolha uma das [EC2 instâncias recomendadas da Amazon para DataSync agentes](#).
7. Em Par de chaves, escolha um par de chaves existente ou crie outro.
8. Em Configurações de rede, escolha a VPC e a sub-rede em que você deseja implantar o agente.
9. Escolha Iniciar instância.

10. Quando a EC2 instância da Amazon estiver em execução, [escolha seu VPC](#) endpoint.
11. [Ative o agente](#).

Etapa 4: criar um local DataSync de origem para seu bucket do Google Cloud Storage

Para configurar um DataSync local para seu bucket do Google Cloud Storage, você precisa do ID de acesso e do segredo da chave HMAC que você criou na [Etapa 1](#).

Para criar o local DataSync de origem

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de localização, escolha Armazenamento de objetos.
4. Em Servidor, insira **storage.googleapis.com**.
5. Em Nome do bucket, insira o nome do seu bucket do Google Cloud Storage.
6. Em Pasta, insira um prefixo de objeto.

DataSync copia somente objetos com esse prefixo.

7. Se sua transferência exigir um agente, escolha Usar agentes e escolha o agente que você criou na [Etapa 3](#).
8. Expanda Configurações adicionais. Para Protocolo de servidor, escolha HTTPS. Em Porta do servidor, escolha 443.
9. Role para baixo até a seção Autenticação. Verifique se a caixa de seleção Exige credenciais está marcada e faça o seguinte:
 - Em Chave de acesso, insira o ID de acesso da sua chave HMAC.
 - Em Chave secreta, insira a chave secreta da sua chave HMAC diretamente ou especifique uma chave AWS Secrets Manager secreta que contenha a chave. Para obter mais informações, consulte [Fornecimento de credenciais para locais de armazenamento](#).
10. Escolha Criar local.

Etapa 5: criar um local de DataSync destino para seu bucket do S3

Você precisa de um DataSync local para onde deseja que seus dados acabem.

Para criar o local DataSync de destino

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. [Crie um DataSync local para o bucket do S3](#).

Se você implantou o DataSync agente em sua VPC, este tutorial presume que o bucket do S3 esteja no mesmo Região da AWS que sua VPC e seu agente. DataSync

Etapa 6: criar e iniciar uma DataSync tarefa

Com seus locais de origem e destino configurados, você pode começar a mover seus dados para lá AWS.

Para criar e iniciar a DataSync tarefa

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
3. Na página Configure source location (Configurar local de origem), faça o seguinte:
 - a. Escolha Choose an existing location (Escolher um local existente).
 - b. Escolha o local de origem que você criou na [Etapa 4](#) e, em seguida, escolha Next (Avançar).
4. Na página Configure destination location (Configurar local de destino), faça o seguinte:
 - a. Escolha Choose an existing location (Escolher um local existente).
 - b. Escolha o local de destino que você criou na [Etapa 5](#) e, em seguida, escolha Next (Avançar).
5. Na página Configure settings (Configurar definições), faça o seguinte:
 - a. Em Data transfer configuration (Configuração de transferência de dados), expanda Additional settings (Configurações adicionais) e desmarque a caixa de seleção Copy object tags (Copiar tags de objetos).

 Important

Como a API XML do Google Cloud Storage não é compatível com leitura ou gravação de tags de objetos, sua DataSync tarefa pode falhar se você tentar copiar tags de objetos.

- b. Defina todas as outras configurações de tarefa desejadas e, em seguida, escolha Next (Avançar).
6. Na página Review (Revisar), revise suas configurações e, em seguida, escolha Criar tarefa.
 7. Na página de detalhes da tarefa, escolha Iniciar e, em seguida, escolha uma das seguintes opções:
 - Para executar a tarefa sem modificação, escolha Iniciar com padrões.
 - Para modificar a tarefa antes de executá-la, escolha Iniciar com opções substitutas.

Quando sua tarefa terminar, você verá os objetos do seu bucket do Google Cloud Storage no seu bucket do S3.

Configurar transferências com o Microsoft Azure Blob Storage

Com AWS DataSync, você pode transferir dados entre Microsoft Azure Blob Storage (incluindo armazenamento de Azure Data Lake Storage Gen2 blobs) e os seguintes serviços AWS de armazenamento:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)
- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Para configurar esse tipo de transferência, você cria um [local](#) para o Azure Blob Storage. Você pode usar esse local como origem ou destino de uma transferência. Um DataSync agente é necessário somente ao transferir dados entre o Azure Blob e o Amazon EFS ou Amazon FSx, ou ao usar tarefas

do modo Básico. Você não precisa de um agente para transferir dados entre o Azure Blob e o Amazon S3 usando o modo Avançado.

Fornecendo DataSync acesso ao seu Azure Blob Storage

A forma como você DataSync acessa você Azure Blob Storage depende de vários fatores, incluindo se você está transferindo para ou do armazenamento de blobs e que tipo de [token de assinatura de acesso compartilhado \(SAS\)](#) você está usando. Seus objetos também devem estar em um [nível de acesso](#) que DataSync possa funcionar com.

Tópicos

- [Tokens SAS](#)
- [Níveis de acesso](#)

Tokens SAS

Um token SAS especifica as permissões de acesso para seu armazenamento de blobs. (Para obter mais informações sobre o SAS, consulte a [Documentação do Azure Blob Storage](#).)

Você pode gerar tokens SAS para fornecer diferentes níveis de acesso. DataSync suporta tokens com os seguintes níveis de acesso:

- Conta
- Contêiner

As permissões de acesso DataSync necessárias dependem do escopo do seu token. Não ter as permissões corretas pode fazer com que sua transferência falhe. Por exemplo, sua transferência não será bem-sucedida se você estiver movendo objetos com tags para o Azure Blob Storage, mas seu token SAS não tiver permissões de tag.

Tópicos

- [Permissões de token SAS para acesso no nível da conta](#)
- [Permissões de token SAS para acesso em nível de contêiner](#)
- [Políticas de expiração do SAS](#)

Permissões de token SAS para acesso no nível da conta

DataSync precisa de um token de acesso no nível da conta com as seguintes permissões (dependendo se você está transferindo para ou de). Azure Blob Storage

Transfers from blob storage

- Serviços permitidos: Blob
- Tipos de recursos permitidos: Contêiner, Objeto

Se você não incluir essas permissões, não DataSync poderá transferir os metadados do objeto, incluindo as [tags de objeto](#).

- Permissões permitidas: Ler, Listar
- Permissões de índice de blob permitidas — [Leitura/Gravação \(se você quiser copiar tags DataSync de objetos\)](#)

Transfers to blob storage

- Serviços permitidos: Blob
- Tipos de recursos permitidos: Contêiner, Objeto

Se você não incluir essas permissões, não DataSync poderá transferir os metadados do objeto, incluindo as [tags de objeto](#).

- Permissões permitidas — Ler, Gravar, Listar, Excluir (se você quiser DataSync remover arquivos que não estão na sua fonte de transferência)
- Permissões de índice de blob permitidas — [Leitura/Gravação \(se você quiser copiar tags DataSync de objetos\)](#)

Permissões de token SAS para acesso em nível de contêiner

DataSync precisa de um token de acesso em nível de contêiner com as seguintes permissões (dependendo se você está transferindo para ou de). Azure Blob Storage

Transfers from blob storage

- Leitura
- Lista

- Tag (se você quiser DataSync copiar [tags de objetos](#))

 Note

Você não pode adicionar a permissão de tag ao gerar um token SAS no portal Azure. Para adicionar a permissão de tag, gere o token usando o aplicativo [Azure Storage Explorer](#) ou gere um [token SAS que forneça acesso em nível de conta](#).

Transfers to blob storage

- Leitura
- Escrever
- Lista
- Excluir (se você quiser DataSync remover arquivos que não estão na sua fonte de transferência)
- Tag (se você quiser DataSync copiar [tags de objetos](#))

 Note

Você não pode adicionar a permissão de tag ao gerar um token SAS no portal Azure. Para adicionar a permissão de tag, gere o token usando o aplicativo [Azure Storage Explorer](#) ou gere um [token SAS que forneça acesso em nível de conta](#).

Políticas de expiração do SAS

Certifique-se de que seu SAS não expire antes de você concluir sua transferência. Para obter informações sobre como configurar uma política de expiração do SAS, consulte a [Documentação do Azure Blob Storage](#)

Se o SAS expirar durante a transferência, não DataSync poderá mais acessar sua Azure Blob Storage localização. (Você pode ver um erro de Falha ao abrir o diretório.) Se isso acontecer, [atualize sua localização](#) com um novo token SAS e reinicie sua DataSync tarefa.

Níveis de acesso

Ao transferir de Azure Blob Storage, DataSync pode copiar objetos nas camadas quente e fria. Para objetos na camada de acesso ao arquivamento, você deve reidratar esses objetos para a camada quente ou fria antes de poder copiá-los.

Ao transferir para Azure Blob Storage, DataSync pode copiar objetos para os níveis de acesso quente, frio e arquivamento. Se você estiver copiando objetos na camada de acesso ao arquivamento, não DataSync poderá verificar a transferência se estiver tentando [verificar todos os dados no destino](#).

DataSync não suporta o nível de acesso frio. Para obter mais informações sobre níveis de acesso, consulte a [Documentação do Azure Blob Storage](#).

Considerações sobre transferências Azure Blob Storage

Ao planejar a transferência de dados de ou para Azure Blob Storage com DataSync, há algumas coisas que você deve ter em mente.

Tópicos

- [Custos](#)
- [Tipos de bolhas](#)
- [Disponibilidade do Região da AWS](#)
- [Copiar tags de objeto](#)
- [Transferindo para o Amazon S3](#)
- [Excluindo diretórios em um destino de transferência](#)
- [Limitações](#)

Custos

As taxas associadas à movimentação de dados para dentro ou para fora do Azure Blob Storage podem incluir:

- Executando uma [máquina Azure virtual \(VM\)](#) (se você implantar um DataSync agente em Azure)
- Executando uma EC2 instância [da Amazon](#) (se você implantar um DataSync agente em uma VPC interna) AWS

- Transferir os dados usando [DataSync](#), incluindo cobranças de solicitação relacionadas ao [Azure Blob Storage](#) S3 (se o S3 for um dos seus locais de transferência)
- Transferindo dados para dentro ou para fora do [Azure Blob Storage](#)
- Armazenamento de dados em um [serviço AWS de armazenamento](#) suportado pelo DataSync

Tipos de bolhas

A forma como DataSync funciona com os tipos de blob depende se você está transferindo para ou de. Azure Blob Storage Quando você está movendo dados para o armazenamento de blobs, os objetos ou arquivos DataSync transferidos só podem ser blobs de blocos. Quando você está movendo dados para fora do armazenamento de blobs, DataSync pode transferir blocos, páginas e anexar blobs.

Para obter mais informações sobre , consulte a [documentação do Azure Blob Storage](#).

Disponibilidade do Região da AWS

Você pode criar um local Azure Blob Storage de transferência em qualquer um [Região da AWS que seja suportado pelo DataSync](#).

Copiar tags de objeto

A capacidade de DataSync preservar as tags de objetos durante a transferência de ou para Azure Blob Storage depende dos seguintes fatores:

- O tamanho das tags de um objeto — não é DataSync possível transferir um objeto com tags que excedam 2 KB.
- Se DataSync está configurado para copiar tags de objetos — DataSync [copia tags de objetos](#) por padrão.
- O namespace que sua conta Azure de armazenamento usa — DataSync pode copiar tags de objeto se sua conta de Azure armazenamento usar um namespace plano, mas não se sua conta usar um namespace hierárquico (um recurso do). Azure Data Lake Storage Gen2 Sua DataSync tarefa falhará se você tentar copiar tags de objetos e sua conta de armazenamento usar um namespace hierárquico.
- Se seu token SAS autoriza a marcação: as permissões que você precisa para copiar tags de objetos variam de acordo com o nível de acesso que seu token fornece. Sua tarefa falhará se você tentar copiar tags de objetos e seu token não tiver as permissões corretas para marcação. Para

obter mais informações, verifique os requisitos de permissão para tokens de acesso em [nível de conta ou tokens de acesso](#) ou [tokens de acesso em nível de contêiner](#).

Transferindo para o Amazon S3

Ao transferir para o Amazon S3 DataSync, não Azure Blob Storage transferirá objetos maiores que 5 TB ou objetos com metadados maiores que 2 KB.

Excluindo diretórios em um destino de transferência

Ao transferir para Azure Blob Storage, DataSync pode [remover objetos em seu armazenamento de blobs que não estão presentes na sua fonte de transferência](#). (Você pode configurar essa opção desmarcando a configuração Manter arquivos excluídos no DataSync console. Seu [token SAS](#) também deve ter permissões de exclusão.)

Ao configurar sua transferência dessa forma, DataSync não excluirá diretórios em seu armazenamento de blobs se sua conta de armazenamento estiver usando um Azure namespace hierárquico. Nesse caso, você deve excluir manualmente os diretórios (por exemplo, usando [Azure Storage Explorer](#)).

Limitações

Para transferir dados para ou de um Azure Blob Storage, existem as seguintes limitações:

- DataSync [cria alguns diretórios](#) em um local para ajudar a facilitar sua transferência. Se Azure Blob Storage for um local de destino e sua conta de armazenamento usar um namespace hierárquico, você poderá observar subdiretórios específicos da tarefa (como) na pasta. `task-000011112222abcde /.aws-datasync` DataSync normalmente exclui esses subdiretórios após uma transferência. Se isso não acontecer, você mesmo poderá excluir esses diretórios específicos da tarefa, desde que a tarefa não esteja em execução.
- DataSync não suporta o uso de um token SAS para acessar somente uma pasta específica em seu Azure Blob Storage contêiner.
- Você não pode fornecer DataSync um token SAS de delegação de usuário para acessar seu armazenamento de blobs.

Criando seu DataSync agente (opcional)

Um DataSync agente é necessário somente ao transferir dados entre o Azure Blob e o Amazon EFS ou Amazon FSx, ou ao usar tarefas do modo Básico. Você não precisa de um agente para transferir

dados entre o Azure Blob e o Amazon S3 usando o modo Avançado. Esta seção descreve como implantar e ativar um agente.

 Tip

Embora você possa implantar seu agente em uma EC2 instância da Amazon, usar um Microsoft Hyper-V agente pode resultar em menor latência de rede e maior compactação de dados.

Agentes do Microsoft Hyper-V

Você pode implantar seu DataSync agente diretamente Azure com uma Microsoft Hyper-V imagem.

 Tip

Antes de continuar, considere usar um script de shell que possa ajudá-lo a implantar seu atendente Hyper-V no Azure mais rapidamente. Você pode obter mais informações e baixar o código em [GitHub](#).

Se você usar o script, poderá avançar para a seção sobre [Obtendo a chave de ativação do seu atendente](#).

Tópicos

- [Pré-requisitos](#)
- [Baixando e preparando seu atendente](#)
- [Implantando seu atendente no Azure](#)
- [Obtendo a chave de ativação do seu atendente](#)
- [Ativar o atendente](#)

Pré-requisitos

Para preparar seu DataSync agente e implantá-lo Azure, você deve fazer o seguinte:

- Habilite Hyper-V na sua máquina local.
- Instale [PowerShell](#) (incluindo o Hyper-V Module).

- Instale a [CLI Azure](#).
- Instalar o [AzCopy](#).

Baixando e preparando seu atendente

Baixe um agente do DataSync console. Antes de implantar o atendente Azure, você deve convertê-lo em um disco rígido virtual (VHD) de tamanho fixo. Para obter mais informações, consulte a [documentação do Azure](#).

Para baixar e preparar seu atendente

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação à esquerda, escolha Agentes e, em seguida, escolha Criar agente.
3. Para Hypervisor, escolha Microsoft Hyper-V, em seguida, escolha Baixar a imagem.

O atendente faz o download em um arquivo .zip que contém um arquivo .vhdx.

4. Extraia o arquivo .vhdx na sua máquina local.
5. Abra o PowerShell e faça o seguinte:
 - a. Copie o seguinte Convert-VHD cmdlet:

```
Convert-VHD -Path .\local-path-to-vhdx-file\aws-datasync-2.0.1686143940.1-x86_64.xfs.gpt.vhdx -DestinationPath .\local-path-to-vhdx-file\aws-datasync-2016861439401-x86_64.vhd -VHDType Fixed
```

- b. Substitua cada instância *local-path-to-vhdx-file* de pela localização do arquivo .vhdx na sua máquina local.
- c. Execute o comando.

Seu atendente agora é um VHD de tamanho fixo (com formato de arquivo .vhd) e está pronto para ser implantado no Azure.

Implantando seu atendente no Azure

A implantação de seu DataSync agente Azure envolve:

- Criar um disco gerenciado no Azure

- Fazendo o upload do seu atendente para esse disco gerenciado
- Conectando o disco gerenciado a uma máquina virtual Linux

Para implantar seu atendente no Azure

1. No PowerShell, acesse o diretório que contém o arquivo .vhd do seu atendente.
2. Execute o comando `ls` e salve o valor `Length` (por exemplo, 85899346432).

Esse é o tamanho da imagem do atendente em bytes, necessário ao criar um disco gerenciado que possa conter a imagem.

3. Faça o seguinte para criar um disco gerenciado:
 - a. Copie o seguinte comando da CLI Azure:

```
az disk create -n your-managed-disk `
-g your-resource-group `
-l your-azure-region `
--upload-type Upload `
--upload-size-bytes agent-size-bytes `
--sku standard_lrs
```

- b. Substitua *your-managed-disk* por um nome para seu disco gerenciado.
- c. Substitua *your-resource-group* pelo nome do grupo de recursos Azure ao qual sua conta de armazenamento pertence.
- d. Substitua *your-azure-region* pela região Azure em que seu grupo de recursos está localizado.
- e. Substitua *agent-size-bytes* pelo tamanho da imagem do seu atendente.
- f. Execute o comando.

Esse comando cria um disco gerenciado vazio com um [SKU padrão](#) no qual você pode carregar seu DataSync agente.

4. Para gerar uma assinatura de acesso compartilhado (SAS) que permita acesso de gravação ao disco gerenciado, faça o seguinte:
 - a. Copie o seguinte comando da CLI Azure:

```
az disk grant-access -n your-managed-disk `
```

```
-g your-resource-group `
--access-level Write `
--duration-in-seconds 86400
```

- b. Substitua *your-managed-disk* pelo nome do disco gerenciado que você criou.
- c. Substitua *your-resource-group* pelo nome do grupo de recursos Azure ao qual sua conta de armazenamento pertence.
- d. Execute o comando .

Examine o resultado e anote o URI do SAS. Você precisa desse URI ao fazer o upload do atendente para o Azure.

O SAS permite que você grave no disco por até uma hora. Isso significa que você tem uma hora para carregar seu atendente no disco gerenciado.

5. Para fazer upload do atendente para o disco gerenciado no Azure, faça o seguinte:
 - a. Copie o seguinte comando AzCopy:

```
.\azcopy copy local-path-to-vhd-file sas-uri --blob-type PageBlob
```

- b. Substitua *local-path-to-vhd-file* pela localização do arquivo .vhd do atendente em sua máquina local.
 - c. Substitua *sas-uri* pelo URI SAS que você obteve ao executar o comando `az disk grant-access`.
 - d. Execute o comando .
6. Quando o upload do atendente terminar, revogue o acesso ao seu disco gerenciado. Para fazer isso, copie este comando Azure CLI:

```
az disk revoke-access -n your-managed-disk -g your-resource-group
```

- a. Substitua *your-resource-group* pelo nome do grupo de recursos Azure ao qual sua conta de armazenamento pertence.
 - b. Substitua *your-managed-disk* pelo nome do disco gerenciado criado.
 - c. Execute o comando.
7. Faça o seguinte para conectar seu disco gerenciado a uma nova VM Linux:
 - a. Copie o seguinte comando da CLI Azure:

```
az vm create --resource-group your-resource-group `
--location eastus `
--name your-agent-vm `
--size Standard_E4as_v4 `
--os-type linux `
--attach-os-disk your-managed-disk
```

- b. Substitua *your-resource-group* pelo nome do grupo de recursos Azure ao qual sua conta de armazenamento pertence.
- c. Substitua *your-agent-vm* por um nome para a VM que você possa lembrar.
- d. Substitua *your-managed-disk* pelo nome do disco gerenciado que você está anexando à VM.
- e. Execute o comando .

Você enviou seu atendente. Antes de começar a configurar sua transferência de dados, você deve ativar o atendente.

Obtendo a chave de ativação do seu atendente

Para obter manualmente a chave de ativação do seu DataSync agente, siga estas etapas.

Como alternativa, [DataSync pode obter automaticamente a chave de ativação para você](#), mas essa abordagem requer alguma configuração de rede.

Para obter a chave de ativação do seu atendente

1. No portal Azure, [habilite o diagnóstico de inicialização da VM para seu atendente](#) escolhendo a configuração Habilitar com conta de armazenamento personalizada e especificando sua conta de armazenamento Azure.

Depois de habilitar o diagnóstico de inicialização para a VM do seu atendente, você pode acessar o console local do atendente para obter a chave de ativação.

2. Enquanto ainda estiver no portal Azure, acesse sua VM e escolha Console serial.
3. No console local do atendente, faça login usando as seguintes credenciais padrão:
 - Nome de usuário – **admin**
 - Senha: **password**

Recomendamos, em algum momento, alterar pelo menos a senha do atendente. No console local do atendente, insira **5** no menu principal e use o comando `passwd` para alterar a senha.

4. Insira **0** para obter a chave de ativação do atendente.
5. Insira o Região da AWS local em que você está usando DataSync (por exemplo, **us-east-1**).
6. Escolha o [endpoint de serviço](#) que o agente usará para se conectar AWS.
7. Salve valor da saída `Activation key`.

Ativar o atendente

Depois de ter a chave de ativação, você pode concluir a criação do seu DataSync agente.

Como ativar o agente

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação à esquerda, escolha Agentes e, em seguida, escolha Criar agente.
3. Para Hypervisor, escolha Microsoft Hyper-V.
4. Para Tipo de endpoint, escolha o mesmo tipo de endpoint de serviço que você especificou quando recebeu a chave de ativação do seu agente (por exemplo, escolha Endpoints de serviço público em). *Region name*
5. Configure sua rede para funcionar com o tipo de endpoint de serviço que seu atendente está usando. Para obter informações sobre os requisitos de rede de endpoints de serviço, consulte os tópicos a seguir:
 - [Endpoints do VPC](#)
 - [Endpoints públicos](#)
 - [Endpoints do Federal Information Processing Standard \(FIPS – Padrões Federais de Processamento de Informações\)](#)
6. Para a Chave de ativação, faça o seguinte:
 - a. Escolha Inserir manualmente a chave de ativação do seu agente.
 - b. Insira a chave de ativação que você obteve do console local do agente.
7. Escolha Criar agente.

Seu agente está pronto para se conectar ao seu Azure Blob Storage. Para obter mais informações, consulte [Criar seu local de transferência Azure Blob Storage](#).

EC2 Agentes da Amazon

Você pode implantar seu DataSync agente em uma EC2 instância da Amazon.

Para criar um EC2 agente da Amazon

1. [Implante um EC2 agente da Amazon](#).
2. [Escolha um endpoint de serviço](#) que o atendente use para se comunicar ao AWS.

Nessa situação, recomendamos o uso de um endpoint de serviço de nuvem privada virtual (VPC).

3. Configure sua rede para funcionar com [endpoints de serviço do VPC](#).
4. [Ative o agente](#).

Criar seu local de transferência Azure Blob Storage

Você pode configurar DataSync para usar o seu Azure Blob Storage como fonte ou destino de transferência.

Antes de começar

Certifique-se de saber [como DataSync acessa Azure Blob Storage](#) e trabalha com [camadas de acesso](#) e tipos de [blob](#). Você também precisa de um [DataSync agente](#) que possa se conectar ao seu Azure Blob Storage contêiner.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de local, escolha Microsoft Azure Blob Storage.
4. Em URL do contêiner, insira o URL do contêiner envolvido na sua transferência.
5. (Opcional) Para Nível de acesso quando usado como destino, escolha o [nível de acesso](#) para o qual você deseja que seus objetos ou arquivos sejam transferidos.

6. Em Pasta, insira segmentos de caminho se quiser limitar sua transferência a um diretório virtual em seu contêiner (por exemplo, /my/images).
7. Se sua transferência exigir um agente, escolha Usar agentes e escolha o DataSync agente que pode se conectar ao seu Azure Blob Storage contêiner.
8. Para o token SAS, forneça as credenciais necessárias DataSync para acessar seu armazenamento de blobs. Alguns conjuntos de dados públicos no armazenamento de Blobs do Azure não exigem credenciais. Você pode inserir um token SAS diretamente ou especificar um AWS Secrets Manager segredo que contenha o token. Para obter mais informações, consulte [Fornecimento de credenciais para locais de armazenamento](#).

Seu token SAS faz parte da string de URI SAS que vem depois do URI do recurso de armazenamento e de um ponto de interrogação (?). Um token é semelhante ao seguinte:

```
sp=r&st=2023-12-20T14:54:52Z&se=2023-12-20T22:54:52Z&spr=https&sv=2021-06-08&sr=c&sig=aBBKD%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
```

9. (Opcional) Forneça valores para os campos Chave e Valor para marcar o local.

As tags ajudam você a gerenciar, filtrar e pesquisar seus AWS recursos. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

10. Escolha Criar local.

Usando o AWS CLI

1. Copie o seguinte comando create-location-azure-blob:

```
aws datasync create-location-azure-blob \
  --container-url "https://path/to/container" \
  --authentication-type "SAS" \
  --sas-configuration '{
    "Token": "your-sas-token"
  }' \
  --agent-arns my-datasync-agent-arn \
  --subdirectory "/path/to/my/data" \
  --access-tier "access-tier-for-destination" \
  --tags [{"Key": "key1", "Value": "value1"}]
```

2. Para o parâmetro --container-url, especifique o URL do contêiner Azure Blob Storage envolvido na sua transferência.

3. Para o parâmetro `--authentication-type`, especifique SAS. Se você estiver acessando um conjunto de dados público que não exige autenticação, especifique `NONE`.
4. Para a Token opção do `--sas-configuration` parâmetro, especifique o token SAS que permite DataSync acessar seu armazenamento de blobs.

Você também pode fornecer parâmetros adicionais para proteger suas chaves usando AWS Secrets Manager. Para obter mais informações, consulte [Fornecimento de credenciais para locais de armazenamento](#).

Seu token SAS faz parte da string de URI SAS que vem depois do URI do recurso de armazenamento e de um ponto de interrogação (?). Um token é semelhante ao seguinte:

```
sp=r&st=2023-12-20T14:54:52Z&se=2023-12-20T22:54:52Z&spr=https&sv=2021-06-08&sr=c&sig=aBBKD%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
```

5. (Opcional) Para o `--agent-arns` parâmetro, especifique o Amazon Resource Name (ARN) do DataSync agente que pode se conectar ao seu contêiner.

Aqui está um exemplo de agente ARN: `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

Você pode especificar mais de um atendente. Para obter mais informações, consulte [Usando vários DataSync agentes](#).

6. Para o parâmetro `--subdirectory`, especifique segmentos de caminho se quiser limitar sua transferência para um diretório virtual em seu contêiner (por exemplo, `/my/images`).
7. (Opcional) Para o parâmetro `--access-tier`, especifique o [nível de acesso](#) (HOT, COOL ou ARCHIVE) para a qual você deseja transferir seus objetos ou arquivos.

Esse parâmetro se aplica somente quando você está usando esse local como destino de transferência.

8. (Opcional) Para o parâmetro `--tags`, especifique pares chave-valor que ajudam a gerenciar, filtrar e pesquisar sua localização.

Recomendamos criar uma etiqueta de nome para a sua localização.

9. Execute o comando `create-location-azure-blob`.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN do local que você criou. Por exemplo:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh"
}
```

Visualizando seu local de transferência Azure Blob Storage

Você pode obter detalhes sobre o local de DataSync transferência existente para o seu Azure Blob Storage.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e, em seguida, escolha Locais.
3. Escolha seu local Azure Blob Storage.

Você pode ver detalhes sobre sua localização, incluindo todas as tarefas de DataSync transferência que a estão usando.

Usando o AWS CLI

1. Copie o seguinte comando `describe-location-azure-blob`:

```
aws datasync describe-location-azure-blob \
  --location-arn "your-azure-blob-location-arn"
```

2. Para o parâmetro `--location-arn`, especifique o ARN do local Azure Blob Storage que você criou (por exemplo, `arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. Execute o comando `describe-location-azure-blob`.

Você recebe uma resposta que mostra detalhes sobre sua localização. Por exemplo:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh",
  "LocationUri": "azure-blob://my-user.blob.core.windows.net/container-1",
}
```

```

    "AuthenticationType": "SAS",
    "Subdirectory": "/my/images",
    "AgentArns": ["arn:aws:datasync:us-east-1:123456789012:agent/
agent-01234567890deadfb"],
  }

```

Atualizando seu local de transferência Azure Blob Storage

Se necessário, você pode modificar a configuração da sua localização no console ou usando o AWS CLI.

Usando o AWS CLI

1. Copie o seguinte comando `update-location-azure-blob`:

```

aws datasync update-location-azure-blob \
  --location-arn "your-azure-blob-location-arn" \
  --authentication-type "SAS" \
  --sas-configuration '{
    "Token": "your-sas-token"
  }' \
  --agent-arns my-datasync-agent-arn \
  --subdirectory "/path/to/my/data" \
  --access-tier "access-tier-for-destination"

```

2. Para o parâmetro `--location-arn`, especifique o ARN do local Azure Blob Storage que você está atualizando (por exemplo, `arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. Para o parâmetro `--authentication-type`, especifique SAS.
4. Para a Token opção do `--sas-configuration` parâmetro, especifique o token SAS que permite DataSync acessar seu armazenamento de blobs.

O token faz parte da string SAS URI que vem depois do URI do recurso de armazenamento e de um ponto de interrogação (?). Um token é semelhante ao seguinte:

```

sp=r&st=2022-12-20T14:54:52Z&se=2022-12-20T22:54:52Z&spr=https&sv=2021-06-08&sr=c&sig=qCBKD
%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D

```

5. Para o `--agent-arns` parâmetro, especifique o Amazon Resource Name (ARN) do DataSync agente que você deseja conectar ao seu contêiner.

Aqui está um exemplo de agente ARN: `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

Você pode especificar mais de um atendente. Para obter mais informações, consulte [Usando vários DataSync agentes](#).

6. Para o parâmetro `--subdirectory`, especifique segmentos de caminho se quiser limitar sua transferência para um diretório virtual em seu contêiner (por exemplo, `/my/images`).
7. (Opcional) Para o parâmetro `--access-tier`, especifique o [nível de acesso](#) (HOT, COOL ou ARCHIVE) para o qual você deseja que seus objetos sejam transferidos.

Esse parâmetro se aplica somente quando você está usando esse local como destino de transferência.

Próximas etapas

Depois de terminar de criar um DataSync local para o seu Azure Blob Storage, você pode continuar configurando sua transferência. Veja aqui alguns dos próximos passos a considerar:

1. Se ainda não o fez, [crie outro local](#) onde você planeja transferir seus dados de ou para o seu Azure Blob Storage.
2. Saiba como DataSync [lidar com metadados e arquivos especiais](#), especialmente se seus locais de transferência não tiverem uma estrutura de metadados semelhante.
3. Configure como os dados são transferidos. Por exemplo, você pode [transferir apenas um subconjunto de seus dados](#) ou excluir arquivos do armazenamento de blobs que não estejam no local de origem (desde que o [token SAS](#) tenha permissões de exclusão).
4. [Inicie sua transferência](#).

Configurando AWS DataSync transferências com Microsoft Azure Files Ações de pequenas e médias empresas

Você pode configurar AWS DataSync para transferir dados de ou para um Microsoft Azure Files Compartilhamento do Server Message Block (SMB).

 Tip

[Para obter uma explicação completa sobre como mover dados dos compartilhamentos SMB dos Arquivos do Azure para AWS, consulte o AWS Blog de Armazenamento.](#)

Fornecendo DataSync acesso a compartilhamentos de pequenas e médias empresas

DataSync se conecta ao seu compartilhamento SMB usando o protocolo SMB e se autentica com as credenciais fornecidas por você.

Tópicos

- [Versões do protocolo SMB compatíveis](#)
- [Permissões obrigatórias](#)

Versões do protocolo SMB compatíveis

Por padrão, escolhe DataSync automaticamente uma versão do protocolo SMB com base na negociação com seu servidor de arquivos SMB.

Você também pode configurar DataSync para usar uma versão SMB específica, mas recomendamos fazer isso somente se DataSync tiver problemas para negociar com o servidor de arquivos SMB automaticamente. DataSync oferece suporte às versões 1.0 e posteriores do SMB. Por motivos de segurança, recomendamos usar a versão 3.0.2 ou posterior do SMB. Versões anteriores, como a SMB 1.0, contêm vulnerabilidades de segurança conhecidas que os invasores podem explorar para comprometer seus dados.

Consulte a tabela a seguir para ver uma lista de opções no DataSync console e na API:

Opção do console	Opção de API	Descrição
Automatic	AUTOMATIC	DataSync e o servidor de arquivos SMB negociam a versão mais alta do SMB que eles suportam mutuamente entre 2.1 e 3.1.1. Essa é a opção recomendada e também a padrão. Se, em vez disso, você escolher uma versão específica que

Opção do console	Opção de API	Descrição
		seu servidor de arquivos não suporta, você pode receber um erro <code>Operation Not Supported</code> .
SMB 3.0.2	SMB3	Restringe a negociação do protocolo somente à versão 3.0.2 do SMB.
SMB 2.1	SMB2	Restringe a negociação do protocolo somente à versão 2.1 do SMB.
SMB 2.0	SMB2_0	Restringe a negociação do protocolo somente à versão 2.0 do SMB.
SMB 1.0	SMB1	: restringe a negociação do protocolo somente à versão 3.0.2 do SMB.

Permissões obrigatórias

DataSync precisa de um usuário que tenha permissão para montar e acessar sua localização SMB. Esse usuário pode ser um usuário local em seu servidor de arquivos do Windows ou pode ser um usuário de domínio definido no Active Directory.

Para definir a propriedade do objeto, é necessário o `SE_RESTORE_NAME` privilégio, que geralmente é concedido aos membros dos grupos integrados do Active Directory Operadores de Backup e Administradores de Domínio. Fornecer esse privilégio DataSync a um usuário também ajuda a garantir permissões suficientes para arquivos, pastas e metadados de arquivos, exceto para listas de controle de acesso do sistema NTFS (). SACLs

Privilégios adicionais são necessários para copiar SACLs. Essa operação requer especificamente o privilégio `SE_SECURITY_NAME` do Windows, que é concedido aos membros do grupo Administradores de domínio. Se você configurar sua tarefa para copiar SACLs, verifique se o usuário tem os privilégios necessários. Para saber mais sobre como configurar uma tarefa para copiar SACLs, consulte [Configuração de como lidar com arquivos, objetos e metadados](#).

Quando você copia dados entre um servidor de arquivos SMB e o sistema de arquivos Amazon FSx for Windows File Server, os locais de origem e destino devem pertencer ao mesmo domínio do Microsoft Active Directory ou ter uma relação de confiança do Active Directory entre seus domínios.

Criar o local de transferência de arquivos do Azure usando o console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de local, escolha Server Message Block (SMB).

Você configurará esse local como origem ou destino posteriormente.

4. Para Agentes, escolha um ou mais DataSync agentes que você deseja conectar ao seu compartilhamento SMB.

Se você escolher mais de um agente, certifique-se de entender o uso de [vários agentes em um local](#).

5. Para Servidor SMB, insira o nome do Sistema de Nomes de Domínio (DNS) ou o endereço IP do compartilhamento SMB que seu DataSync agente montará.

Note

Você não pode especificar um endereço IP versão 6 (IPv6).

6. Em Nome do compartilhamento, insira o nome do compartilhamento exportado pelo seu compartilhamento SMB onde os dados DataSync serão lidos ou gravados.

Você pode incluir um subdiretório no caminho de compartilhamento (por exemplo, `/path/to/subdirectory`). Certifique-se de que outros clientes do SMB em sua rede também possam montar este caminho.

Para copiar todos os dados no subdiretório, DataSync deve ser capaz de montar o compartilhamento SMB e acessar todos os seus dados. Para obter mais informações, consulte [Permissões obrigatórias](#).

7. (Opcional) Expanda Configurações adicionais e escolha uma versão SMB DataSync para usar ao acessar seu compartilhamento SMB.

Por padrão, escolha DataSync automaticamente uma versão com base na negociação com o compartilhamento SMB. Para ter mais informações, consulte [Versões compatíveis do SMB](#).

8. Em Usuário, insira um nome de usuário que possa montar o compartilhamento SMB e tenha permissão para acessar os arquivos e pastas envolvidos na sua transferência.

Para obter mais informações, consulte [Permissões obrigatórias](#).

9. Em Senha, insira a senha do usuário que pode montar o local e que tem as permissões para acessar arquivos e pastas no local do SMB.
10. (Opcional) Em Domínio, insira o nome de domínio do Windows ao qual o compartilhamento SMB pertence.

Se você tiver vários domínios em seu ambiente, definir essa configuração garante que ele se DataSync conecte ao compartilhamento correto.

11. (Opcional) Escolha Adicionar tag para marcar sua localização.

As Tags são pares de chave-valor que ajudam você a gerenciar, filtrar e pesquisar seus locais. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

12. Escolha Criar local.

Configurar transferências de com outro armazenamento de objetos na nuvem

Com AWS DataSync, você pode transferir dados entre [serviços AWS de armazenamento](#) e os seguintes provedores de armazenamento de objetos na nuvem:

- [Wasabi Cloud Storage](#)
- [DigitalOcean Spaces](#)
- [Oracle Cloud Infrastructure Object Storage](#)
- [Cloudflare R2 Storage](#)
- [Backblaze B2 Cloud Storage](#)
- [NAVER Cloud Object Storage](#)
- [Alibaba Cloud Object Storage Service](#)
- [IBM Cloud Object Storage](#)
- [Seagate Lyve Cloud](#)

Um DataSync agente é necessário somente ao transferir dados entre sistemas de armazenamento em outras nuvens e o Amazon EFS ou Amazon FSx, ou ao usar tarefas do modo Básico. Você não precisa de um agente para transferir dados entre sistemas de armazenamento em outras nuvens e no Amazon S3 usando o modo Enhanced.

Independentemente de usar um agente, você também deve criar um [local](#) de transferência para seu armazenamento de objetos na nuvem (especificamente um local de armazenamento de objetos). DataSync pode usar esse local como origem ou destino para sua transferência.

Fornecendo DataSync acesso ao seu outro armazenamento de objetos na nuvem

A forma como DataSync acessa seu armazenamento de objetos na nuvem depende de vários fatores, incluindo se seu armazenamento é compatível com a API do Amazon S3 e as permissões e credenciais DataSync necessárias para acessar seu armazenamento.

Tópicos

- [Compatibilidade da API do Amazon S3](#)
- [Permissões de armazenamento e endpoints](#)
- [Credenciais de armazenamento](#)

Compatibilidade da API do Amazon S3

Seu armazenamento de objetos na nuvem deve ser compatível com as seguintes [operações de API do Amazon S3](#) para se conectar DataSync a ele:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- DeleteObjectTagging
- GetBucketLocation
- GetObject
- GetObjectTagging
- HeadBucket
- HeadObject
- ListObjectsV2

- PutObject
- PutObjectTagging
- UploadPart

Permissões de armazenamento e endpoints

Você deve configurar as permissões que permitem DataSync acessar seu armazenamento de objetos na nuvem. Se seu armazenamento de objetos for um local de origem, DataSync precisará de permissões de leitura e lista para o bucket do qual você está transferindo dados. Se seu armazenamento de objetos for um local de destino, DataSync precisará de permissões de leitura, lista, gravação e exclusão para o bucket.

DataSync também precisa de um endpoint (ou servidor) para se conectar ao seu armazenamento. A tabela a seguir descreve os endpoints que DataSync podem ser usados para acessar outros armazenamentos de objetos na nuvem:

Outro provedor de nuvem	Endpoint
Wasabi Cloud Storage	S3. <i>region</i> .wasabisys.com
DigitalOcean Spaces	<i>region</i> .digitaloceanspaces.com
Oracle Cloud Infrastructure Object Storage	<i>namespace</i> .compat.objectstorage. <i>region</i> .oraclecloud.com
Cloudflare R2 Storage	<i>account-id</i> .r2.cloudflarestorage.com
Backblaze B2 Cloud Storage	S3. <i>region</i> .backblazeb2.com
NAVER Cloud Object Storage	<i>region</i> .object.ncloudstorage.com (maioria das regiões)
Alibaba Cloud Object Storage Service	<i>region</i> .aliyuncs.com
IBM Cloud Object Storage	s3. <i>region</i> .cloud-object-storage.appdomain.cloud
Seagate Lyve Cloud	s3. <i>region</i> .lyvecloud.seagate.com

 Important

Para obter detalhes sobre como configurar permissões de bucket e informações atualizadas sobre endpoints de armazenamento, consulte a documentação do seu provedor de nuvem.

Credenciais de armazenamento

DataSync também precisa das credenciais para acessar o bucket de armazenamento de objetos envolvido na sua transferência. Isso pode ser uma chave de acesso e uma chave secreta ou algo semelhante, dependendo de como seu provedor de armazenamento na nuvem se refere a essas credenciais.

Para obter mais informações, consulte a documentação do seu provedor de nuvem.

Considerações ao transferir de outro armazenamento de objetos na nuvem

Ao planejar a transferência de objetos de ou para outro provedor de armazenamento em nuvem usando DataSync, há algumas coisas que você deve ter em mente.

Tópicos

- [Custos](#)
- [Classes de armazenamento](#)
- [Tags de objetos](#)
- [Transferindo para o Amazon S3](#)

Custos

As taxas associadas à movimentação de dados para dentro e para fora de outro provedor de armazenamento em nuvem podem incluir:

- Executando uma EC2 instância [da Amazon](#) para seu DataSync agente
- Transferir os dados usando [DataSync](#), incluindo cobranças de solicitação relacionadas ao seu armazenamento de objetos na nuvem e ao [Amazon S3](#) (se o S3 for seu destino de transferência)
- Transferir dados para dentro ou para fora do seu armazenamento em nuvem (verifique os preços do seu provedor de nuvem)
- Armazenamento de dados em um [serviço AWS de armazenamento](#) suportado pelo DataSync

- Armazenamento de dados em outro provedor de nuvem (verifique os preços do seu provedor de nuvem)

Classes de armazenamento

Alguns provedores de armazenamento em nuvem têm classes de armazenamento (semelhantes às do [Amazon S3](#)) que não DataSync podem ser lidas sem serem restauradas primeiro. Por exemplo, Oracle Cloud Infrastructure Object Storage tem uma classe de armazenamento de arquivos. Você precisa restaurar objetos nessa classe de armazenamento antes de DataSync poder transferi-los. Para obter mais informações, consulte a documentação do seu provedor de nuvem.

Tags de objetos

Nem todos os provedores de nuvem são compatíveis com tags de objetos. Os que permitem podem não permitir a consulta de tags por meio da API do Amazon S3. Em qualquer situação, sua tarefa DataSync de transferência pode falhar se você tentar copiar tags de objeto.

Você pode evitar isso desmarcando a caixa de seleção Copiar tags de objeto no DataSync console ao criar, iniciar ou atualizar sua tarefa.

Transferindo para o Amazon S3

Ao transferir para o Amazon S3 DataSync, não é possível transferir objetos maiores que 5 TB. DataSync também só pode copiar metadados de objetos de até 2 KB.

Criando seu DataSync agente

Um DataSync agente é necessário somente ao transferir dados entre sistemas de armazenamento em outras nuvens e o Amazon EFS ou Amazon FSx, ou ao usar tarefas do modo Básico. Você não precisa de um agente para transferir dados entre sistemas de armazenamento em outras nuvens e no Amazon S3 usando o modo Enhanced. Esta seção descreve como implantar e ativar um agente em uma EC2 instância da Amazon em sua nuvem privada virtual (VPC) em AWS.

Para criar um EC2 agente da Amazon

1. [Implante um EC2 agente da Amazon](#).
2. [Escolha um endpoint de serviço](#) que o agente use para se comunicar AWS.

Nessa situação, recomendamos o uso de um endpoint de serviço da VPC.

3. Configure sua rede para funcionar com [endpoints de serviço do VPC](#).
4. [Ative o atendente](#).

Criação de um local de transferência para outro armazenamento de objetos na nuvem

Você pode configurar DataSync para usar seu armazenamento de objetos na nuvem como local de origem ou destino.

Antes de começar

Verifique se você sabe [como DataSync acessa seu armazenamento de objetos na nuvem](#). Você também precisa de um [DataSync agente](#) que possa se conectar ao seu armazenamento de objetos na nuvem.

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e escolha Locais e Criar local.
3. Em Tipo de localização, escolha Armazenamento de objetos.
4. Em Servidor, insira o [endpoint](#) que DataSync pode ser usado para acessar seu armazenamento de objetos na nuvem:
 - Wasabi Cloud Storage – S3.*region*.wasabisys.com
 - DigitalOcean Spaces – *region*.digitaloceanspaces.com
 - Oracle Cloud Infrastructure Object Storage –
namespace.compat.objectstorage.*region*.oraclecloud.com
 - Cloudflare R2 Storage – *account-id*.r2.cloudflarestorage.com
 - Backblaze B2 Cloud Storage – S3.*region*.backblazeb2.com
 - NAVER Cloud Object Storage: *region*.object.ncloudstorage.com (maioria das regiões)
 - Alibaba Cloud Object Storage Service – *region*.aliyuncs.com
 - IBM Cloud Object Storage – s3.*region*.cloud-object-storage.appdomain.cloud
 - Seagate Lyve Cloud – s3.*region*.lyvecloud.seagate.com
5. Em Nome do bucket, insira o nome do bucket de armazenamento de objetos de ou para o qual você está transferindo dados.
6. Em Pasta, insira um prefixo de objeto. DataSync transfere somente objetos com esse prefixo.

7. Se sua transferência exigir um agente, escolha Usar agentes e escolha o DataSync agente que pode se conectar ao seu armazenamento de objetos na nuvem.
8. Expanda Configurações adicionais. Para Protocolo de servidor, escolha HTTPS. Em Porta do servidor, escolha 443.
9. Role para baixo até a seção Autenticação. Verifique se a caixa de seleção Exige credenciais está marcada e forneça DataSync suas [credenciais de armazenamento](#).
 - Em Chave de acesso, insira a ID para acessar seu armazenamento de objetos na nuvem.
 - Em Chave secreta, forneça a chave secreta para acessar seu armazenamento de objetos na nuvem. Você pode inserir a chave diretamente ou especificar um AWS Secrets Manager segredo que contenha a chave. Para obter mais informações, consulte [Fornecimento de credenciais para locais de armazenamento](#).
10. (Opcional) Forneça valores para os campos Chave e Valor para marcar o local.

As tags ajudam você a gerenciar, filtrar e pesquisar seus AWS recursos. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.
11. Escolha Criar local.

Próximas etapas

Depois de terminar de criar um DataSync local para seu armazenamento de objetos na nuvem, você poderá continuar configurando sua transferência. Veja aqui alguns dos próximos passos a considerar:

1. Se ainda não o fez, [crie outro local](#) para onde você planeja transferir seus dados de ou para dentro AWS.
2. Saiba como DataSync [lidar com metadados e arquivos especiais](#) para locais de armazenamento de objetos.
3. Configure como os dados são transferidos. Por exemplo, talvez você deseje [transferir apenas um subconjunto dos dados](#).

Important

Certifique-se de configurar como DataSync copia as tags de objeto corretamente. Para obter mais informações, consulte considerações com [tags de objetos](#).

4. [Inicie a transferência](#).

Transferindo de ou para um armazenamento compatível com S3 no Snowball Edge

Com AWS DataSync, você pode transferir objetos entre o [armazenamento compatível com o Amazon S3 em um AWS Snowball Edge](#) dispositivo ou cluster e qualquer um dos seguintes serviços de AWS armazenamento:

- [Amazon S3](#)
- [Amazon Elastic File System \(Amazon EFS\)](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)
- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Pré-requisitos

Antes de iniciar, faça o seguinte:

- Criou um recurso AWS de armazenamento na Região da AWS local de onde você planeja transferir dados de ou para. Por exemplo, isso pode ser um bucket do S3 ou um sistema de arquivos do Amazon EFS na região Leste dos EUA (Norte da Virgínia).
- Estabeleceu uma conexão de rede de longa distância (WAN) para o tráfego de entrada e saída do seu ambiente de armazenamento on-premises. Por exemplo, você pode estabelecer esse tipo de conexão com [AWS Direct Connect](#).

Ao [criar seu DataSync agente](#), você configurará essa conexão WAN para que DataSync possa transferir dados entre seu armazenamento compatível com Amazon S3 que está no local e seu recurso de armazenamento em. AWS

- Baixei e instalei o cliente [Snowball Edge](#).

Fornecendo DataSync acesso ao armazenamento compatível com S3

Para acessar seu bucket de armazenamento compatível com o Amazon S3, é DataSync necessário o seguinte:

- Credenciais de usuário no dispositivo ou cluster do Snowball Edge que podem acessar o bucket para o qual você está transferindo dados.
- Um certificado HTTPS que permite verificar DataSync a autenticidade da conexão entre o DataSync agente e o s3api endpoint em seu dispositivo ou cluster.

Tópicos

- [Obter as credenciais do usuário para acessar o bucket do S3](#)
- [Obter um certificado para a conexão de endpoint s3api](#)

Obter as credenciais do usuário para acessar o bucket do S3

DataSync precisa da chave de acesso e da chave secreta de um usuário que possa acessar o bucket com o qual você está trabalhando no seu dispositivo ou cluster do Snowball Edge.

Para obter as credenciais do usuário e acessar o bucket

1. Abra um terminal e execute o cliente Snowball Edge.

Para obter mais informações sobre a execução do cliente Snowball Edge, consulte [Usar o cliente Snowball Edge](#) no Guia do desenvolvedor AWS Snowball Edge .

2. Para obter as chaves de acesso associadas ao seu dispositivo ou cluster, execute o seguinte comando snowballEdge:

```
snowballEdge list-access-keys
```

3. Na saída, localize a chave de acesso do bucket com o qual DataSync funcionará (por exemplo, AKIAIOSFODNN7EXAMPLE).
4. Para obter a chave de acesso secreta, execute o comando snowballEdge a seguir. Substitua *access-key-for-datasync* pela chave de acesso que você localizou na etapa anterior.

```
snowballEdge get-secret-access-key --access-key-id access-key-for-datasync
```

A saída inclui a chave secreta correspondente à chave de acesso (por exemplo, wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY).

5. Salve a chave de acesso e a chave secreta em algum lugar que você possa lembrar.

Você precisará dessas chaves ao [configurar o local de DataSync origem da](#) sua transferência.

Obter um certificado para a conexão de endpoint **s3api**

Você precisa de um certificado HTTPS que possa verificar a autenticidade da conexão entre seu DataSync agente e um s3api endpoint em seu dispositivo ou cluster Snowball Edge.

Para obter um certificado para a conexão de endpoint **s3api**

1. No cliente do Snowball Edge, execute o seguinte comando `list-certificates`:

```
snowballEdge list-certificates
```

NA saída, anote o valor de `CertificateArn`. Esse é o nome do recurso da Amazon (ARN) do certificado. Você precisa do ARN para obter o conteúdo do certificado.

2. Execute o seguinte comando `get-certificate` que especifica o ARN do certificado que você acabou de recuperar:

```
snowballEdge get-certificate --certificate-arn arn:aws:snowball-  
device::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7
```

3. Copie a saída, incluindo as linhas `BEGIN CERTIFICATE` e `END CERTIFICATE`, e salve-a como um arquivo `.pem`.

Exemplo de saída de **get-certificate**:

```
-----BEGIN CERTIFICATE-----  
Certificate  
-----END CERTIFICATE-----
```

Você especifica esse `.pem` arquivo ao [criar o local de DataSync origem](#) para sua transferência.

Criação de um DataSync agente em seu ambiente de armazenamento local

Durante uma transferência, DataSync usa um [agente](#) para ler ou gravar no armazenamento compatível com o Amazon S3 em seu dispositivo ou cluster Snowball Edge.

Esse agente deve ser implantado no ambiente de armazenamento on-premises, onde ele pode se conectar ao seu dispositivo ou cluster por meio de sua rede. Por exemplo, você pode executar o agente em um VMware ESXi hipervisor que tenha acesso à rede local ao seu cluster.

Para criar um DataSync agente em seu ambiente de armazenamento local

1. Certifique-se de que o [DataSync agente possa ser executado em seu hipervisor](#) e que você [aloque recursos suficientes de máquina virtual \(VM\) para o agente](#).
2. Implantar o agente no ambiente on-premises.

Para obter instruções, consulte um dos tópicos a seguir dependendo do tipo de hipervisor no qual você está implantando o agente:

- [Implante seu agente em VMware](#)
- [Implantar o agente em uma máquina baseada em kernel Linux \(KVM\)](#)
- [Implantar o agente no Microsoft Hyper-V](#)
- [Implante seu agente na Amazon EC2](#)

 Warning

Não recomendamos a implantação de um agente no EC2 agente da Amazon para acessar o armazenamento local devido ao aumento da latência da rede.

3. Configure sua rede para permitir o seguinte tráfego entre o agente e o armazenamento compatível com o Amazon S3:

De	Para	Porta e protocolo
DataSync agente	Uma interface de rede virtual (VNI) para um endpoint <code>s3api</code> no dispositivo ou cluster. Se você tiver um cluster, ele pode ser qualquer VNI de endpoint <code>s3api</code> .	TCP 443 (HTTPS)

Se você precisa encontrar uma VNI no dispositivo ou cluster, consulte [descrever interfaces de rede virtual](#) no Snowball Edge.

4. [Escolha um endpoint de serviço](#) que o agente use para se comunicar com o DataSync serviço.
5. [Ative o agente](#).

Configurar o local de origem para sua transferência

Depois de criar seu agente, você pode configurar o local de origem da sua DataSync transferência.

Note

As instruções a seguir pressupõem que você está transferindo do armazenamento compatível com o Amazon S3, mas você também pode usar esse local como destino de transferência.

Para configurar o local de origem usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados. Selecione Criar e escolha Banco de dados.
3. Na página Configurar local de origem, selecione Criar um novo local.
4. Em Tipo de localização, escolha Armazenamento de objetos.
5. Para Agentes, escolha o DataSync agente que você criou em seu ambiente de armazenamento local.
6. Em Servidor, insira o VNI do endpoint `s3api` usado pelo armazenamento compatível com o Amazon S3.

Se você tiver um cluster do Snowball Edge em vez de um único dispositivo, poderá especificar qualquer endpoint do `s3api` cluster. VNIs

7. Em Nome do bucket, insira o bucket de armazenamento compatível com o Amazon S3 do qual você está transferindo objetos.
8. Em Pasta, insira um prefixo de objeto.

DataSync transfere somente objetos com esse prefixo.

9. Para configurar a DataSync conexão com o dispositivo ou cluster do Snowball Edge, expanda Configurações adicionais e faça o seguinte:

- a. Para Protocolo de servidor, escolha HTTPS.
- b. Em Porta do servidor, insira **443**.
- c. Em Certificado, escolha o arquivo de certificado para a [Conexão de endpoint s3api](#).

10. Selecione Requer credenciais e insira a Chave de acesso e a Chave secreta para [acessar o bucket de armazenamento compatível com o Amazon S3](#) no dispositivo ou cluster Snowball Edge.
11. Escolha Próximo.

Configurar o local de destino para sua transferência

O local de destino da sua transferência deve estar no mesmo Região da AWS local Conta da AWS em que você criou seu agente.

Antes de começar: verifique se você [configurou o local de origem](#) da sua transferência.

Para configurar o local de destino para sua transferência usando o DataSync console

1. Na página Configurar local de destino, escolha Criar um novo local ou Escolher um local existente para o recurso AWS de armazenamento para o qual você está transferindo objetos.

Se você estiver criando um novo local, consulte um dos seguintes tópicos:

- [Amazon S3](#)
- [Amazon EFS](#)
- [FSx para Windows File Server](#)
- [FSx para Lustre](#)
- [FSx para OpenZFS](#)
- [FSx para ONTAP](#)

2. Quando terminar de configurar o local de destino, escolha Avançar.

Definir as configurações de transferência

Com DataSync, você pode especificar um cronograma de transferência, personalizar como a integridade dos dados é verificada e especificar se deseja transferir somente um subconjunto de objetos, entre outras opções.

Antes de começar: verifique se você [configurou o local de origem](#) da sua transferência.

Para definir suas configurações de transferência usando o DataSync console

1. Na página Definir configurações, altere as configurações de transferência ou use os padrões.

Para ter mais informações sobre essas configurações, consulte [Escolhendo quais AWS DataSync transferências](#).

2. Escolha Próximo.
3. Revise os detalhes do seu caso e escolha Criar tarefa.

Iniciar sua transferência.

Depois de criar sua tarefa de transferência, você está pronto para começar a mover os dados. Para obter instruções sobre como iniciar uma tarefa usando o DataSync console ou AWS CLI, consulte [Iniciando sua tarefa](#).

Limitações

- Se seu sistema de armazenamento de origem usa o protocolo NFS (como o Amazon EFS), não é DataSync possível transferir arquivos com links físicos para um dispositivo Snowball Edge.
- DataSync não é possível transferir objetos com mais de 1.024 bytes de um dispositivo Snowball Edge para um bucket do S3. Para obter mais informações, consulte o [Guia do usuário do Amazon S3](#).

Criando uma tarefa para transferir seus dados

Uma tarefa descreve onde e como AWS DataSync transfere dados. Uma tarefa consiste no seguinte:

- [Local de origem](#) — O sistema ou serviço de armazenamento de onde os dados são DataSync transferidos.
- [Local de destino](#) — O sistema ou serviço de armazenamento para o qual os dados são DataSync transferidos.
- [Opções de tarefas](#) — configurações como quais arquivos transferir, como os dados são verificados, quando a tarefa é executada e muito mais.
- [Execuções de tarefas](#): quando você executa uma tarefa, ela é chamada de execução de tarefa.

Criação da tarefa do

Ao criar uma DataSync tarefa, você especifica seus locais de origem e destino. Você também pode personalizar a tarefa escolhendo quais arquivos transferir, como os metadados são tratados, configurando um agendamento etc.

Antes de criar sua tarefa, certifique-se de entender [como as DataSync transferências funcionam](#) e revise as [cotas da tarefa](#).

Important

Se você planeja transferir dados de ou para um local do Amazon S3, analise [como isso DataSync pode afetar as cobranças de suas solicitações do S3](#) e a [página de DataSync preços](#) antes de começar.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. Verifique se você está em um das Regiões da AWS locais onde planeja transferir dados.
3. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
4. Na página Configurar local de origem, [crie](#) ou escolha um local de origem e depois escolha Avançar.
5. Na página Configurar local de destino, [crie](#) ou escolha um local de destino e depois escolha Avançar.
6. (Recomendado) Na página Definir configurações, dê à sua tarefa um nome de que você possa se lembrar.
7. Ainda na página Definir configurações, escolha as opções de tarefa ou use as configurações padrão.

Talvez você se interesse por algumas das seguintes opções:

- Especifique o [modo de tarefa](#) que você deseja usar.
- Especifique quais dados transferir usando um [manifesto](#) ou [filtros](#).
- Configure como [lidar com metadados de arquivos](#) e [verificar a integridade dos dados](#).

- Monitore sua transferência com [relatórios de tarefas](#) ou com a [Amazon CloudWatch](#). Recomendamos configurar algum tipo de monitoramento para a tarefa.

Quando concluir, selecione Próximo.

8. Revise a configuração da tarefa e escolha Criar tarefa.

Você está pronto para [iniciar a tarefa](#).

Usando o AWS CLI

Depois de [criar seus locais de DataSync origem e destino](#), você pode criar sua tarefa.

1. Nas suas AWS CLI configurações, verifique se você está usando um dos Regiões da AWS locais para onde planeja transferir dados.
2. Copie o seguinte comando create-task:

```
aws datasync create-task \
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --name "task-name"
```

3. Em --source-location-arn, especifique o nome do recurso da Amazon (ARN) do local de origem na transferência.
4. Em --destination-location-arn, especifique o ARN do local de destino.

Se você estiver transferindo entre Regiões da AWS nossas contas, certifique-se de que o ARN inclua a outra ID de região ou conta.

5. (Recomendado) Em --name, especifique um nome para a tarefa de que você possa se lembrar.
6. Especifique outras opções de tarefa conforme necessário. Talvez você esteja interessado em algumas das seguintes opções:
 - Especifique quais dados transferir usando um [manifesto](#) ou [filtros](#).
 - Configure como [lidar com metadados de arquivos](#) e [verificar a integridade dos dados](#).
 - Monitore sua transferência com [relatórios de tarefas](#) ou com a [Amazon CloudWatch](#). Recomendamos configurar algum tipo de monitoramento para a tarefa.

Para obter mais opções, consulte [create-task](#). Aqui está um exemplo do comando create-task que especifica várias opções:

```
aws datasync create-task \
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --cloud-watch-log-group-arn "arn:aws:logs:region:account-id" \
  --name "task-name" \
  --options
VerifyMode=NONE,OverwriteMode=NEVER,Atime=BEST_EFFORT,Mtime=PRESERVE,Uid=INT_VALUE,Gid=INT
```

7. Execute o comando create-task.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN da tarefa que você criou. Por exemplo:

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/task-08de6e6697796f026"
}
```

Você está pronto para [iniciar a tarefa](#).

Status da tarefa

Ao criar uma DataSync tarefa, você pode verificar seu status para ver se ela está pronta para ser executada.

Status do console	Status da API	Descrição
Available (Disponível)	AVAILABLE	A tarefa está pronta para começar a transferir dados.

Status do console	Status da API	Descrição
Em execução	RUNNING	A execução de uma tarefa está em andamento. Para obter mais informações, consulte Status de execução de tarefa .
Unavailable (Indisponível)	UNAVAILABLE	Um DataSync agente usado pela tarefa está off-line. Para obter mais informações, consulte O que eu faço se meu agente estiver off-line? .
Enfileirado	QUEUED	Outra execução de tarefa que usa o mesmo DataSync agente está em andamento. Para obter mais informações, consulte Como saber quando a tarefa está na fila .

Particionamento de grandes conjuntos de dados com várias tarefas

Se você estiver transferindo um grande conjunto de dados, como [migrar](#) milhões de arquivos ou objetos, recomendamos particionar seu conjunto de dados com várias tarefas. DataSync Particionar seus dados de origem em várias tarefas (e possivelmente em [agentes](#), dependendo de suas localizações) ajuda a reduzir o tempo necessário DataSync para preparar e transferir seus dados.

Considere algumas das maneiras pelas quais você pode particionar um grande conjunto de dados em várias DataSync tarefas:

- Crie tarefas que transfiram pastas separadas. Por exemplo, você pode criar duas tarefas que tenham como destino `/FolderA` e `/FolderB`, respectivamente, em seu armazenamento de origem.
- Crie tarefas que transfiram subconjuntos de arquivos, objetos e pastas usando um [manifesto](#) ou [filtros](#).

Lembre-se de que essa abordagem pode aumentar I/O as operações no armazenamento e afetar a largura de banda da rede. Para obter mais informações, consulte o blog sobre [Como acelerar suas transferências de dados com arquiteturas DataSync escaláveis](#).

Segmentação de dados transferidos com várias tarefas

Se estiver transferindo conjuntos diferentes de dados para o mesmo destino, você poderá criar várias tarefas para ajudar a segmentar os dados que serão transferidos.

Por exemplo, se você estiver transferindo para o mesmo bucket do S3 denominado MyBucket, poderá criar prefixos diferentes no bucket que correspondam a cada tarefa. Essa abordagem evita conflitos de nomes de arquivos nos conjuntos de dados e permite que você defina permissões diferentes para cada prefixo. Veja como você pode configurar isso:

1. Crie três prefixos no destino MyBucket denominados task1, task2 e task3:
 - s3://MyBucket/task1
 - s3://MyBucket/task2
 - s3://MyBucket/task3
2. Crie três DataSync tarefas chamadas task1, task2, e task3 que sejam transferidas para o prefixo correspondente em MyBucket.

Escolhendo um modo de tarefa para sua transferência de dados

Sua AWS DataSync tarefa pode ser executada em um dos seguintes modos:

- Modo aprimorado — transfira um número praticamente ilimitado de objetos com desempenho superior ao do modo Básico. As tarefas do modo aprimorado otimizam o processo de transferência de dados listando, preparando, transferindo e verificando os dados em paralelo. Atualmente, o modo aprimorado está disponível para transferências entre locais do Amazon S3, transferências entre Azure Blob e o Amazon S3 sem um agente e transferências entre outras nuvens e o Amazon S3 sem um agente.
- Modo básico — Transfira arquivos ou objetos entre o AWS armazenamento e todos os outros DataSync locais compatíveis. As tarefas do modo básico estão sujeitas a [cotas](#) no número de arquivos, objetos e diretórios em um conjunto de dados. O modo básico prepara, transfere e verifica os dados sequencialmente, tornando-o mais lento do que o modo Avançado para a maioria das cargas de trabalho.

Entendendo as diferenças do modo de tarefa

As informações a seguir podem ajudá-lo a determinar qual modo de tarefa usar.

Recurso	Comportamento do modo aprimorado	Comportamento do modo básico
Desempenho	DataSync lista, prepara, transfere e verifica seus dados paralelamente. Oferece maior desempenho do que o modo Básico para a maioria das cargas de trabalho (como a transferência de objetos grandes)	DataSync prepara, transfere e verifica seus dados sequencialmente. O desempenho é mais lento do que o modo Avançado para a maioria das cargas de trabalho
Número de itens em um conjunto de dados que DataSync podem funcionar por execução de tarefa	Número virtualmente ilimitado de objetos	As cotas se aplicam
Contadores e métricas de transferência de dados	Mais contadores e métricas do que o modo Básico, como o número de objetos DataSync encontrados no local de origem e quantos objetos são preparados durante a execução de cada tarefa	Menos contadores e métricas do que o modo Avançado
Registro em log	Registros estruturados (formato JSON)	Registros não estruturados
Localizações suportadas	Atualmente, para transferências entre locais do Amazon S3, transferências entre Azure Blob e o Amazon S3 sem um agente e transferências entre outras nuvens e o Amazon S3 sem um agente.	Para transferências entre todos os locais que oferecem DataSync suporte

Recurso	Comportamento do modo aprimorado	Comportamento do modo básico
Opções de verificação de dados	DataSync verifica somente os dados transferidos	DataSync verifica todos os dados por padrão
Limites de largura de banda	Não aplicável	Compatível
Custo	Para obter mais informações, consulte a página DataSync de preços	Para obter mais informações, consulte a página DataSync de preços
Tratamento de falhas para tags de objeto não suportadas	Para transferências de armazenamento em nuvem de ou para locais que não oferecem suporte à marcação de objetos, a execução da tarefa falhará imediatamente se a ObjectTags opção não for especificada ou definida como. PRESERVE	Para transferências de armazenamento em nuvem de ou para locais que não oferecem suporte à marcação de objetos, a execução da tarefa será executada normalmente, mas relatará falhas por objeto para objetos marcados se a ObjectTags opção não for especificada ou definida como. PRESERVE

Escolhendo um modo de tarefa

Você pode escolher o modo Avançado somente para transferências entre locais do Amazon S3, transferências entre Azure Blob e o Amazon S3 sem um agente e transferências entre outras nuvens e o Amazon S3 sem um agente. Caso contrário, você deve usar o modo Básico. Por exemplo, uma transferência de um local [NFS local para um local](#) do S3 requer o modo Básico.

As opções de tarefas e o desempenho podem variar dependendo do modo de tarefa escolhido. Depois de criar sua tarefa, você não poderá alterar o modo da tarefa.

Permissões obrigatórias

Para criar uma tarefa no modo Avançado, a função do IAM DataSync com a qual você está usando precisa ter a `iam:CreateServiceLinkedRole` permissão.

Para obter suas permissões de DataSync usuário, considere usar [AWSDataSyncFullAccess](#). Essa é uma política AWS gerenciada que fornece ao usuário acesso total DataSync e acesso mínimo às suas dependências.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

4. Para o modo Tarefa, escolha uma das seguintes opções:
 - Aprimorado
 - Básico

Para obter mais informações, consulte [Entendendo as diferenças do modo de tarefa](#).

5. Ainda na página Definir configurações, escolha outras opções de tarefa ou use as configurações padrão.

Talvez você esteja interessado em algumas das seguintes opções:

- Especifique quais dados transferir usando um [manifesto](#) ou [filtros](#).
- Configure como [lidar com metadados de arquivos](#) e [verificar a integridade dos dados](#).
- Monitore sua transferência com [relatórios de tarefas](#) ou [Amazon CloudWatch Logs](#).

Quando concluir, selecione Próximo.

6. Revise a configuração da tarefa e escolha Criar tarefa.

Usando o AWS CLI

1. Nas suas AWS CLI configurações, verifique se você está usando um dos Regiões da AWS locais para onde planeja transferir dados.

2. Copie o seguinte comando create-task:

```
aws datasync create-task \  
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --task-mode "ENHANCED-or-BASIC"
```

3. Em `--source-location-arn`, especifique o nome do recurso da Amazon (ARN) do local de origem na transferência.
4. Em `--destination-location-arn`, especifique o ARN do local de destino.

Se você estiver transferindo entre Regiões da AWS nossas contas, verifique se o ARN inclui a outra ID de região ou conta.

5. Para `--task-mode`, especifique ENHANCED ou BASIC.

Para obter mais informações, consulte [Entendendo as diferenças do modo de tarefa](#).

6. Especifique outras opções de tarefa conforme necessário. Talvez você esteja interessado em algumas das seguintes opções:
 - Especifique quais dados transferir usando um [manifesto](#) ou [filtros](#).
 - Configure como [lidar com metadados de arquivos](#) e [verificar a integridade dos dados](#).
 - Monitore sua transferência com [relatórios de tarefas](#) ou [Amazon CloudWatch Logs](#).

Para obter mais opções, consulte [create-task](#). Aqui está um exemplo de create-task comando que especifica o modo Avançado e várias outras opções:

```
aws datasync create-task \  
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \  
  --name "task-name" \  
  --task-mode "ENHANCED" \  
  --options  
  TransferMode=CHANGED,VerifyMode=ONLY_FILES_TRANSFERRED,ObjectTags=PRESERVE,LogLevel=TRANSF
```

7. Execute o comando create-task.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN da tarefa que você criou. Por exemplo:

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Usando a DataSync API

Você pode especificar o modo de DataSync tarefa configurando o TaskMode parâmetro na [CreateTask](#) operação.

Escolhendo quais AWS DataSync transferências

AWS DataSync permite que você escolha o que transferir e como deseja que seus dados sejam tratados. Algumas opções incluem:

- Transferir uma lista exata dos arquivos ou objetos usando um manifesto.
- Incluir ou excluir certos tipos de dados na transferência usando um filtro.
- Para transferências recorrentes, mova apenas os dados que foram alterados desde a última transferência
- Substituir os dados no local de destino para correspondam ao que existe no local de origem.
- Escolher quais metadados de arquivo ou objeto preservar entre seus locais de armazenamento.

Tópicos

- [Transferência de arquivos ou objetos específicos usando um manifesto](#)
- [Transferência de arquivos, objetos e pastas específicos usando filtros](#)
- [Entendendo como DataSync manipula metadados de arquivos e objetos](#)
- [Links e diretórios copiados pelo AWS DataSync](#)
- [Configuração de como lidar com arquivos, objetos e metadados](#)

Transferência de arquivos ou objetos específicos usando um manifesto

Um manifesto é uma lista de arquivos ou objetos que você AWS DataSync deseja transferir. Por exemplo, em vez de precisar transferir tudo em um bucket do S3 com potencialmente milhões de objetos, DataSync transfere somente os objetos que você lista em seu manifesto.

Os manifestos são semelhantes aos [filtros](#), mas permitem identificar exatamente quais arquivos ou objetos transferir em vez de dados que correspondem a um padrão de filtro.

Criação do manifesto

Um manifesto é um arquivo formatado em valores separados por vírgula (CSV) que lista os arquivos ou objetos no local de origem que você deseja transferir. DataSync Se a origem for um bucket do S3, você também poderá incluir qual versão de um objeto transferir.

Tópicos

- [Diretrizes](#)
- [Exemplos de manifesto](#)

Diretrizes

Use essas diretrizes para ajudá-lo a criar um manifesto que funcione com DataSync.

Do

- Especifique o caminho completo de cada arquivo ou objeto que você deseja transferir.

Você não pode especificar apenas um diretório ou uma pasta com a intenção de transferir todo o seu conteúdo. Para essas situações, considere usar um [filtro de inclusão](#) em vez de um manifesto.

- Certifique-se de que cada caminho de arquivo ou objeto seja relativo ao caminho de montagem, pasta, diretório ou prefixo que você especificou ao configurar seu local de DataSync origem.

Por exemplo, digamos que você [configure um local do S3](#) com um prefixo denominado photos. Esse prefixo inclui um objeto `my-picture.png` que você deseja transferir. No manifesto, você só precisa especificar o objeto (`my-picture.png`) em vez de especificar o prefixo e o objeto (`photos/my-picture.png`).

- Para especificar a versão do objeto Amazon S3 IDs, separe o caminho do objeto e o ID da versão usando uma vírgula.

O exemplo a seguir mostra uma entrada de manifesto com dois campos. O primeiro campo inclui um objeto denominado `picture1.png`. O segundo campo é separado por vírgula e inclui um ID de versão de `111111`:

```
picture1.png,111111
```

- Use aspas nas seguintes situações:
 - Quando um caminho contiver caracteres especiais (vírgulas, aspas e fins de linha):

```
"filename,with,commas.txt"
```

- Quando um caminho se estender por várias linhas:

```
"this  
is  
a  
filename.txt"
```

- Quando um caminho incluir aspas:

```
filename""with""quotes.txt
```

Isso representa um caminho denominado `filename"with"quotes.txt`.

Essas regras de aspas também se aplicam aos campos de ID de versão. Em geral, se um campo de manifesto tiver aspas, você deverá usar outras aspas como caractere de escape.

- Separe cada entrada de arquivo ou objeto com uma nova linha.

Você pode separar as linhas usando quebras de linha no estilo do Linux (alimentação de linha ou retorno de carro) ou do Windows (retorno de carro seguido por uma alimentação de linha).

- Salve o manifesto (por exemplo, `my-manifest.csv` ou `my-manifest.txt`).
- Faça upload do manifesto em um bucket do S3 que [DataSync possa ser acessado](#).

Esse bucket não precisa estar na mesma conta Região da AWS ou na mesma conta em que você está usando DataSync.

Don't

- Especifique apenas um diretório ou uma pasta com a intenção de transferir todo o seu conteúdo.

Um manifesto pode incluir somente caminhos completos para os arquivos ou os objetos que você deseja transferir. Se você configurar o local de origem para usar um caminho de montagem, pasta, diretório ou prefixo específico, não precisará incluí-lo em seu manifesto.

- Especifique um caminho de arquivo ou objeto que exceda 4.096 caracteres.
- Especifique um caminho de arquivo, caminho de objeto ou ID de versão de objeto Amazon S3 que exceda 1.024 bytes.
- Especifique caminhos duplicados de arquivos ou objetos.
- Inclua um ID de versão do objeto se o local de origem não for um bucket do S3.
- Inclua mais de dois campos em uma entrada de manifesto.

Uma entrada só pode incluir um caminho de arquivo ou objeto e (se aplicável) um ID de versão de objeto Amazon S3.

- Inclua caracteres que não estejam em conformidade com a codificação UTF-8.
- Inclua espaços não intencionais em seus campos de entrada fora das aspas.

Exemplos de manifesto

Use esses exemplos para ajudá-lo a criar um manifesto que funcione com DataSync o.

Manifesto com caminhos completos de arquivos ou objetos

O exemplo a seguir mostra um manifesto com caminhos completos dos arquivos ou objetos para transferir.

```
photos/picture1.png
photos/picture2.png
photos/picture3.png
```

Manifesto somente com chaves de objeto

O exemplo a seguir mostra um manifesto com objetos a serem transferidos de um local de origem do Amazon S3. Como o [local é configurado](#) com o prefixo photos, apenas as chaves do objeto são especificadas.

```
picture1.png  
picture2.png  
picture3.png
```

Manifesto com caminhos e versão do objeto IDs

As duas primeiras entradas no exemplo de manifesto a seguir incluem as versões específicas de objetos do Amazon S3 a serem transferidas.

```
photos/picture1.png,111111  
photos/picture2.png,121212  
photos/picture3.png
```

Manifesto com caracteres UTF-8

O exemplo a seguir mostra um manifesto com arquivos que incluem caracteres UTF-8.

```
documents/résumé1.pdf  
documents/résumé2.pdf  
documents/résumé3.pdf
```

Fornecendo DataSync acesso ao seu manifesto

Você precisa de uma função AWS Identity and Access Management (IAM) que dê DataSync acesso ao seu manifesto em seu bucket do S3. Esse perfil inclui as seguintes permissões:

- `s3:GetObject`
- `s3:GetObjectVersion`

Você pode gerar essa função automaticamente no DataSync console ou criar a função você mesmo.

Note

Se seu manifesto estiver em um outro Conta da AWS, você deverá criar essa função manualmente.

Criação automática de um perfil do IAM

Ao criar ou iniciar uma tarefa de transferência no console, DataSync pode criar uma função do IAM para você com `s3:GetObject` as `s3:GetObjectVersion` permissões necessárias para acessar seu manifesto.

Permissões necessárias para criar automaticamente o perfil

Para criar automaticamente a função, certifique-se de que a função que você está usando para acessar o DataSync console tenha as seguintes permissões:

- `iam:CreateRole`
- `iam:CreatePolicy`
- `iam:AttachRolePolicy`

Criação do perfil do IAM (mesma conta)

Você pode criar manualmente a função do IAM que DataSync precisa acessar seu manifesto. As instruções a seguir pressupõem que você esteja no mesmo Conta da AWS local em que usa DataSync e que o bucket S3 do seu manifesto esteja localizado.

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação esquerdo, em Gerenciamento de acesso, escolha Perfis e, em seguida, escolha Criar perfil.
3. Na página Selecionar entidade confiável, para Tipo de entidade confiável, escolha AWS service (Serviço da AWS).
4. Em Caso de uso, escolha DataSyncna lista suspensa e selecione. DataSync Escolha Próximo.
5. Na página Adicionar permissões, escolha Próximo. Forneça um nome ao perfil e escolha Criar perfil.
6. Na página Perfis, procure o perfil que você acabou de criar e escolha seu nome.
7. Na página do perfil, escolha a guia Permissões. Selecione Adicionar permissões e, em seguida, Criar política em linha.
8. Escolha a guia JSON e cole o seguinte exemplo de política no editor de políticas:

JSON

```
{
```

```

    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DataSyncAccessManifest",
        "Effect": "Allow",
        "Action": [
            "s3:GetObject",
            "s3:GetObjectVersion"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/my-manifest.csv"
    }]
}

```

9. No exemplo de política que você acabou de colar, substitua os seguintes valores pelos seus:
 - a. Substitua *amzn-s3-demo-bucket* pelo nome do bucket do S3 que está hospedando o manifesto.
 - b. Substitua *my-manifest.csv* pelo nome do arquivo do manifesto.
10. Escolha Próximo. Digite um nome para a política e escolha Criar política.
11. (Recomendado) Para evitar o [problema “confused deputy” entre serviços](#), faça o seguinte:
 - a. Na página Detalhes do perfil, escolha a guia Relações de confiança. Escolha Editar política de confiança.
 - b. Atualize a política de confiança usando o exemplo a seguir, que inclui as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount`:

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Service": "datasync.amazonaws.com"
        },
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "account-id"
            },
            "StringLike": {

```

```
    "aws:SourceArn": "arn:aws:datasync:region:account-id:"  
  }  
}  
}]  
}
```

- Substitua cada instância **account-id** pelo Conta da AWS ID em que você está usando DataSync.
 - **region** Substitua pelo Região da AWS local em que você está usando DataSync.
- c. Escolha Atualizar política.

Você criou uma função do IAM que permite DataSync acessar seu manifesto. Especifique esse perfil ao [criar](#) ou [iniciar](#) a tarefa.

Criação do perfil do IAM (outra conta)

Se seu manifesto estiver em um bucket do S3 que pertença a outro Conta da AWS, você deverá criar manualmente a função do IAM DataSync usada para acessar o manifesto. Em seguida, no Conta da AWS local em que seu manifesto está localizado, você precisa incluir a função na política de bucket do S3.

Criar a função

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação esquerdo, em Gerenciamento de acesso, escolha Perfis e, em seguida, escolha Criar perfil.
3. Na página Selecionar entidade confiável, para Tipo de entidade confiável, escolha AWS service (Serviço da AWS).
4. Em Caso de uso, escolha DataSync na lista suspensa e selecione. DataSync Escolha Próximo.
5. Na página Adicionar permissões, escolha Próximo. Forneça um nome ao perfil e escolha Criar perfil.
6. Na página Perfis, procure o perfil que você acabou de criar e escolha seu nome.
7. Na página do perfil, escolha a guia Permissões. Selecione Adicionar permissões e, em seguida, Criar política em linha.
8. Escolha a guia JSON e cole o seguinte exemplo de política no editor de políticas:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DataSyncAccessManifest",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/my-manifest.csv"
  }]
}
```

9. No exemplo de política que você acabou de colar, substitua os seguintes valores pelos seus:
 - a. Substitua *amzn-s3-demo-bucket* pelo nome do bucket do S3 que está hospedando o manifesto.
 - b. Substitua *my-manifest.csv* pelo nome do arquivo do manifesto.
10. Escolha Próximo. Digite um nome para a política e escolha Criar política.
11. (Recomendado) Para evitar o [problema “confused deputy” entre serviços](#), faça o seguinte:
 - a. Na página Detalhes do perfil, escolha a guia Relações de confiança. Escolha Editar política de confiança.
 - b. Atualize a política de confiança usando o exemplo a seguir, que inclui as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount`:

JSON

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



```

        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "account-id"
            },
            "StringLike": {
                "aws:SourceArn": "arn:aws:datasync:region:account-id:*"
            }
        }
    }
}

```

- Substitua cada instância do *account-id* pelo Conta da AWS ID em que você está usando DataSync.
 - *region* Substitua pelo Região da AWS local em que você está usando DataSync.
- c. Escolha Atualizar política.

Você criou o perfil do IAM que pode incluir na política de bucket do S3.

Atualização da política de bucket do S3 com o perfil

Depois de criar a função do IAM, você deve adicioná-la à política de bucket do S3 no outro Conta da AWS local em que seu manifesto está localizado.

1. No AWS Management Console, mude para a conta com o bucket S3 do seu manifesto.
2. Abra o console do Amazon S3 em <https://console.aws.amazon.com/s3/>.
3. Na página do perfil, escolha a guia Permissões.
4. Em Política de bucket, escolha Editar e faça o seguinte para modificar sua política de bucket do S3:
 - a. Atualize o que está no editor para incluir as seguintes declarações de política:

```

{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "DataSyncAccessManifestBucket",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:role/datasync-role"
      }
    }
  ]
}

```

```
    },
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
  }
]
```

- b. **account-id** Substitua pelo Conta da AWS ID da conta DataSync com a qual você está usando.
 - c. **datasync-role** Substitua pela função do IAM que você acabou de criar e que DataSync permite acessar seu manifesto.
 - d. Substitua **amzn-s3-demo-bucket** pelo nome do bucket do S3 que está hospedando o manifesto na outra Conta da AWS.
5. Escolha Salvar alterações.

Você criou uma função do IAM que permite DataSync acessar seu manifesto na outra conta. Especifique esse perfil ao [criar](#) ou [iniciar](#) a tarefa.

Especificação do manifesto ao criar uma tarefa

Você pode especificar o manifesto que DataSync deseja usar ao criar uma tarefa.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, escolha Tarefas e depois escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

4. Em Conteúdo a ser varrido, escolha Arquivos, objetos e pastas específicos e selecione Usando um manifesto.
5. Em URI do S3, escolha seu manifesto hospedado em um bucket do S3.

Outra opção é inserir o URI (por exemplo, `s3://bucket/prefix/my-manifest.csv`).

6. Em Versão do objeto, escolha a versão do manifesto que você DataSync deseja usar.

Por padrão, DataSync usa a versão mais recente do objeto.

7. Em Perfil de acesso ao manifesto, faça uma das seguintes alternativas:
 - Escolha Autogenerate DataSync para criar automaticamente uma função do IAM com as permissões necessárias para acessar seu manifesto em seu bucket do S3.
 - Escolha um perfil do IAM existente que possa acessar o manifesto.

Para obter mais informações, consulte [Fornecendo DataSync acesso ao seu manifesto](#).

8. Defina todas as outras configurações de tarefa necessárias e escolha Avançar.
9. Escolha Criar tarefa.

Usando o AWS CLI

1. Copie o seguinte comando create-task:

```
aws datasync create-task \  
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/  
loc-12345678abcdefgh \\  
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/loc-  
abcdefgh12345678 \  
  --manifest-config {  
    "Source": {  
      "S3": {  
        "ManifestObjectPath": "s3-object-key-of-manifest",  
        "BucketAccessRoleArn": "bucket-iam-role",  
        "S3BucketArn": "amzn-s3-demo-bucket-arn",  
        "ManifestObjectVersionId": "manifest-version-to-use"  
      }  
    }  
  }
```

2. No parâmetro --source-location-arn, especifique o nome do recurso da Amazon (ARN) do local de onde você está transferindo os dados.
3. No parâmetro --destination-location-arn, especifique o ARN do local para onde você está transferindo os dados.
4. No parâmetro --manifest-config faça o seguinte:
 - ManifestObjectPath: especifique a chave de objeto do S3 do manifesto.

- `BucketAccessRoleArn`— Especifique a função do IAM que permite DataSync acessar seu manifesto em seu bucket do S3.

Para obter mais informações, consulte [Fornecendo DataSync acesso ao seu manifesto](#).

- `S3BucketArn`: especifique o ARN do bucket do S3 que está hospedando o manifesto.
- `ManifestObjectVersionId`— Especifique a versão do manifesto que você DataSync deseja usar.

Por padrão, DataSync usa a versão mais recente do objeto.

5. Execute o comando `create-task` para criar sua tarefa.

Quando tudo estiver pronto, você poderá [iniciar a tarefa de transferência](#).

Especificação do manifesto ao iniciar uma tarefa

Você pode especificar o manifesto que DataSync deseja usar ao executar uma tarefa.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação da esquerda, escolha Tarefas e depois a tarefa que você deseja iniciar.
3. Na página de visão geral da tarefa, escolha Iniciar e depois Iniciar com opções de substituição.
4. Em Conteúdo a ser varrido, escolha Arquivos, objetos e pastas específicas e selecione Usando um manifesto.
5. Em URI do S3, escolha seu manifesto hospedado em um bucket do S3.

Outra opção é inserir o URI (por exemplo, `s3://bucket/prefix/my-manifest.csv`).

6. Em Versão do objeto, escolha a versão do manifesto que você DataSync deseja usar.

Por padrão, DataSync usa a versão mais recente do objeto.

7. Em Perfil de acesso ao manifesto, faça uma das seguintes alternativas:
 - Escolha Autogenerate DataSync para criar automaticamente uma função do IAM para acessar seu manifesto em seu bucket do S3.
 - Escolha um perfil do IAM existente que possa acessar o manifesto.

Para obter mais informações, consulte [Fornecendo DataSync acesso ao seu manifesto](#).

8. Escolha Iniciar para começar a transferência.

Usando o AWS CLI

1. Copie o seguinte comando `start-task-execution`:

```
aws datasync start-task-execution \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh \
  --manifest-config {
    "Source": {
      "S3": {
        "ManifestObjectPath": "s3-object-key-of-manifest",
        "BucketAccessRoleArn": "bucket-iam-role",
        "S3BucketArn": "amzn-s3-demo-bucket-arn",
        "ManifestObjectVersionId": "manifest-version-to-use"
      }
    }
  }
```

2. No parâmetro `--task-arn`, especifique o nome do recurso da Amazon (ARN) da tarefa que você está iniciando.
3. No parâmetro `--manifest-config` faça o seguinte:
 - `ManifestObjectPath`: especifique a chave de objeto do S3 do manifesto.
 - `BucketAccessRoleArn`— Especifique a função do IAM que permite DataSync acessar seu manifesto em seu bucket do S3.

Para obter mais informações, consulte [Fornecendo DataSync acesso ao seu manifesto](#).

- `S3BucketArn`: especifique o ARN do bucket do S3 que está hospedando o manifesto.
- `ManifestObjectVersionId`— Especifique a versão do manifesto que você DataSync deseja usar.

Por padrão, DataSync usa a versão mais recente do objeto.

4. Execute o comando `start-task-execution` para iniciar a transferência.

Limitações

- Você não pode usar um manifesto junto com [filtros](#).
- Você não pode especificar apenas um diretório ou uma pasta com a intenção de transferir todo o seu conteúdo. Para essas situações, considere usar um [filtro de inclusão](#) em vez de um manifesto.
- Você não pode usar a opção de tarefa Manter arquivos excluídos (`PreserveDeletedFilesna API`) para [manter arquivos ou objetos no destino que não estejam na origem](#). DataSync transfere apenas o que está listado no seu manifesto e não exclui nada no destino.

Solução de problemas

Se você estiver transferindo objetos com uma versão específica IDs de um bucket do S3, talvez veja um erro relacionado a `HeadObject` ou `GetObjectTagging`. Por exemplo, aqui está um erro relacionado a `GetObjectTagging`:

```
[WARN] Failed to read metadata for file /picture1.png (versionId: 111111): S3 Get
Object Tagging Failed
[ERROR] S3 Exception: op=GetObjectTagging photos/picture1.png, code=403, type=15,
exception=AccessDenied,
msg=Access Denied req-hdrs: content-type=application/xml, x-amz-api-version=2006-03-01
rsp-hdrs: content-type=application/xml,
date=Wed, 07 Feb 2024 20:16:14 GMT, server=AmazonS3, transfer-encoding=chunked,
x-amz-id-2=IOWQ4fDEXAMPLEQM+ey7N9WgVhSnQ6JEXAMPLEZb7hSQDASK+Jd1vEXAMPLEa3Km, x-amz-
request-id=79104EXAMPLEB723
```

Se você ver algum desses erros, valide se a função do IAM DataSync usada para acessar seu local de origem do S3 tem as seguintes permissões:

- `s3:GetObjectVersion`
- `s3:GetObjectVersionTagging`

Se você precisar atualizar o perfil com essas permissões, consulte [Criação de uma função do IAM DataSync para acessar sua localização no Amazon S3](#).

Próximas etapas

Se ainda não o fez, [inicie a tarefa](#). Do contrário, [monitore as atividades da tarefa](#).

Transferência de arquivos, objetos e pastas específicos usando filtros

AWS DataSync permite aplicar filtros para incluir ou excluir dados do local de origem em uma transferência. Por exemplo, se você não quiser transferir arquivos temporários que terminem com `.tmp`, poderá criar um filtro de exclusão para que esses arquivos não vão para o local de destino.

Você pode usar uma combinação de filtros de exclusão e inclusão na mesma tarefa de transferência. Se você modificar os filtros de uma tarefa, essas alterações serão aplicadas a próxima vez que você executar a tarefa.

Filtrar termos, definições e sintaxe

Familiarize-se com os conceitos relacionados à DataSync filtragem:

Filtro

A string completa que representa um filtro específico (por exemplo, `*.tmp | *.temp` ou `/folderA|/folderB`).

Filtros são compostos por padrões delimitados por uma barra vertical (`|`). Você não precisa de um delimitador ao adicionar padrões no DataSync console porque adiciona cada padrão separadamente.

Note

Os filtros diferenciam maiúsculas de minúsculas. Por exemplo, o filtro `/folderA` não corresponderá a `/FolderA`.

Padrão

Um padrão dentro de um filtro. Por exemplo, `*.tmp` é um padrão que faz parte do filtro `*.tmp | *.temp`. Se o filtro tiver vários padrões, você delimitará cada padrão usando uma barra vertical (`|`).

Pastas

- Todos os filtros se referem ao caminho do local de origem. Por exemplo, suponha que você especifica `/my_source/` como o caminho de origem ao criar a tarefa e o local de origem e especifica o filtro de inclusão `/transfer_this/`. Nesse caso, DataSync transfere somente o diretório `/my_source/transfer_this/` e seu conteúdo.

- Para especificar uma pasta diretamente sob o local de origem, inclua uma barra (/) na frente do nome da pasta. No exemplo anterior, o padrão usa `/transfer_this`, e não `transfer_this`.
- DataSync interpreta os padrões a seguir da mesma forma e combina a pasta e seu conteúdo.

`/dir`

`/dir/`

- Quando você está transferindo dados de ou para um bucket do Amazon S3 DataSync, trata `/` o caractere na chave do objeto como o equivalente a uma pasta em um sistema de arquivos.

Caracteres especiais

Veja a seguir caracteres especiais para usar com a filtragem.

Caractere especial	Descrição
* (curinga)	Um caractere usado para corresponder a zero ou mais caracteres. Por exemplo, <code>/movies_folder*</code> corresponde a <code>/movies_folder</code> e <code>/movies_folder1</code> .
(barra vertical)	Um caractere usado como um delimitador entre padrões. Permite especificar vários padrões, em que qualquer um deles pode corresponder ao filtro. Por exemplo, <code>*.tmp *.temp</code> corresponde a arquivos que terminam com <code>tmp</code> ou <code>temp</code>.  Note Este delimitador não é necessário ao adicionar padrões no console, pois você adiciona cada padrão em uma linha separada.
\ (barra invertida)	Um caractere usado para caracteres especiais de escape (*, , \) no nome de um arquivo ou objeto. Uma dupla barra invertida (\\) é necessária quando uma barra invertida fizer parte do nome de um arquivo. Da mesma

Caractere especial	Descrição
	forma, \\ \\ representa duas barras invertidas consecutivas em um nome de arquivo.
	Uma barra invertida seguida de uma barra vertical (\\) é necessária quando uma barra vertical fizer parte do nome de um arquivo.
	Uma barra (\\) seguida por qualquer outro caractere, ou no final de um padrão, será ignorada.

Exemplo de filtros

Os exemplos a seguir mostram filtros comuns com os quais você pode usar DataSync.

Note

Há limites para o número de caracteres que você pode usar em um filtro. Para obter mais informações, consulte [DataSync cotas](#).

Excluir algumas pastas do local de origem

Em alguns casos, você poderá querer a exclusão de pastas no seu local de origem para não copiá-las para o seu local de destino. Por exemplo, se você tiver work-in-progress pastas temporárias, poderá usar algo como o filtro a seguir:

`*/*.temp`

Para excluir pastas com conteúdo semelhante (como `/reports2021` e `/reports2022`), você pode usar um filtro de exclusão como o seguinte:

`/reports*`

Para excluir pastas em qualquer nível da hierarquia de arquivos, você pode usar um filtro de exclusão, como o que segue.

`*/folder-to-exclude-1|*/folder-to-exclude-2`

Para excluir pastas no nível superior do local de origem, você pode usar um filtro de exclusão, como o que segue.

```
/top-level-folder-to-exclude-1|/top-level-folder-to-exclude-2
```

Inclua apenas um subconjunto das pastas do local de origem

Em alguns casos, seu local de origem pode ser um grande compartilhamento e você deseja transferir um subconjunto das pastas da raiz. Para incluir pastas específicas, inicie uma execução de tarefa com um filtro de inclusão, como o seguinte.

```
/folder-to-transfer/*
```

Excluir tipos de arquivo específicos

Para excluir determinados tipos de arquivo da transferência, crie uma execução de tarefa com um filtro de exclusão, como `*.temp`.

Transferir arquivos individuais especificados

Para transferir uma lista de arquivos individuais, inicie uma execução de tarefa com um filtro de inclusão, como o seguinte: `/folder/subfolder/file1.txt|/folder/subfolder/file2.txt|/folder/subfolder/file2.txt`

Criação de filtros de inclusão

Os filtros de inclusão definem os arquivos, objetos e pastas que você DataSync deseja transferir. Você pode configurar filtros de inclusão ao criar, editar ou iniciar uma tarefa.

DataSync verifica e transfere somente arquivos e pastas que correspondam aos filtros de inclusão. Por exemplo, para incluir um subconjunto das suas pastas de origem, você pode especificar `/important_folder_1|/important_folder_2`.

Note

Atualmente, os filtros de inclusão oferecem suporte ao caractere (*) apenas como o caractere mais à direita em um padrão. Por exemplo, `/documents*|/code*` é aceito, mas `*.txt` não.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, escolha Tarefas e depois escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para ter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#)

4. Em Conteúdo a ser varrido, escolha Arquivos, objetos e pastas específicos e selecione Usando filtros.
5. Em Inclui, insira seu filtro (por exemplo, /important_folders para incluir um diretório importante) e escolha Adicionar padrão.
6. Adicione outros filtros de inclusão conforme necessário.

Usando o AWS CLI

Ao usar o AWS CLI, você deve usar aspas simples (') ao redor do filtro e um | (pipe) como delimitador se você tiver mais de um filtro.

O exemplo a seguir especifica dois filtros de inclusão /important_folder1 e /important_folder2 ao executar o comando create-task.

```
aws datasync create-task
  --source-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \
  --destination-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \
  --includes FilterType=SIMPLE_PATTERN,Value='/important_folder1|/important_folder2'
```

Criação de filtros de exclusão

Os filtros de exclusão definem os arquivos, objetos e pastas em seu local de origem que você não DataSync deseja transferir. Você pode configurar estes filtros ao criar, editar ou iniciar uma tarefa.

Tópicos

- [Dados excluídos por padrão](#)

Dados excluídos por padrão

DataSync exclui automaticamente alguns dados da transferência:

- `.snapshot`— DataSync ignora qualquer caminho que termine com `.snapshot`, que normalmente é usado para point-in-time capturas instantâneas dos arquivos ou diretórios de um sistema de armazenamento.
- `/.aws-datasync` / `/.awssync` — DataSync cria essas pastas em sua localização para ajudar a facilitar sua transferência.
- `/.zfs`— Você pode ver essa pasta com os locais da Amazon FSx for OpenZFS.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, escolha Tarefas e depois escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para ter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#)

4. Em Exclusões, insira seu filtro (por exemplo, `*/temp` para excluir pastas temporárias) e escolha Adicionar padrão.
5. Adicione outros filtros de exclusão conforme necessário.
6. Se necessário, adicione [filtros de inclusão](#).

Usando o AWS CLI

Ao usar o AWS CLI, você deve usar aspas simples (`'`) ao redor do filtro e um `|` (pipe) como delimitador se você tiver mais de um filtro.

O exemplo a seguir especifica dois filtros de exclusão `*/temp` e `*/tmp` ao executar o comando `create-task`.

```
aws datasync create-task \
  --source-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \
  --destination-location-arn 'arn:aws:datasync:region:account-id:location/location-id' \
  --excludes FilterType=SIMPLE_PATTERN,Value='*/temp|*/tmp'
```

Entendendo como DataSync manipula metadados de arquivos e objetos

AWS DataSync pode preservar seus metadados de arquivo ou objeto durante uma transferência de dados. A forma como seus metadados são copiados depende dos locais de transferência e se esses locais usam tipos semelhantes de metadados.

Metadados no nível de sistema

Em geral, DataSync não copia metadados no nível do sistema. Por exemplo, ao transferir a partir de um servidor de arquivos SMB, as permissões que você configurou no nível do sistema de arquivos não são copiadas para o sistema de armazenamento de destino.

Há exceções. Ao transferir entre o Amazon S3 e outro armazenamento de objetos DataSync, copia [alguns metadados de objetos definidos pelo sistema](#).

Metadados copiados nas transferências do Amazon S3

As tabelas a seguir descrevem quais metadados DataSync podem ser copiados quando uma transferência envolve uma localização do Amazon S3.

Tópicos

- [Para o Amazon S3](#)
- [Entre o Amazon S3 e outros armazenamentos de objetos](#)
- [Entre o Amazon S3 e o HDFS](#)

Para o Amazon S3

Ao copiar a partir de um desses locais	Para este local	DataSync pode copiar
• NFS • Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP (usando NFS)	• Amazon S3	O seguinte como metadados do usuário do Amazon S3: • Time stamps de modificação de arquivos e pastas • Carimbos de data/hora de acesso a arquivos e pastas (só é DataSync possível

Ao copiar a partir de um desses locais	Para este local	DataSync pode copiar
		fazer isso com base no melhor esforço) • ID do usuário e ID do grupo • Permissões POSIX Os metadados de arquivo armazenados nos metadados do usuário do Amazon S3 são interoperáveis com compartilhamentos NFS nos gateways de arquivo usando AWS Storage Gateway. Um gateway de arquivos permite o acesso de baixa latência das redes locais aos dados que foram copiados para o Amazon S3 pelo DataSync. Esses metadados também são interoperáveis com FSx for Lustre. Quando DataSync copia objetos que contêm esses metadados de volta para um servidor NFS, os metadados do arquivo são restaurados. Restaurar metadados exige conceder permissões elevadas para o servidor NFS. Para obter mais informações, consulte Configurando AWS DataSync transferências com um servidor de arquivos NFS.

Entre o Amazon S3 e outros armazenamentos de objetos

Ao copiar entre esses locais	DataSync pode copiar
• Armazenamento de objetos • Amazon S3	• Metadados do objeto definidos pelo usuário • Tags de objetos • Os seguintes metadados de objetos definidos pelo sistema: • Content-Disposition • Content-Encoding • Content-Language • Content-Type Observação: DataSync copia metadados no nível do sistema para todos os objetos durante uma transferência inicial. Se você configurar sua tarefa para transferir somente os dados que foram alterados, DataSync não copiará os metadados do sistema nas transferências subsequentes, a menos que o conteúdo do objeto ou os metadados do usuário também tenham sido modificados. DataSync não copia outros metadados do objeto, como listas de controle de acesso a objetos (ACLs), versões anteriores do objeto ou a chave da última modificação.

Entre o Amazon S3 e o HDFS

Ao copiar entre esses locais	DataSync pode copiar
• Hadoop Distributed File System (HDFS) • Amazon S3	O seguinte como metadados do usuário do Amazon S3:

Ao copiar entre esses locais	DataSync pode copiar
	• Time stamps de modificação de arquivos e pastas • Carimbos de data/hora de acesso a arquivos e pastas (só é DataSync possível fazer isso com base no melhor esforço) • ID do usuário e ID do grupo • Permissões POSIX O HDFS usa cadeias de caracteres para armazenar a propriedade de usuários e grupos de arquivos e pastas, em vez de identificadores numéricos, como e. UIDs GIDs

Metadados copiados em transferências de NFS

A tabela a seguir descreve quais metadados DataSync podem ser copiados entre locais que usam o Network File System (NFS).

Ao copiar entre esses locais	DataSync pode copiar
• NFS • Amazon EFS • Amazon FSx para Lustre • Amazon FSx para OpenZFS • Amazon FSx para NetApp ONTAP (usando NFS)	• Time stamps de modificação de arquivos e pastas • Carimbos de data/hora de acesso a arquivos e pastas (só é DataSync possível fazer isso com base no melhor esforço) • ID do usuário (UID) e ID do grupo (GID) • Permissões POSIX

Metadados copiados em transferências de SMB

A tabela a seguir descreve quais metadados DataSync podem ser copiados entre locais que usam o Server Message Block (SMB).

Ao copiar entre esses locais	DataSync pode copiar
• SMB • Servidor FSx de arquivos Amazon para Windows • FSx para ONTAP (usando SMB)	• Time stamps de arquivo: tempo de acesso, tempo de modificação e tempo de criação • Identificador de segurança do proprietário do arquivo (SID) • Atributos de arquivo padrão: somente leitura (R), arquivamento (A), sistema (S), oculto (H), compactado (C), não indexado ao conteúdo (I), criptografado (E), temporário (T), off-line (O) e esparso (P) DataSync tenta copiar os atributos de arquivamento (A), compactado (C), não indexado ao contexto (I), esparsos (P) e temporários (T) com base no melhor esforço. Se esses atributos não forem aplicados ao destino, eles serão ignorados durante a verificação da tarefa. • Listas de acesso discricionário do NTFS (DACLS), que determinam se o acesso a um objeto deve ser concedido. • Listas de controle de acesso do sistema NTFS (SACLs), que são usadas pelos administradores para registrar tentativas de acessar um objeto protegido. Nota: não SACLs são copiados se você usar a versão 1.0 do SMB. Copiar DACLS e SACLs requer a concessão de permissões específicas ao usuário do Windows que DataSync usa para acessar sua localização usando SMB. Para obter mais informações, consulte criar um local para SMB, FSx Windows File Server ou FSx

Ao copiar entre esses locais	DataSync pode copiar
	ONTAP (dependendo do tipo de local em sua transferência).

Metadados copiados em outros cenários de transferência

DataSync trata os metadados das seguintes maneiras ao copiar entre esses sistemas de armazenamento (a maioria dos quais tem estruturas de metadados diferentes).

Ao copiar a partir de um desses locais	Para um desses locais	DataSync pode copiar
- SMB - FSx para Windows File Server - FSx para ONTAP (usando SMB)	- Amazon EFS - FSx para Lustre - FSx para OpenZFS - FSx para ONTAP (usando NFS) - Amazon S3 - Armazenamento de objetos - Azure Blob Storage - NFS	Metadados POSIX padrão para todos os arquivos e pastas no sistema de arquivos de destino ou objetos no bucket do S3 de destino. Essa abordagem inclui o uso dos valores do ID de usuário POSIX e do ID de grupo. Metadados baseados em Windows (como ACLs) não são preservados.
- Armazenamento de objetos - Amazon S3 - Azure Blob Storage	- Amazon EFS - FSx para Lustre - FSx para OpenZFS - FSx para ONTAP (usando NFS)	Metadados POSIX padrão nos arquivos e nas pastas de destino. Essa abordagem inclui o uso dos valores do ID de usuário POSIX e do ID de grupo.
- Amazon EFS - FSx para Lustre - FSx para OpenZFS	Azure Blob Storage	O seguinte é um metadado definido pelo usuário: Time stamps de modificação de arquivos e pastas

Ao copiar a partir de um desses locais	Para um desses locais	DataSync pode copiar
FSx para ONTAP (usando NFS)		- Carimbos de data/hora de acesso a arquivos e pastas (só é DataSync possível fazer isso com base no melhor esforço) - ID do usuário e ID do grupo - Permissões POSIX
HDFS	- Amazon EFS - FSx para Lustre - FSx para OpenZFS - FSx para ONTAP (usando NFS)	- Time stamps de modificação de arquivos e pastas - Carimbos de data/hora de acesso a arquivos e pastas (só é DataSync possível fazer isso com base no melhor esforço) - Permissões POSIX O HDFS armazena a propriedade de usuários e grupos de arquivos e pastas como cadeias de caracteres em vez de identificadores numéricos (como e). UIDs GIDs Os valores padrão para UIDs e GIDs são aplicados no sistema de arquivos de destino. Para obter mais informações, consulte Compreender quando e como DataSync aplica os metadados POSIX padrão.

Ao copiar a partir de um desses locais	Para um desses locais	DataSync pode copiar
• Amazon S3 • Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para Windows File Server • FSx para ONTAP	• HDFS	Data e hora de arquivos e pastas do local de origem. O proprietário do arquivo ou da pasta é definido com base no usuário do HDFS ou na entidade principal do Kerberos que você especificou ao criar o local de transferência do HDFS. A configuração do mapeamento de grupos no cluster do Hadoop determina o grupo.
• Amazon S3 • Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP (usando NFS) • Armazenamento de objetos • NFS • HDFS	• SMB • FSx para Windows File Server • FSx para ONTAP (usando SMB)	Data e hora de arquivos e pastas do local de origem. A propriedade é definida com base no usuário do Windows que foi especificado DataSync para acessar o compartilhamento da Amazon FSx ou SMB. As permissões são herdadas do diretório principal.
• Azure Blob Storage	• FSx para Windows File Server • FSx para ONTAP (usando SMB)	

Compreender quando e como DataSync aplica os metadados POSIX padrão

DataSync aplica metadados POSIX padrão nas seguintes situações:

- Quando os locais de origem e destino da sua transferência não têm estruturas de metadados semelhantes
- Quando não há metadados no local de origem

A tabela a seguir descreve como os metadados POSIX padrão são DataSync aplicados durante esses tipos de transferências:

Origem	Destination (Destino)	Permissões de arquivo	Permissões da pasta	UID	GID
• Amazon S3¹ • Armazenamento de objetos¹ • Armazenamento de Blobs do Microsoft Azure¹	• Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP (usando NFS) • NFS	0755	0755	65534	65534
• SMB	• Amazon S3 • Armazenamento de objetos • Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	0644	0755	65534	65534

Origem	Destination (Destino)	Permissões de arquivo	Permissões da pasta	UID	GID
	(usando NFS)				
	• NFS				
• HDFS	• Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP (usando NFS) • NFS	0644	0755	65534	65534

¹ Nos casos em que os objetos não têm metadados que foram aplicados anteriormente por DataSync.

Links e diretórios copiados pelo AWS DataSync

AWS DataSync trata links físicos, links simbólicos e diretórios de forma diferente, dependendo dos locais de armazenamento envolvidos na transferência.

Links rígidos

Veja como DataSync lidar com links físicos em alguns cenários comuns de transferência:

- Ao transferir entre um servidor de arquivos NFS, FSx para Lustre, para OpenZFS, FSx para ONTAP (usando NFS) e Amazon EFS, os links físicos são preservados.
- Ao transferir para o Amazon S3, cada arquivo subjacente referenciado por um link fixo é transferido apenas uma vez. Durante as transferências incrementais, objetos separados são criados no bucket do S3. Se um link físico não for alterado no Amazon S3, ele será restaurado

corretamente quando transferido para um servidor de arquivos NFS, para Lustre FSx , para OpenZFS FSx FSx , para ONTAP (usando NFS) ou sistema de arquivos Amazon EFS.

- Ao transferir para o Microsoft Azure Blob Storage, cada arquivo subjacente referenciado por um link fixo é transferido apenas uma vez. Durante as transferências incrementais, objetos separados são criados no armazenamento de blobs se houver novas referências na origem. Ao transferir de Azure Blob Storage, DataSync transfere links físicos como se fossem arquivos individuais.
- Ao transferir entre um servidor de arquivos SMB, FSx para o Windows File Server e FSx para o ONTAP (usando SMB), os links físicos não são suportados. Se DataSync encontrar links físicos nessas situações, a tarefa de transferência será concluída com um erro. Para saber mais, verifique seus CloudWatch registros.
- Ao transferir para o HDFS, os links físicos não são suportados. CloudWatch os registros mostram esses links como ignorados.

Links simbólicos

Veja como DataSync lidar com links simbólicos em alguns cenários comuns de transferência:

- Ao transferir entre um servidor de arquivos NFS, FSx para Lustre, para OpenZFS, FSx FSx para ONTAP (usando NFS) e Amazon EFS, os links simbólicos são preservados.
- Ao transferir para o Amazon S3, o caminho de destino do link é armazenado no objeto do Amazon S3. O link é restaurado corretamente quando transferido para um servidor de arquivos NFS, FSx para Lustre, para OpenZFS, FSx FSx para ONTAP ou sistema de arquivos Amazon EFS.
- Ao transferir para Azure Blob Storage, links simbólicos não são suportados. CloudWatch os registros mostram esses links como ignorados.
- Ao transferir entre um servidor de arquivos SMB, FSx para o Windows File Server e FSx para o ONTAP (usando SMB), links simbólicos não são suportados. DataSync não transfere um link simbólico em si, mas sim um arquivo referenciado pelo link simbólico. Para reconhecer arquivos duplicados e desduplicá-los com links simbólicos, você deve configurar a desduplicação no sistema de arquivos de destino.
- Ao transferir para o HDFS, links simbólicos não são suportados. CloudWatch os registros mostram esses links como ignorados.

Diretórios

Em geral, DataSync preserva os diretórios ao transferir entre sistemas de armazenamento. Esse não é o caso nas seguintes situações:

- Ao transferir para o Amazon S3, os diretórios são representados como objetos vazios que têm prefixos e terminam com uma barra (/).
- Ao transferir para o Azure Blob Storage sem um namespace hierárquico, não existem diretórios. O que parece ser um diretório é apenas parte do nome de um objeto.

Configuração de como lidar com arquivos, objetos e metadados

Você pode configurar como AWS DataSync manipula seus arquivos, objetos e seus metadados associados ao transferir entre locais.

Por exemplo, com transferências recorrentes, talvez você queira substituir os arquivos no destino com alterações na origem para manter os locais sincronizados. Você pode copiar propriedades como permissões POSIX para arquivos e pastas, tags associadas a objetos e listas de controle de acesso (ACLs).

Opções do modo de transferência

Você pode configurar se DataSync transfere somente os dados (incluindo metadados) que foram alterados após uma cópia inicial ou todos os dados toda vez que você executa a tarefa. Se você planeja transferências recorrentes, talvez queira transferir apenas o que mudou desde a execução anterior da tarefa.

Opção no console	Opção na API	Descrição
Transferir somente dados que foram alterados	TransferMode definido como CHANGED	Após a transferência inicial completa, DataSync copia somente os dados e os metadados que diferem entre o local de origem e o local de destino.
Transferir todos os dados	TransferMode definido como ALL	DataSync copia tudo na origem para o destino sem comparar as diferenças entre os locais.

Opções de manipulação de arquivos e objetos

Você pode controlar alguns aspectos de como DataSync trata seus arquivos ou objetos no local de destino. Por exemplo, DataSync pode excluir arquivos no destino que não estão na origem.

Opção no console	Opção na API	Descrição
Manter arquivos excluídos	PreserveDeletedFiles	Especifica se DataSync mantém arquivos ou objetos no local de destino que não existem na origem. Se você configurar sua tarefa para excluir objetos do seu bucket do Amazon S3, poderá incorrer em cobranças mínimas de duração de armazenamento para determinadas classes de armazenamento. Para obter informações detalhadas, consulte Considerações sobre a classes de armazenam ento com transferências do Amazon S3.  Warning Você não pode configurar sua tarefa para excluir dados no destino e também transferir todos os dados. Quando você transfere todos os dados, DataSync não escaneia sua localizaç

Opção no console	Opção na API	Descrição
		ção de destino e não sabe o que excluir.
Sobrescrever arquivos	OverwriteMode	Especifica se DataSync modifica os dados no local de destino quando os dados de origem ou os metadados são alterados. Se você não configurar sua tarefa para substituir dados, os dados de destino não serão substituídos, mesmo que os dados de origem sejam diferentes. Se a tarefa substituir objetos, você poderá estar sujeito a cobranças adicionais para determinadas classes de armazenamento (por exemplo, para recuperação ou exclusão antecipada). Para obter informações detalhadas, consulte Considerações sobre a classes de armazenam ento com transferências do Amazon S3.

Opções de tratamento de metadados

DataSync pode preservar metadados de arquivos e objetos durante uma transferência. Os metadados que DataSync podem ser preservados dependem dos sistemas de armazenamento envolvidos e se esses sistemas usam uma estrutura de metadados semelhante.

Antes de configurar sua tarefa, certifique-se de entender como DataSync manipula [metadados](#) e [arquivos especiais](#) ao transferir entre seus locais de origem e destino.

⚠ Important

DataSync suporta transferências de e para determinados sistemas de armazenamento em nuvem de terceiros, como o Google Cloud Storage e o IBM Cloud Object Storage, que manipulam os metadados do sistema de uma forma que não é totalmente compatível com o S3. Para essas transferências, DataSync tente copiar atributos de metadados `ContentType`, como, `ContentEncoding` `ContentLanguage`, e com `CacheControl` base no melhor esforço. Se o sistema de armazenamento de destino não aplicar esses atributos, eles serão ignorados durante a verificação da tarefa.

Opção no console	Opção na API	Descrição
Propriedade da cópia	Gid e Uid	Especifica se DataSync copia a propriedade do arquivo e da pasta POSIX, como o ID do grupo dos proprietários do arquivo e o ID do usuário do proprietário do arquivo.
Copiar permissões	PosixPermissions	Especifica se DataSync copia as permissões POSIX para arquivos e pastas da origem para o destino.
Copiar carimbos de data/hora	Atime e Mtime	Especifica se DataSync copia os metadados do carimbo de data/hora da origem para o destino.
Copiar tags de objetos	ObjectTags	Especifica se DataSync preserva as tags associadas aos seus objetos ao transferir entre sistemas de armazenamento de objetos.

Opção no console	Opção na API	Descrição
Propriedade da cópia DACLs, e SACLs	SecurityDescriptorCopyFlags definido como OWNER_DACL_SACL	DataSync copia o seguinte: • O proprietário do objeto. • Listas de acesso discricionário do NTFS (DACLs), que determinam se o acesso a um objeto deve ser concedido. • Listas de controle de acesso do sistema NTFS (SACLs), que são usadas pelos administradores para registrar tentativas de acessar um objeto protegido. Nota: não SACLs são copiados se você usar a versão 1.0 do SMB. Copiar DACLs e SACLs requer a concessão de permissões específicas ao usuário do Windows que DataSync usa para acessar sua localização usando SMB. Para obter mais informações, consulte criar um local para SMB, FSx Windows File Server ou FSx ONTAP (dependem do tipo de local em sua transferência).

Opção no console	Opção na API	Descrição
Propriedade da cópia e DACLs	SecurityDescriptorCopyFlags definido como OWNER_DACL	DataSync copia o seguinte: • O proprietário do objeto. • DACLs, que determinam se o acesso a um objeto deve ser concedido. DataSync não copiará SACLs quando você escolher essa opção.
Não copie a propriedade ou ACLs	SecurityDescriptorCopyFlags definido como NONE	DataSync não copia nenhum dado de propriedade ou permissão. Os objetos que DataSync gravam em seu local de destino pertencem ao usuário cujas credenciais são fornecidas DataSync para acessar o destino. As permissões do objeto de destino são determinadas com base nas permissões configuradas no servidor de destino.

Configurando opções de tratamento de arquivos, objetos e metadados

Você pode configurar como DataSync manipula arquivos, objetos e metadados ao criar, editar ou iniciar sua tarefa de transferência.

Usar o console de DataSync

As instruções a seguir descrevem como configurar as opções de tratamento de arquivos, objetos e metadados ao criar uma tarefa.

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.

2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

4. Para Modo de transferência, selecione uma das seguintes opções:
 - Transferir somente dados que foram alterados
 - Transferir todos os dados

Para obter mais informações sobre essas opções, consulte [Opções do modo de transferência](#).

5. Selecione Manter arquivos excluídos se DataSync quiser manter arquivos ou objetos no local de destino que não existem na origem.

Se você não escolher essa opção e sua tarefa excluir objetos de seu bucket Amazon S3, você poderá estar sujeito a cobranças mínimas de duração de armazenamento para determinadas classes de armazenamento. Para obter informações detalhadas, consulte [Considerações sobre as classes de armazenamento com transferências do Amazon S3](#).

 Warning

Você não pode desmarcar essa opção e ativar a opção Transferir todos os dados. Quando você transfere todos os dados, DataSync não escaneia sua localização de destino e não sabe o que excluir.

6. Selecione Substituir arquivos se quiser DataSync modificar os dados no local de destino quando os dados de origem ou os metadados forem alterados.

Se a tarefa substituir objetos, você poderá estar sujeito a cobranças adicionais para determinadas classes de armazenamento (por exemplo, para recuperação ou exclusão antecipada). Para obter informações detalhadas, consulte [Considerações sobre as classes de armazenamento com transferências do Amazon S3](#).

Se você não escolher essa opção, os dados de destino não serão substituídos, mesmo que os dados de origem sejam diferentes.

7. Em Opções de transferência, selecione como você deseja DataSync lidar com os metadados. Para obter mais informações sobre essas opções, consulte [Opções de tratamento de metadados](#).

 Important

As opções que você vê no console dependem dos locais de origem e destino da tarefa. Talvez seja necessário expandir Configurações adicionais para ver algumas dessas opções.

- Propriedade da cópia
- Copiar permissões
- Copiar carimbos de data/hora
- Copiar tags de objetos
- Propriedade da cópia DACLs, e SACLs
- Propriedade da cópia e DACLs
- Não copie a propriedade ou ACLs

Usando a DataSync API

Você pode configurar as opções de tratamento de arquivos, objetos e metadados usando o `Options` parâmetro com qualquer uma das seguintes operações:

- [CreateTask](#)
- [StartTaskExecution](#)
- [UpdateTask](#)

Configurando como AWS DataSync verifica a integridade dos dados

Durante uma transferência, AWS DataSync usa a verificação de soma de verificação para verificar a integridade dos dados que você copia entre locais. Você também pode configurar DataSync para realizar uma verificação adicional ao final da transferência.

Opções de verificação de dados

Use as informações a seguir para ajudá-lo a decidir se e como você DataSync deseja realizar essas verificações adicionais.

Opção do console	Opção de API	Descrição
Verifique somente os dados transferidos (recomendado)	VerifyMode definido como ONLY_FILES_TRANSFERRED	DataSync calcula a soma de verificação dos dados transferidos (incluindo metadados) no local de origem. Ao final da transferência, DataSync compara essa soma de verificação com a soma de verificação calculada com base nos mesmos dados no destino. Recomendamos essa opção ao transferir para o S3 Glacier Flexible Retrieval ou para classes de armazenamento do S3 Glacier Deep Archive. Para obter mais informações, consulte Considerações sobre a classes de armazenam ento com transferências do Amazon S3.
Verifique todos os dados	VerifyMode definido como POINT_IN_TIME_CONSISTENT	Ao final da transferência, DataSync verifique toda a origem e o destino para verificar se os dois locais estão totalmente sincronizados.

Opção do console	Opção de API	Descrição
		 Note Não é suportado quando sua tarefa usa o modo Avançado. Se você usa um manifesto, DataSync apenas digitaliza e verifica o que está listado no manifesto. Você não usa essa opção ao transferir para o S3 Glacier Flexible Retrieval ou para classes de armazenamento do S3 Glacier Deep Archive. Para obter mais informações, consulte Considerações sobre a classes de armazenam ento com transferências do Amazon S3.
Não verifique os dados após a transferência	VerifyMode definido como NONE	DataSync realiza verificações de integridade de dados somente durante sua transferência. Ao contrário de outras opções, não há verificação adicional no fim da transferência.

Configurando a verificação de dados

Você pode configurar as opções de verificação de dados ao criar uma tarefa, atualizar uma tarefa ou iniciar a execução de uma tarefa.

Usar o console de DataSync

As instruções a seguir descrevem como configurar as opções de verificação de dados ao criar uma tarefa.

Para configurar a verificação de dados usando o console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

4. Em Verificação, escolha uma das seguintes opções:
 - Verifique somente os dados transferidos (recomendado)
 - Verifique todos os dados
 - Não verifique os dados após a transferência

Uso da API DataSync

Você pode configurar como DataSync verifica os dados usando o `VerifyMode` parâmetro com qualquer uma das seguintes operações:

- [CreateTask](#)
- [UpdateTask](#)
- [StartTaskExecution](#)

Definir limites de largura de banda para a tarefa de AWS DataSync

Você pode configurar limites de largura de banda de rede para sua AWS DataSync tarefa e cada uma de suas execuções.

Note

Não aplicável às [tarefas do modo Avançado](#).

Limitar a largura de banda para uma tarefa

Defina um limite de largura de banda ao criar, editar ou iniciar uma tarefa.

Usar o console de DataSync

As instruções a seguir descrevem como configurar um limite de largura de banda para a tarefa ao criá-la.

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

4. Em Limite de largura de banda, escolha uma das seguintes opções:
 - Selecione Usar disponível para usar toda a largura de banda da rede disponível para cada execução de tarefa.
 - Selecione Definir limite de largura de banda (MiB/s) e insira a largura de banda máxima que você deseja usar DataSync para cada execução de tarefa.

Usando a DataSync API

Você pode configurar o limite de largura de banda de uma tarefa usando o parâmetro `BytesPerSecond` com qualquer uma das seguintes operações:

- [CreateTask](#)
- [UpdateTask](#)
- [StartTaskExecution](#)

Controle de utilização da largura de banda para a execução de uma tarefa

Você pode modificar o limite de largura de banda para a execução de uma tarefa em execução ou em fila.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação, expanda Transferência de dados e, em seguida, escolha Tarefas.
3. Escolha a tarefa e, em seguida, selecione Histórico para ver as execuções da tarefa.
4. Escolha a execução da tarefa que você deseja modificar e, em seguida, escolha Editar.
5. Na caixa de diálogo Fazer upload, escolha uma das seguintes:
 - Selecione Usar disponível para usar toda a largura de banda da rede disponível para a execução da tarefa.
 - Selecione Definir limite de largura de banda (MiB/s) e insira a largura de banda máxima que você deseja usar DataSync para a execução da tarefa.
6. Escolha Salvar alterações.

O novo limite de largura de banda entra em vigor em 60 segundos.

Uso da API DataSync

Você pode modificar o limite de largura de banda para a execução de uma tarefa em execução ou em fila usando o BytesPerSecond parâmetro com a operação. [UpdateTaskExecution](#)

Agendamento quando sua AWS DataSync tarefa é executada

Você pode configurar um agendamento de AWS DataSync tarefas para transferir dados periodicamente entre os locais de armazenamento.

Como funciona o DataSync agendamento de tarefas

Uma DataSync tarefa agendada é executada na frequência especificada por você, com um intervalo mínimo de 1 hora. Você pode criar um agendamento de tarefas usando as expressões cron ou rate.

Important

Você não pode agendar uma tarefa para ser executada a intervalos de menos de 1 hora.

Usar expressões cron

Use expressões cron para agendamentos de tarefas executadas em hora e dia específicos. Por exemplo, veja como você pode configurar o agendamento de uma tarefa na AWS CLI para ser executada todo domingo e toda quarta-feira às 12h UTC.

```
cron(0 12 ? * SUN,WED *)
```

Uso de expressões rate

Use expressões rate para agendamentos de tarefas que são executadas a intervalos regulares, como a cada 12 horas. Por exemplo, veja como você pode configurar um agendamento de tarefas no AWS CLI que é executado a cada 12 horas:

```
rate(12 hours)
```

Tip

Para obter mais informações sobre a sintaxe de expressão cron e de taxa, consulte o Guia [EventBridge do usuário da Amazon](#).

Criação de um cronograma de DataSync tarefas

Você pode programar a frequência com que sua tarefa é executada usando o DataSync AWS CLI console ou a DataSync API.

Usando o DataSync console

As instruções a seguir descrevem como configurar um agendamento ao criar uma tarefa. Você pode modificar o agendamento posteriormente quando editar a tarefa.

No console, algumas opções de agendamento permitem que você especifique a hora exata que a tarefa é executada (como diariamente às 22h30). Se você não incluir um horário para essas opções, a tarefa será executada no momento que você a criar (ou atualizar).

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.

3. Configure os locais de origem e destino da sua tarefa.

Para ter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#)

4. Em Frequência, escolha uma das seguintes opções:

- Escolha Não agendada se não quiser agendar a execução periódica da tarefa.
- Escolha A cada hora e depois escolha a quantos minutos da hora você deseja que a tarefa seja executada.
- Escolha Diariamente e insira a hora UTC que você deseja que a tarefa seja executada.
- Escolha Semanalmente e o dia da semana, e insira a hora UTC que você deseja que a tarefa seja executada.
- Escolha Dias da semana, escolha um dia ou dias específicos e insira a hora UTC que a tarefa deve ser executada no formato HH:MM.
- Escolha Personalizado e selecione Expressão Cron ou Expressão rate. Insira o agendamento da tarefa com um intervalo mínimo de 1 hora.

Usando o AWS CLI

Você pode criar um cronograma para sua DataSync tarefa usando o `--schedule` parâmetro com o `start-task-execution` comando `create-task` ou `update-task`, ou.

As instruções a seguir descrevem como fazer isso com o comando `create-task`.

1. Copie o seguinte comando `create-task`:

```
aws datasync create-task \
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh \
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-abcdefgh12345678 \
  --schedule '{
    "ScheduleExpression": "cron(0 12 ? * SUN,WED *)"
  }'
```

2. No parâmetro `--source-location-arn`, especifique o nome do recurso da Amazon (ARN) do local de onde você está transferindo os dados.

3. No parâmetro `--destination-location-arn`, especifique o ARN do local para onde você está transferindo os dados.
4. No parâmetro `--schedule`, especifique uma expressão cron ou rate para o agendamento.

No exemplo, a expressão cron `cron(0 12 ? * SUN,WED *)` define um agendamento de tarefa para execução todo domingo e toda quarta-feira às 12h UTC.

5. Execute o comando `create-task` para criar a tarefa com o agendamento.

Pausando um agendamento de DataSync tarefas

Pode haver situações em que você precise pausar seu cronograma de DataSync tarefas. Por exemplo, pode ser necessário desabilitar temporariamente uma transferência recorrente para corrigir um problema com a tarefa ou realizar a manutenção do sistema de armazenamento.

DataSync pode desativar seu agendamento de tarefas automaticamente pelos seguintes motivos:

- Falhas recorrentes na tarefa com o mesmo erro.
- Você [desabilita uma Região da AWS](#) que a tarefa está usando.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e selecione Tarefas.
3. Escolha a tarefa cujo agendamento você deseja pausar e escolha Editar.
4. Em Agendamento, desative Habilitar agendamento. Escolha Salvar alterações.

Usando o AWS CLI

1. Copie o seguinte comando `update-task`:

```
aws datasync update-task \  
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh \  
  --schedule '{  
    "ScheduleExpression": "cron(0 12 ? * SUN,WED *)",  
    "Status": "DISABLED"  
  }'
```

2. No parâmetro `--task-arn`, especifique o ARN da tarefa cujo agendamento você deseja pausar.
3. No parâmetro `--schedule` faça o seguinte:
 - Em `ScheduleExpression`, especifique uma expressão cron ou rate para o agendamento.

No exemplo, a expressão `cron(0 12 ? * SUN,WED *)` define o agendamento de uma tarefa para execução todo domingo e toda quarta-feira às 12h UTC.
 - Em `Status`, especifique `DISABLED` para pausar o agendamento da tarefa.
4. Execute o comando `update-task`.
5. Para retomar o agendamento, execute o mesmo comando `update-task` com `Status` definido como `ENABLED`.

Verificando o status de um agendamento de DataSync tarefas

Você pode ver se sua agenda de DataSync tarefas está ativada.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e selecione Tarefas.
3. Na coluna Agendamento, verifique se o agendamento da tarefa está habilitado ou desabilitado.

Usando o AWS CLI

1. Copie o seguinte comando `describe-task`:

```
aws datasync describe-task \  
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

2. No parâmetro `--task-arn`, especifique o ARN da tarefa sobre a qual você deseja informações.
3. Execute o comando `describe-task`.

Você recebe uma resposta que fornece detalhes sobre a tarefa, incluindo seu agendamento. (O foco do exemplo a seguir é principalmente na configuração do agendamento de tarefa e não mostra uma resposta completa a `describe-task`.)

O exemplo mostra que o agendamento da tarefa foi desabilitado manualmente. Se o agendamento for desativado pelo DataSync SERVICE, você verá uma mensagem de erro `DisabledReason` para ajudá-lo a entender por que a tarefa continua falhando. Para obter mais informações, consulte [???](#).

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh",
  "Status": "AVAILABLE",
  "Schedule": {
    "ScheduleExpression": "cron(0 12 ? * SUN,WED *)",
    "Status": "DISABLED",
    "StatusUpdateTime": 1697736000,
    "DisabledBy": "USER",
    "DisabledReason": "Manually disabled by user."
  },
  ...
}
```

Marcando suas tarefas AWS DataSync

As tags são pares de valores-chave que ajudam você a gerenciar, filtrar e pesquisar seus AWS DataSync recursos. Você pode adicionar até 50 tags a cada DataSync tarefa e execução de tarefas.

Por exemplo, você pode criar uma tarefa para uma grande migração de dados e marcar a tarefa com a chave **Project** e o valor **Large Migration**. Para organizar ainda mais a migração, você pode marcar uma execução da tarefa com a chave **Transfer Date** e o valor **May 2021** (as execuções de tarefas subsequentes podem ser marcadas **June 2021**, **July 2021** e assim por diante).

Marcando sua tarefa DataSync

Você pode marcar sua DataSync tarefa somente ao criar a tarefa.

Usar o console de DataSync

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

4. Na página Definir configurações, escolha Adicionar tag para marcar a tarefa.

Usando o AWS CLI

1. Copie o seguinte comando `create-task`:

```
aws datasync create-task \  
  --source-location-arn 'arn:aws:datasync:region:account-id:location/source-  
location-id' \  
  --destination-location-arn 'arn:aws:datasync:region:account-  
id:location/destination-location-id' \  
  --tags Key=tag-key,Value=tag-value
```

2. Especifique os seguintes parâmetros no comando:

- `--source-location-arn`: especifique o nome do recurso da Amazon (ARN) do local de origem na transferência.
- `--destination-location-arn`: especifique o ARN do local de destino na transferência.
- `--tags`: especifique as tags que você deseja aplicar à tarefa.

Para mais de uma tag, separe cada par de valores-chave com um espaço.

3. (Opcional) Especifique outros parâmetros que façam sentido para o cenário de transferência.

Para obter uma lista de `--options`, consulte o comando [create-task](#).

4. Execute o comando `create-task`.

Você recebe uma resposta que mostra a tarefa que você acabou de criar.

```
{  
  "TaskArn": "arn:aws:datasync:us-east-2:123456789012:task/task-  
abcdef01234567890"  
}
```

Para ver as tags que você adicionou a essa tarefa, você pode usar o [list-tags-for-resource](#) comando.

Marcando sua execução de DataSync tarefas

Você pode marcar cada execução da sua DataSync tarefa.

Se sua tarefa já tiver tags, lembre-se do seguinte sobre o uso de tags com execuções de tarefas:

- Se você iniciar sua tarefa com o console, as tags criadas pelo usuário serão aplicadas automaticamente à execução da tarefa. No entanto, as tags criadas pelo sistema que começam com `aws:` não são aplicadas.
- Se você iniciar sua tarefa com a DataSync API ou AWS CLI, suas tags não serão aplicadas automaticamente à execução da tarefa.

Usar o console de DataSync

Para adicionar, editar ou remover tags da execução de uma tarefa, você deve iniciar a tarefa com opções de substituição.

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e selecione Tarefas.
3. Escolha a tarefa.
4. Escolha Iniciar e, em seguida, uma das seguintes opções:
 - Iniciar com padrões: aplica todas as tags associadas à tarefa.
 - Iniciar com opções de substituição: permite adicionar, editar ou remover tags para a execução dessa tarefa específica.

Usando o AWS CLI

1. Copie o seguinte comando `start-task-execution`:

```
aws datasync start-task-execution \
  --task-arn 'arn:aws:datasync:region:account-id:task/task-id' \
  --tags Key=tag-key,Value=tag-value
```

2. Especifique os seguintes parâmetros no comando:
 - `--task-arn`: especifique o ARN da tarefa que você deseja iniciar.
 - `--tags`: especifique as tags que você deseja aplicar a essa execução específica da tarefa.

Para mais de uma tag, separe cada par de valores-chave com um espaço.

3. (Opcional) Especifique outros parâmetros que façam sentido para a sua situação.

Para obter mais informações, consulte o comando [start-task-execution](#).

4. Execute o comando `start-task-execution`.

Você recebe uma resposta que mostra a execução da tarefa que você acabou de iniciar.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-2:123456789012:task/task-
  abcdef01234567890"
}
```

Para ver as tags que você adicionou a essa tarefa, você pode usar o [list-tags-for-resource](#) comando.

Iniciando uma tarefa para transferir seus dados

Depois de criar sua tarefa AWS DataSync de transferência, você pode começar a mover os dados. Cada execução de uma tarefa é chamada de execução de tarefa. Para obter informações sobre o que acontece durante a execução de uma tarefa, consulte [Como DataSync transfere arquivos, objetos e diretórios](#).

Important

Se você planeja transferir dados de ou para um local do Amazon S3, analise [como isso DataSync pode afetar as cobranças de suas solicitações do S3](#) e a [página de DataSync preços](#) antes de começar.

Iniciando sua tarefa

Depois de criar sua tarefa, você pode começar a mover os dados imediatamente.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e selecione Tarefas.
3. Escolha a tarefa que você deseja executar.

Certifique-se de que a tarefa tenha um status Disponível. Você também pode selecionar várias tarefas.

4. Escolha Ações e, em seguida, escolha uma das seguintes opções:

- Iniciar: executa a tarefa (ou tarefas, se você selecionou mais de uma).
- Iniciar com opções de substituição: permite que você modifique algumas das configurações da tarefa antes de começar a mover os dados. Quando estiver pronto, escolha Iniciar.

5. Escolha Ver detalhes da execução para ver detalhes sobre a execução da tarefa em execução.

Usando o AWS CLI

Para iniciar sua DataSync tarefa, você só precisa especificar o Amazon Resource Name (ARN) da tarefa que você deseja executar. Veja um exemplo de comando `start-task-execution`:

```
aws datasync start-task-execution \  
  --task-arn 'arn:aws:datasync:region:account-id:task/task-id'
```

O exemplo a seguir inicia uma tarefa com algumas configurações diferentes das configurações padrão da tarefa:

```
aws datasync start-task-execution \  
  --override-options VerifyMode=NONE,OverwriteMode=NEVER,PosixPermissions=NONE
```

O comando retorna um ARN para a execução da sua tarefa semelhante ao exemplo a seguir:

```
{  
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:209870788375:task/  
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"  
}
```

Note

Cada agente pode executar uma única tarefa por vez.

Usando a DataSync API

Você pode iniciar sua tarefa usando a [StartTaskExecution](#) operação. Use a [DescribeTaskExecution](#) operação para obter detalhes sobre a execução da tarefa em execução.

Depois de iniciada, você pode [verificar o status da execução da tarefa](#) enquanto DataSync copia seus dados. Você também pode [limitar a largura de banda da execução da tarefa](#), se necessário.

Status de execução de tarefa

Ao iniciar uma DataSync tarefa, você pode ver esses status. (Os [status da tarefa](#) são diferentes dos status de execução da tarefa.)

Status do console	Status da API	Descrição
Enfileiramento	QUEUED	Outra execução de tarefa é executar e usar o mesmo DataSync agente. Para obter mais informações, consulte Como saber quando a tarefa está na fila .
Launching	LAUNCHING	DataSync está inicializando a execução da tarefa. Esse status geralmente desaparece rapidamente, mas pode levar até alguns minutos.
Preparação	PREPARING	DataSync está determinando quais dados transferir. A preparação pode levar apenas alguns minutos, algumas horas ou até mais, dependendo do número de arquivos, objetos ou diretórios nos dois locais e de como você configura sua tarefa. A forma como a preparação funciona também depende do seu modo de tarefa. Para obter mais informações, consulte Como DataSync prepara sua transferência de dados .
Em transferência	TRANSFERRING	DataSync está realizando a transferência de dados real.
Verificando	VERIFYING	DataSync está verificando a integridade dos seus dados no final da transferência.

Status do console	Status da API	Descrição
Bem-sucedida	SUCCESS	A execução da tarefa foi bem-sucedida.
Cancelando	CANCELLING	A execução da tarefa está em processo de ser cancelada.
Erro	ERROR	Houve falha na execução da tarefa.

Como saber quando a tarefa está na fila

Ao executar várias tarefas (por exemplo, você está [transferindo um grande conjunto](#) de dados), DataSync pode colocar as tarefas na fila para serem executadas em uma série (primeiro a entrar, primeiro a sair). Alguns exemplos de quando isso acontece incluem:

- Você executa tarefas diferentes que usam o mesmo DataSync agente. Embora você possa usar o mesmo agente para várias tarefas, o agente só pode executar uma tarefa de cada vez.
- A execução de uma tarefa está em andamento e você inicia execuções adicionais da mesma tarefa usando [filtros](#) ou [manifestos](#) diferentes.

Em cada exemplo, as tarefas na fila não começam até que a tarefa na frente delas termine.

Cancelamento da execução da tarefa

Você pode interromper a execução de qualquer DataSync tarefa em execução ou em fila.

Para cancelar a execução de uma tarefa usando o console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e selecione Tarefas.
3. Selecione o ID da tarefa da tarefa em execução que você deseja monitorar.

O status da tarefa deve ser Em execução.

4. Escolha Histórico para ver as execuções da tarefa.
5. Selecione a execução da tarefa que você deseja interromper e, em seguida, escolha Parar.
6. Na caixa de diálogo, escolha Parar.

Para cancelar uma tarefa em execução ou em fila usando a DataSync API, consulte.

[CancelTaskExecution](#)

Monitorando suas AWS DataSync transferências

O monitoramento é importante para manter a confiabilidade e o desempenho de suas atividades de AWS DataSync transferência. Recomendamos que você colete dados de monitoramento para que possa depurar mais facilmente erros, caso ocorram. Antes de começar a monitorar DataSync, no entanto, crie um plano de monitoramento que inclua respostas às seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

AWS fornece vários serviços e ferramentas para monitoramento DataSync. Você pode configurar algumas dessas para fazer o monitoramento em seu lugar; algumas delas exigem intervenção manual. Recomendamos que as tarefas de monitoramento sejam automatizadas ao máximo possível.

Tópicos

- [Entendendo os contadores de desempenho de transferência de dados](#)
- [Monitoramento de transferências de dados com CloudWatch métricas da Amazon](#)
- [Monitorando suas transferências de dados com relatórios de tarefas](#)
- [Monitoramento de transferências de dados com o Amazon CloudWatch Logs](#)
- [Registrando chamadas de AWS DataSync API com AWS CloudTrail](#)
- [Monitorando eventos usando a Amazon EventBridge](#)
- [Monitoramento AWS DataSync com ferramentas manuais](#)

Entendendo os contadores de desempenho de transferência de dados

Quando você [inicia uma tarefa](#), AWS DataSync fornece contadores para ajudar a monitorar o desempenho e o progresso da transferência de dados.

Use as informações a seguir para entender o que cada contador representa. Você pode ver esses contadores no DataSync console ou em uma [DescribeTaskExecution](#) resposta. Alguns contadores não estão disponíveis em todos os [modos de tarefa](#).

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
–	BytesWritten	Aprimorado, básico	O número de bytes lógicos que DataSync realmente gravam no local de destino.
Taxa de transferência de dados	–	Aprimorado, básico	A taxa na qual DataSync grava bytes lógicos no local de destino. Se você estiver usando DescribeTaskExecution, a forma como você calcula esse contador depende do seu modo de tarefa: • Modo aprimorado: $\text{Divida BytesWritten por TotalDuration}$ • Modo básico: dividir BytesWritten por TransferDuration
Dados transferidos	BytesTransferred	Aprimorado, básico	O número de bytes DataSync enviados para a rede antes da compactação (se

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
			a compactação for possível). Para saber o número de bytes transferidos pela rede, consulte o contador de taxa de transferência de rede (no console) ou BytesCompressed (in DescribeTaskExecution).
Excluído do destino	FilesDeleted	Aprimorado, básico	O número de arquivos, objetos e diretórios que DataSync realmente são excluídos em seu local de destino. Se você não configurar sua tarefa para excluir dados no destino que não estão na origem: - Excluído do destino não é exibido no console. - FilesDeleted sempre mostra um valor de 0.

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
–	EstimatedBytesToTransfer	Aprimorado, básico	O número de bytes lógicos que DataSync esperam gravar no local de destino.
–	EstimatedFilesToDelete	Aprimorado, básico	O número de arquivos, objetos e diretórios que você DataSync espera excluir no local de destino. Se você não configurar sua tarefa para excluir os dados no destino que não estão na origem, o valor sempre será 0.

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
–	EstimatedFilesToTransfer	Aprimorado, básico	O número de arquivos, objetos e diretórios que DataSync esperam ser transferidos pela rede. Esse valor é calculado enquanto DataSync prepara a transferência. A forma como isso é calculado depende principalmente do modo de transferência que você está usando: - Se o modo de transferência estiver definido para transferir somente dados que foram alterados: o cálculo é baseado na comparação do conteúdo dos locais de origem e destino e na determinação da diferença que precisa ser transferida. A diferença pode incluir: - Tudo o que for adicionado ou

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
			modificado no local de origem. - Qualquer coisa que esteja nos dois locais e modificada no destino após uma transferência inicial (a menos que você configure sua tarefa para não sobrescrever dados no destino). (Somente no modo básico) O número de itens que você DataSync espera excluir (se você configurar sua tarefa para excluir dados no destino). - Se o modo de transferência estiver definido para transferir todos os dados: o cálculo é baseado somente nos itens DataSync

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
			encontrados no local de origem.
Taxa de transferência de arquivos	–	Aprimorado, básico	A taxa na qual DataSync transfere arquivos, objetos e diretórios pela rede. Se você estiver usando DescribeTaskExecution, a forma como você calcula esse contador depende do seu modo de tarefa: • Modo aprimorado: Divida FilesTransferred por TotalDuration • Modo básico: dividir FilesTransferred por TransferDuration

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
–	FilesFailed	Aprimorado	O número de objetos que DataSync falham na preparação, transferência, verificação e exclusão durante a execução da tarefa. Se houver falhas, você poderá vê-las ao lado dos contadores Preparado, Transferido, Ignorado e Excluído do console de destino, respectivamente.

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
Listado na fonte	FilesListed.AtSource	Aprimorado	O número de objetos DataSync encontrados no local de origem. - Com um manifesto, DataSync lista somente o que está em seu manifesto (e não tudo em seu local de origem). - Com um filtro de inclusão, DataSync lista somente o que corresponde ao filtro no local de origem. - Com um filtro de exclusão, DataSync lista tudo no local de origem antes de aplicar o filtro.
–	FilesListed.AtDestinationForDelete	Aprimorado	O número de objetos DataSync encontrados no local de destino. Esse contador só é aplicável se você configurar sua tarefa para excluir dados no destino que não estejam na origem.

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
Taxa de transferência da rede *	BytesCompressed	Aprimorado, básico	O número de bytes físicos que são DataSync transferidos pela rede após a compactação (se a compactação for possível). Esse número geralmente é menor do que os dados transferidos (no console) ou BytesTransferred (em DescribeTaskExecution), a menos que os dados não sejam compactáveis. * — No modo Avançado, a taxa de transferência da rede não é exibida no console.

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
Porcentagem comprimida	–	Básico	A porcentagem de dados de transferência que DataSync foram compactados antes de serem enviados pela rede. Se você estiver usando DescribeTaskExecution, você pode calcular esse contador com <pre>1 - BytesCompressed / BytesWritten .</pre>

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
Preparado	FilesPrepared	Aprimorado	O número de objetos que DataSync tentarão ser transferidos depois de comparar seus locais de origem e destino. No console, esse contador também pode mostrar o número de objetos que DataSync pulam durante a preparação. Para obter mais informações, consulte Como DataSync prepara sua transferência de dados. Esse contador não é aplicável se você configurar sua tarefa para transferir todos os dados. Nesse cenário, DataSync copia tudo da origem ao destino sem comparar as diferenças entre os locais.

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
Taxa de processamento	–	Aprimorado, básico	A taxa na qual DataSync lê arquivos, objetos e diretórios no local de origem. A taxa de processamento é baseada em várias CloudWatch métricas. As métricas exatas dependem do modo de tarefa que você está usando. Modo aprimorado: - FilesListedSource - FilesPrepared - FilesTransferred - FilesVerified Modo básico: - FilesPreparedSource - FilesPreparedDestination - FilesTransferred - FilesVerifiedSource

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
			FilesVerifiedDestination
Restante	–	Básico	O número restante de arquivos, objetos e diretórios que DataSync esperam ser transferidos pela rede. Se você estiver usando DescribeTaskExecution, você pode calcular esse contador FilesTransferred subtraindo de EstimatedFilesToTransfer

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
Ignorado *	FilesSkipped	Aprimorado, básico	O número de arquivos, objetos e diretórios que são DataSync ignorados durante a transferência. * — No modo Avançado, Skipped não é exibido no console. Em vez disso, os itens ignorados são incluídos no contador preparado ao transferir somente os dados que foram alterados ou no contador transferido ao transferir todos os dados.

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
Transferido	FilesTransferred	Aprimorado, básico	O número de arquivos, objetos e diretórios que são DataSync transferidos pela rede. Esse valor é atualizado periodicamente durante a execução da tarefa quando algo é lido da fonte e enviado pela rede. Se DataSync não conseguir transferir algo, esse valor pode ser menor que <code>EstimatedFilesToTransfer</code>. Em alguns casos, esse valor também pode ser maior que <code>EstimatedFilesToTransfer</code>. Esse contador é específico de implementação para alguns tipos de localização, portanto, não o use como uma indicação exata do que está sendo transferido ou para

Console	DescribeTaskExecution	Suporte ao modo de tarefa	Descrição
			monitorar a execução da tarefa. No console, esse contador também pode mostrar o número de objetos que DataSync pula durante a transferência de uma tarefa do modo Avançado. Para obter mais informações, consulte Como DataSync transfere seus dados.
Verificado	FilesVerified	Aprimorado, básico	O número de arquivos, objetos e diretórios que são DataSync verificados durante a transferência. Quando você configura sua tarefa para verificar somente os dados transferidos, DataSync não verifica diretórios em algumas situações nem arquivos ou objetos que falham na transferência.

Monitoramento de transferências de dados com CloudWatch métricas da Amazon

CloudWatch A Amazon fornece métricas para monitorar o desempenho da DataSync transferência e solucionar problemas com sua tarefa de transferência.

Você pode monitorar o desempenho da AWS DataSync transferência usando CloudWatch as métricas da Amazon. DataSync as métricas são enviadas automaticamente CloudWatch em intervalos de 5 minutos (independentemente de como você [configura o registro](#)). As métricas são mantidas por um período de 15 meses.

Para ver CloudWatch as métricas de DataSync, você pode usar as seguintes ferramentas:

- O CloudWatch console
- O CloudWatch CLI
- A CloudWatch API
- O DataSync console (na página de detalhes da execução da tarefa)

Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).

CloudWatch métricas para DataSync

DataSync as métricas usam o `aws/datasync` namespace e fornecem métricas para as seguintes dimensões:

- `AgentId`— O ID exclusivo do agente (se sua tarefa usar um agente).
- `TaskId`— O ID exclusivo da tarefa. Ele segue o formato `task-01234567890abcdef`.

O namespace `aws/datasync` inclui as métricas a seguir. Algumas métricas não estão disponíveis em todos os [modos de tarefa](#).

CloudWatch métrica	Suporte ao modo de tarefa	Descrição
<code>BytesCompressed</code>	Básico	O número de bytes físicos que são DataSync transferidos pela rede após a compactação (se a compactação

CloudWatch métrica	Suporte ao modo de tarefa	Descrição
		for possível). Esse número geralmente é menor do que, <code>BytesTransferred</code> a menos que os dados não sejam compactáveis. Unidade: bytes
<code>BytesPreparedDestination</code>	Básico	O número de bytes lógicos que são DataSync preparados no local de destino. Unidade: bytes
<code>BytesPreparedSource</code>	Básico	O número de bytes lógicos que são DataSync preparados no local de origem. Unidade: bytes
<code>BytesTransferred</code>	Básico	O número de bytes DataSync enviados para a rede antes da compactação (se a compactação for possível). Para saber o número de bytes transferidos pela rede, consulte a <code>BytesCompressed</code> métrica. Unidade: bytes
<code>BytesVerifiedDestination</code>	Básico	O número de bytes lógicos que são DataSync verificados no local de destino. Unidade: bytes
<code>BytesVerifiedSource</code>	Básico	O número de bytes lógicos que são DataSync verificados no local de origem. Unidades: bytes
<code>BytesWritten</code>	Aprimorado, básico	O número de bytes lógicos DataSync gravados no local de destino. Unidade: bytes

CloudWatch métrica	Suporte ao modo de tarefa	Descrição
FilesDeleted	Aprimorado, básico	O número de arquivos, objetos e diretórios que são DataSync excluídos em seu local de destino. Se você não configurar sua tarefa para excluir os dados no destino que não estão na origem, o valor sempre será 0. Unidade: contagem
FilesListedSource	Aprimorado	O número de objetos DataSync encontrados no local de origem. Unidade: contagem
FilesPrepared	Aprimorado	O número de objetos que DataSync tentarão ser transferidos depois de comparar seus locais de origem e destino. Para obter mais informações, consulte Como DataSync prepara sua transferência de dados. Essa métrica não é aplicável se você configurar sua tarefa para transferir todos os dados. Nesse cenário, DataSync copia tudo da origem ao destino sem comparar as diferenças entre os locais. Unidade: contagem
FilesPreparedDestination	Básico	O número de arquivos, objetos e diretórios que são DataSync preparados no local de destino. Unidade: contagem
FilesPreparedSource	Básico	O número de arquivos, objetos e diretórios que são DataSync preparados no local de origem. Unidade: contagem

CloudWatch métrica	Suporte ao modo de tarefa	Descrição
FilesSkipped	Básico	O número de arquivos, objetos e diretórios que são DataSync ignorados durante a transferência. Unidade: contagem
FilesTransferred	Aprimorado, básico	O número de arquivos, objetos e diretórios que são DataSync transferidos pela rede. Esse valor é atualizado periodicamente durante a execução da tarefa quando algo é lido da fonte e enviado pela rede.  Note Esse valor pode ser menor do que EstimatedFilesToTransfer em uma DescribeTaskExecution resposta se DataSync não conseguir transferir algo. Em alguns casos, esse valor também pode ser maior que EstimatedFilesToTransfer. Essa métrica é específica da implementação para alguns tipos de local e, portanto, não a use como uma indicação exata do que foi transferido nem para monitorar a execução da tarefa. Unidade: contagem
FilesVerified	Aprimorado	O número de objetos que são DataSync verificados durante sua transferência. Unidade: contagem
FilesVerifiedDestination	Básico	O número de arquivos, objetos e diretórios que são DataSync verificados no local de destino. Unidade: contagem

CloudWatch métrica	Suporte ao modo de tarefa	Descrição
FilesVerifiedSource	Básico	O número de arquivos, objetos e diretórios DataSync verificados no local de origem. Unidade: contagem

Monitorando suas transferências de dados com relatórios de tarefas

Os relatórios de tarefas fornecem informações detalhadas sobre quais AWS DataSync tentativas transferir, ignorar, verificar e excluir durante a execução de uma tarefa. Para obter mais informações, consulte [Como DataSync transfere arquivos, objetos e diretórios](#).

Os relatórios de tarefa são gerados em formato JSON. Você pode personalizar o nível de detalhes dos relatórios:

- [Os relatórios de tarefas somente resumidos](#) fornecem os detalhes necessários sobre a execução da tarefa, como quantos arquivos foram transferidos e se DataSync foi possível verificar a integridade dos dados desses arquivos.
- Os [relatórios de tarefas padrão](#) incluem um resumo e relatórios detalhados que listam cada arquivo, objeto ou pasta que DataSync tenta transferir, ignorar, verificar e excluir. Com um relatório de tarefa padrão, você também pode especificar o [nível do relatório](#) para mostrar somente os erros da execução da tarefa ou seus sucessos e erros.

Casos de uso

Aqui estão algumas situações em que relatórios de tarefa podem ajudar você a monitorar e auditar as transferências de dados:

- Ao migrar milhões de arquivos, identifique rapidamente os arquivos DataSync com problemas de transferência.
- Verifique chain-of-custody os processos dos seus arquivos.

Relatórios de tarefas somente resumidos

Um relatório que é apenas um resumo da execução de uma tarefa inclui os seguintes detalhes:

- O Conta da AWS que executou a execução da tarefa
- Os locais de origem e de destino
- O número total de arquivos, objetos e pastas que foram ignorados, transferidos, verificados e excluídos
- O total de bytes (lógicos e físicos) que foram transferidos
- Se a execução da tarefa foi concluída, cancelada ou encontrou algum erro
- Os horários de início e término (incluindo o tempo total da transferência)
- As configurações da tarefa (como limites de largura de banda, verificação da integridade dos dados e outras opções para sua DataSync transferência)

Relatórios de tarefas padrão

Um relatório de tarefas padrão inclui um [resumo](#) da execução da tarefa, além de relatórios detalhados sobre quais DataSync tentativas transferir, ignorar, verificar e excluir.

Tópicos

- [Nível do relatório](#)
- [Relatórios de transferidos](#)
- [Relatórios de ignorados](#)
- [Relatórios verificados](#)
- [Relatório de excluídos](#)

Nível do relatório

Com os relatórios de tarefas padrão, você pode escolher um dos seguintes níveis de relatório:

- Somente erros
- Sucessos e erros (essencialmente uma lista de tudo o que aconteceu durante a execução da tarefa)

Por exemplo, talvez você queira ver quais arquivos DataSync foram ignorados com sucesso durante a transferência e quais não foram. Os arquivos que DataSync foram ignorados com sucesso podem ser aqueles que você deseja DataSync excluir propositalmente porque eles já existem no seu local de destino. No entanto, um erro ignorado, por exemplo, pode indicar que DataSync ele não tem as permissões corretas para ler um arquivo.

Relatórios de transferidos

Uma lista de arquivos, objetos e diretórios que DataSync tentaram ser transferidos durante a execução da tarefa. Um relatório de transferidos inclui os seguintes detalhes:

- Os caminhos para os dados transferidos
- O que foi transferido (conteúdo, metadados ou ambos)
- Os metadados, que incluem o tipo de dados, o tamanho do conteúdo (somente objetos e arquivos) e muito mais
- A hora em que um item foi transferido
- A versão do objeto (se o destino for um bucket do Amazon S3 com versionamento habilitado)
- Se algo foi sobrescrito no destino
- Se um item foi transferido com sucesso

Note

Ao mover dados entre buckets do S3, o prefixo que você especifica no seu [local de origem](#) pode aparecer no seu relatório (ou nos CloudWatch registros da Amazon), mesmo que esse prefixo não exista como um objeto no seu local de destino. (No DataSync console, você também pode notar que esse prefixo aparece como dados ignorados ou verificados.)

Relatórios de ignorados

Uma lista de arquivos, objetos e diretórios DataSync encontrados no local de origem, mas que não tentaram transferir. Os motivos pelos quais DataSync os dados são ignorados podem depender de vários fatores, como a forma como você configura suas tarefas e as permissões do sistema de armazenamento. Veja alguns exemplos:

- Existe um arquivo nos locais de origem e de destino. O arquivo na origem não foi modificado desde a execução anterior da tarefa. Como você está [transferindo apenas dados que foram alterados](#), DataSync não transfere esse arquivo na próxima vez que executar sua tarefa.
- Um objeto que existe em ambas as suas localizações muda em sua fonte. Ao executar sua tarefa, DataSync ignora esse objeto em seu destino porque sua tarefa não [sobrescreve os dados no destino](#).
- DataSync ignora um objeto em sua fonte que está usando uma [classe de armazenamento de arquivamento](#) e não é restaurado. Você deve restaurar um objeto arquivado DataSync para poder lê-lo.
- DataSync ignora um arquivo, objeto ou diretório em seu local de origem porque não consegue lê-lo. Se isso acontecer e não for esperado, verifique as permissões de acesso do seu armazenamento e certifique-se de que ele DataSync possa ler o que foi ignorado.

Um relatório de ignorados inclui os seguintes detalhes:

- Os caminhos para dados ignorados
- A hora em que um item foi ignorado
- O motivo pelo qual foi ignorado
- Se um item foi ignorado com sucesso

Note

Os relatórios de ignorados podem ser grandes quando incluem sucessos e erros, você configura a tarefa para [transferir apenas os dados que foram alterados](#) e os dados de origem já existem no destino.

Relatórios verificados

Uma lista de arquivos, objetos e diretórios que DataSync tentaram verificar a integridade durante a execução da tarefa. Um de verificados inclui os seguintes detalhes:

- Os caminhos para dados verificados
- A hora em que um item foi verificado
- O motivo da falha na verificação (se for o caso)

- As SHA256 somas de verificação de origem e destino (somente arquivos)
- Se um item foi verificado com sucesso

Observe o seguinte sobre os relatórios verificados:

- Quando você configura sua tarefa para [verificar somente os dados transferidos](#), DataSync não verifica diretórios em algumas situações nem arquivos ou objetos que falham na transferência. Em ambos os casos, DataSync não inclui dados não verificados neste relatório.
- Se você estiver usando o [modo Avançado](#), a verificação poderá demorar mais do que o normal se você estiver transferindo objetos grandes.

Relatório de excluídos

Uma lista de arquivos, diretórios e objetos que foram excluídos durante a execução da tarefa. DataSync gera esse relatório somente se você [configurar sua tarefa](#) para excluir dados no local de destino que não esteja na origem. Um relatório de dados excluídos inclui os seguintes detalhes:

- Os caminhos para dados excluídos
- Se um item foi excluído com sucesso
- A hora em que um item foi excluído

Exemplos de relatórios de tarefa

Você define o nível de detalhe em seu relatório de tarefas. Aqui estão alguns exemplos de relatórios de dados transferidos com a seguinte configuração:

- Tipo de relatório: padrão
- Nível do relatório: sucessos e erros

Note

Os relatórios usam o padrão ISO-8601 para o formato de carimbo de data/hora. Os horários estão em UTC e medidos em nanossegundos. Esse comportamento difere de como algumas outras métricas do relatório de tarefas são medidas. Por exemplo, [detalhes da execução da tarefa](#), como `TransferDuration` e `VerifyDuration`, são medidos em milissegundos.

Os relatórios de tarefas do modo aprimorado usam um esquema um pouco diferente dos relatórios de tarefas do modo Básico. Os exemplos a seguir podem ajudá-lo a saber o que esperar dos seus relatórios, dependendo do [modo de tarefa](#) usado.

Exemplo de relatórios de dados transferidos com status de sucesso

Os relatórios a seguir mostram transferências bem-sucedidas para um objeto chamado `object1.txt`.

Enhanced mode

```
{
  "TaskExecutionId": "exec-abcdefgh12345678",
  "Transferred": [{
    "RelativePath": "object1.txt",
    "SourceMetadata": {
      "Type": "Object",
      "ContentSize": 6,
      "LastModified": "2024-10-04T14:40:55Z",
      "SystemMetadata": {
        "ContentType": "binary/octet-stream",
        "ETag": "\"9b2d7e1f8054c3a2041905d0378e6f14\"",
        "ServerSideEncryption": "AES256"
      },
      "UserMetadata": {},
      "Tags": []
    },
    "Overwrite": "False",
    "DstS3VersionId": "jqtRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
    "TransferTimestamp": "2024-10-04T14:48:39.748862183Z",
    "TransferType": "CONTENT_AND_METADATA",
    "TransferStatus": "SUCCESS"
  ]
}
```

Basic mode

```
{
  "TaskExecutionId": "exec-abcdefgh12345678",
  "Transferred": [{
    "RelativePath": "/object1.txt",
    "SrcMetadata": {
      "Type": "Regular",
```

```

        "ContentSize": 6,
        "Mtime": "2022-01-07T16:59:26.136114671Z",
        "Atime": "2022-01-07T16:59:26.136114671Z",
        "Uid": 0,
        "Gid": 0,
        "Mode": "0644"
    },
    "Overwrite": "False",
    "DstS3VersionId": "jttqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
    "TransferTimestamp": "2022-01-07T16:59:45.747270957Z",
    "TransferType": "CONTENT_AND_METADATA",
    "TransferStatus": "SUCCESS"
  ]
}

```

Exemplo de relatórios de dados transferidos com status de erro

Os relatórios a seguir fornecem exemplos de quando não é DataSync possível transferir um objeto chamado `object1.txt`.

Enhanced mode

Esse relatório mostra que não DataSync consigo acessar um objeto chamado `object1.txt` devido a um problema de AWS KMS permissões. (Se receber um erro como esse, consulte [Acessar buckets do S3 usando criptografia no lado do servidor.](#))

```

{
  "TaskExecutionId": "exec-abcdefgh12345678",
  "Transferred": [{
    "RelativePath": "object1.txt",
    "SourceMetadata": {
      "Type": "Object",
      "ContentSize": 6,
      "LastModified": "2022-10-07T20:48:32Z",
      "SystemMetadata": {
        "ContentType": "binary/octet-stream",
        "ETag": "\"3a7c0b2f1d9e5c4a6f8b2e0d1c9f7a3b2\"",
        "ServerSideEncryption": "AES256"
      },
      "UserMetadata": {},
      "Tags": []
    },
    "Overwrite": "False",

```

```

    "TransferTimestamp": "2022-10-09T16:05:11.134040717Z",
    "TransferType": "CONTENT_AND_METADATA",
    "TransferStatus": "FAILED",
    "ErrorCode": "AccessDenied",
    "ErrorDetail": "User: arn:aws:sts::111222333444:assumed-role/
AWSDataSyncS3Bucket/AwsSync-loc-0b3017fc4ba4a2d8d is not authorized
to perform: kms:GenerateDataKey on resource: arn:aws:kms:us-
east-1:111222333444:key/1111aaaa-22bb-33cc-44d-5555eeee6666 because no identity-
based policy allows the kms:GenerateDataKey action"
  ]
}

```

Basic mode

Esse relatório mostra que um objeto denominado `object1.txt` não foi transferido devido a um problema de permissões do bucket do S3. (Se receber um erro como esse, consulte [Fornecendo DataSync acesso aos buckets do S3.](#))

```

{
  "TaskExecutionId": "exec-abcdefgh12345678",
  "Transferred": [{
    "RelativePath": "/object1.txt",
    "SrcMetadata": {
      "Type": "Regular",
      "ContentSize": 6,
      "Mtime": "2022-01-07T16:59:26.136114671Z",
      "Atime": "2022-01-07T16:59:26.136114671Z",
      "Uid": 0,
      "Gid": 0,
      "Mode": "0644"
    },
    "Overwrite": "False",
    "DstS3VersionId": "jqtqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
    "TransferTimestamp": "2022-01-07T16:59:45.747270957Z",
    "TransferType": "CONTENT_AND_METADATA",
    "TransferStatus": "FAILED",
    "FailureReason": "S3 Get Object Failed",
    "FailureCode": 40974
  ]
}

```

Limitações

- Os relatórios de tarefas individuais não podem exceder 5 MB. Se você estiver copiando um grande número de arquivos, seu relatório de tarefas poderá ser dividido em vários relatórios.
- Há situações em que criar relatórios de tarefa pode afetar a performance da transferência de dados. Por exemplo, isso pode ser percebido quando a conexão de rede tem alta latência e os arquivos sendo transferidos são pequenos ou você só está copiando alterações de metadados.

Criando seus relatórios de DataSync tarefas

AWS DataSync os relatórios de tarefas podem ser apenas um resumo da execução da tarefa ou um conjunto de relatórios detalhados sobre quais DataSync tentativas transferir, ignorar, verificar e excluir.

Pré-requisitos

Antes de poder criar um relatório de tarefas, é necessário fazer o seguinte.

Tópicos

- [Criar um bucket do S3 para os relatórios de tarefa](#)
- [Permita DataSync o upload de relatórios de tarefas para seu bucket do S3](#)

Criar um bucket do S3 para os relatórios de tarefa

Se você ainda não tiver um, [crie um bucket do S3](#) para DataSync fazer o upload do seu relatório de tarefas. Os relatórios são armazenados na classe de armazenamento S3 Standard.

Recomendamos o seguinte para esse bucket:

- Se você planeja transferir dados para um bucket do S3, não use o mesmo bucket para seu relatório de tarefa se você [desativar a opção Manter arquivos excluídos](#). Caso contrário, DataSync excluirá todos os relatórios de tarefas anteriores sempre que você executar uma tarefa, pois esses relatórios não existem no seu local de origem.
- Para evitar uma configuração complexa de permissões de acesso, verifique se o bucket do relatório de tarefas está na mesma Conta da AWS região da tarefa DataSync de transferência.

Permita DataSync o upload de relatórios de tarefas para seu bucket do S3

Você deve configurar uma função AWS Identity and Access Management (IAM) que permita DataSync fazer o upload de um relatório de tarefas para seu bucket do S3.

No DataSync console, você pode criar uma função do IAM que, na maioria dos casos, inclui automaticamente as permissões para carregar um relatório de tarefas no seu bucket. Lembre-se de que essa função gerada automaticamente pode não atender às suas necessidades do ponto de vista de privilégios mínimos. Essa função também não funcionará se seu bucket for criptografado com uma chave gerenciada pelo cliente AWS Key Management Service (AWS KMS) (SSE-KMS). Nesses casos, você pode criar a função manualmente, desde que ela faça pelo menos o seguinte:

- [Prevenção do problema de anexo confuso](#) na entidade confiável da função.

O exemplo completo a seguir mostra como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves de contexto para evitar o problema confuso do substituto com DataSync.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:datasync:us-
east-2:123456789012:*"
        }
      }
    }
  ]
}
```

- Permite DataSync fazer o upload de um relatório de tarefas para seu bucket do S3.

O exemplo a seguir faz isso incluindo a ação `s3:PutObject` somente para um prefixo específico (`reports/`) em seu bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "s3:PutObject"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::your-task-reports-bucket/reports/*"
  }]
}
```

- Se seu bucket do S3 for criptografado com uma chave SSE-KMS gerenciada pelo cliente, a [política da chave](#) deverá incluir a função do IAM DataSync usada para acessar o bucket.

Para obter mais informações, consulte [Acessar buckets do S3 usando criptografia no lado do servidor](#).

Criar um relatório de tarefas somente resumido

Você pode configurar um relatório de tarefas que inclua um [resumo somente](#) ao criar sua DataSync tarefa, iniciá-la ou atualizá-la.

As etapas a seguir mostram como configurar um relatório de tarefas somente resumido ao criar uma tarefa.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

4. Role para baixo até a seção Relatório de tarefa. Em Tipo de relatório, escolha Resumo somente.
5. Para o bucket do S3 para relatórios, escolha um bucket do S3 no qual você deseja DataSync fazer o upload do seu relatório de tarefas.

 Tip

Se você planeja transferir dados para um bucket do S3, não use o mesmo bucket para seu relatório de tarefa se você [desativar a opção Manter arquivos excluídos](#). Caso contrário, DataSync excluirá todos os relatórios de tarefas anteriores sempre que você executar uma tarefa, pois esses relatórios não existem no seu local de origem.

6. Em Pasta, insira um prefixo para usar no seu relatório de tarefas ao DataSync carregar o relatório no seu bucket do S3 (por exemplo,). **reports/**

Certifique-se de incluir o caractere delimitador apropriado no final do prefixo. Esse caractere geralmente é uma barra para frente (/). Para obter mais informações, consulte [Organizando objetos usando prefixos](#) no Guia de usuário do Amazon S3.

7. Em Perfil do IAM, siga um destes procedimentos:
 - Escolha Autogenerate para criar DataSync automaticamente uma função do IAM com as permissões necessárias para acessar o bucket do S3.

Se uma função do IAM foi criada DataSync anteriormente para esse bucket do S3, essa função é escolhida por padrão.

- Escolha um perfil do IAM personalizado que você criou.

Em alguns casos, talvez seja necessário criar o perfil por conta própria. Para obter mais informações, consulte [Permita DataSync o upload de relatórios de tarefas para seu bucket do S3](#).

 Important

Se seu bucket do S3 for criptografado com uma chave SSE-KMS gerenciada pelo cliente, a política da chave deverá incluir a função do IAM DataSync usada para acessar o bucket.

Para obter mais informações, consulte [Acessar buckets do S3 usando criptografia no lado do servidor](#).

8. Conclua a criação da tarefa e, em seguida, [inicie a tarefa](#) para começar a transferir seus dados.

Quando sua transferência estiver concluída, você poderá [visualizar seu relatório de tarefa](#).

Usando o AWS CLI

1. Copie o seguinte comando create-task AWS Command Line Interface (AWS CLI):

```
aws datasync create-task \
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh \
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-abcdefgh12345678 \
  --task-report-config '{
    "Destination":{
      "S3":{
        "Subdirectory":"reports/",
        "S3BucketArn":"arn:aws:s3:::your-task-reports-bucket",
        "BucketAccessRoleArn":"arn:aws:iam::123456789012:role/bucket-iam-role"
      }
    },
    "OutputType":"SUMMARY_ONLY"
  }'
```

2. Para o parâmetro `--source-location-arn`, especifique o nome do recurso da Amazon (ARN) do local de origem na transferência. `us-east-1` Substitua pelo apropriado Região da AWS, `123456789012` substitua pelo Conta da AWS número apropriado e `12345678abcdefgh` substitua pelo ID do local de origem apropriado.
3. No parâmetro `--destination-location-arn`, especifique o ARN do local de destino em sua transferência. `us-east-1` Substitua pelo apropriado Região da AWS, `123456789012` substitua pelo Conta da AWS número apropriado e `abcdefgh12345678` substitua pelo ID do local de destino apropriado.
4. No parâmetro `--task-report-config` faça o seguinte:
 - `Subdirectory`— `reports/` Substitua pelo prefixo no bucket do S3 em que você deseja DataSync fazer o upload dos relatórios de tarefas.

Certifique-se de incluir o caractere delimitador apropriado no final do prefixo. Esse caractere geralmente é uma barra para frente (/). Para obter mais informações, consulte [Organizando objetos usando prefixos](#) no Guia de usuário do Amazon S3.

- `S3BucketArn`: especifique o ARN do bucket do S3 no qual deseja fazer upload do relatório de tarefa.

 Tip

Se você planeja transferir dados para um bucket do S3, não use o mesmo bucket para seu relatório de tarefas se você [desativar a opção Manter arquivos excluídos](#). Caso contrário, DataSync excluirá todos os relatórios de tarefas anteriores sempre que você executar uma tarefa, pois esses relatórios não existem no seu local de origem.

- `BucketAccessRoleArn`— Especifique a função do IAM que permite DataSync fazer o upload de um relatório de tarefas para seu bucket do S3.

Para obter mais informações, consulte [Permita DataSync o upload de relatórios de tarefas para seu bucket do S3](#).

 Important

Se seu bucket do S3 for criptografado com uma chave SSE-KMS gerenciada pelo cliente, a política da chave deverá incluir a função do IAM DataSync usada para acessar o bucket.

Para obter mais informações, consulte [Acessar buckets do S3 usando criptografia no lado do servidor](#).

- `OutputType`: especifique `SUMMARY_ONLY`.

Para obter mais informações, consulte [Relatórios de tarefas somente resumidos](#).

5. Execute o comando `create-task` para criar sua tarefa.

Você recebe uma resposta como a seguinte, que mostra o ARN da tarefa que você criou. Você precisará desse ARN para executar o comando `start-task-execution`.

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
}
```

6. Copie o seguinte comando `start-task-execution`:

```
aws datasync-task-report start-task-execution \
```

```
--task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

7. Para o parâmetro `--task-arn`, especifique o ARN da tarefa que você está iniciando. Use o ARN que você recebeu ao executar o comando `create-task`.
8. Execute o comando `start-task-execution`.

Quando sua transferência estiver concluída, você poderá [visualizar seu relatório de tarefa](#).

Criar um relatório de tarefas padrão

Você pode configurar um [relatório de tarefas padrão](#) ao criar sua DataSync tarefa, iniciá-la ou atualizá-la.

As etapas a seguir mostram como configurar um relatório de tarefas padrão ao criar uma tarefa.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

4. Role para baixo até a seção Relatório de tarefa. Em Relatório de tarefa, escolha Relatório padrão.
5. Em Nível de relatório, escolha uma das seguintes opções:
 - Somente erros — Seu relatório de tarefas inclui apenas problemas com o que você DataSync tentou transferir, ignorar, verificar e excluir.
 - Sucessos e erros — Seu relatório de tarefas inclui o que foi transferido, ignorado, verificado e excluído DataSync com sucesso e o que não foi.
 - Personalizado: permite que você escolha se deseja ver somente erros ou sucessos e erros em aspectos específicos do seu relatório de tarefas.

Por exemplo, você pode escolher Sucessos e erros para a lista de arquivos transferidos, mas Somente erros para o restante do relatório.

6. Se você estiver transferindo para um bucket do S3 que usa controle de versão de objetos, mantenha a opção **Incluir versões de objetos do Amazon S3** selecionada se quiser que seu relatório inclua a nova versão para cada objeto transferido.
7. Para o bucket do S3 para relatórios, escolha um bucket do S3 no qual você deseja DataSync fazer o upload do seu relatório de tarefas.

 Tip

Se você planeja transferir dados para um bucket do S3, não use o mesmo bucket para seu relatório de tarefa se você [desativar a opção Manter arquivos excluídos](#). Caso contrário, DataSync excluirá todos os relatórios de tarefas anteriores sempre que você executar uma tarefa, pois esses relatórios não existem no seu local de origem.

8. Em Pasta, insira um prefixo para usar no seu relatório de tarefas ao DataSync carregar o relatório no seu bucket do S3 (por exemplo,). **reports/** Certifique-se de incluir o caractere delimitador apropriado no final do prefixo. Esse caractere geralmente é uma barra para frente (/). Para obter mais informações, consulte [Organizando objetos usando prefixos](#) no Guia de usuário do Amazon S3.
9. Em Perfil do IAM, siga um destes procedimentos:
 - Escolha Autogenerate para criar DataSync automaticamente uma função do IAM com as permissões necessárias para acessar o bucket do S3.

Se uma função do IAM foi criada DataSync anteriormente para esse bucket do S3, essa função é escolhida por padrão.

- Escolha um perfil do IAM personalizado que você criou.

Em alguns casos, talvez seja necessário criar o perfil por conta própria. Para obter mais informações, consulte [Permita DataSync o upload de relatórios de tarefas para seu bucket do S3](#).

 Important

Se seu bucket do S3 for criptografado com uma chave SSE-KMS gerenciada pelo cliente, a política da chave deverá incluir a função do IAM DataSync usada para acessar o bucket.

Para obter mais informações, consulte [Acessar buckets do S3 usando criptografia no lado do servidor](#).

10. Conclua a criação da tarefa e [inicie a tarefa](#) para começar a transferir seus dados.

Quando sua transferência estiver concluída, você poderá [visualizar seu relatório de tarefa](#).

Usando o AWS CLI

1. Copie o seguinte comando create-task:

```
aws datasync create-task \
  --source-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-12345678abcdefgh \
  --destination-location-arn arn:aws:datasync:us-east-1:123456789012:location/
loc-abcdefgh12345678 \
  --task-report-config '{
    "Destination":{
      "S3":{
        "Subdirectory":"reports/",
        "S3BucketArn":"arn:aws:s3:::your-task-reports-bucket",
        "BucketAccessRoleArn":"arn:aws:iam::123456789012:role/bucket-iam-role"
      }
    },
    "OutputType":"STANDARD",
    "ReportLevel":"level-of-detail",
    "ObjectVersionIds":"include-or-not"
  }'
```

2. Para o parâmetro `--source-location-arn`, especifique o ARN do local de origem na transferência. `us-east-1` substitua pelo apropriado Região da AWS, `123456789012` substitua pelo Conta da AWS número apropriado e `12345678abcdefgh` substitua pelo ID do local de origem apropriado.
3. No parâmetro `--destination-location-arn`, especifique o ARN do local de destino em sua transferência. `us-east-1` substitua pelo apropriado Região da AWS, `123456789012` substitua pelo Conta da AWS número apropriado e `abcdefgh12345678` substitua pelo ID do local de destino apropriado.
4. No parâmetro `--task-report-config` faça o seguinte:

- **Subdirectory**— *reports/* Substitua pelo prefixo no bucket do S3 em que você deseja DataSync fazer o upload dos relatórios de tarefas. Certifique-se de incluir o caractere delimitador apropriado no final do prefixo. Esse caractere geralmente é uma barra para frente (/). Para obter mais informações, consulte [Organizando objetos usando prefixos](#) no Guia de usuário do Amazon S3.
- **S3BucketArn**: especifique o ARN do bucket do S3 no qual deseja fazer upload do relatório de tarefa.

 Tip

Se você planeja transferir dados para um bucket do S3, não use o mesmo bucket para seu relatório de tarefas se você [desativar a opção Manter arquivos excluídos](#). Caso contrário, DataSync excluirá todos os relatórios de tarefas anteriores sempre que você executar uma tarefa, pois esses relatórios não existem no seu local de origem.

- **BucketAccessRoleArn**— Especifique a função do IAM que permite DataSync fazer o upload de um relatório de tarefas para seu bucket do S3.

Para obter mais informações, consulte [Permita DataSync o upload de relatórios de tarefas para seu bucket do S3](#).

 Important

Se seu bucket do S3 for criptografado com uma chave SSE-KMS gerenciada pelo cliente, a política da chave deverá incluir a função do IAM DataSync usada para acessar o bucket.

Para obter mais informações, consulte [Acessar buckets do S3 usando criptografia no lado do servidor](#).

- **OutputType**: especifique o relatório STANDARD.

Para obter mais informações sobre tipos de dados, consulte [Relatórios de tarefas padrão](#) Tipos de relatórios de tarefas.

- (Opcional) **ReportLevel**: especifique se você deseja ERRORS_ONLY (o padrão) ou SUCCESSES_AND_ERRORS em seu relatório.

- (Opcional) `ObjectVersionIds`: se você estiver fazendo uma transferência para um bucket do S3 que usa controle de versionamento de objetos, especifique `NONE` se não deseja incluir a nova versão de cada objeto transferido no relatório.

Essa opção é definida como `INCLUDE` por padrão.

- (Opcional) `Overrides`: personalize o `ReportLevel` de um aspecto específico do seu relatório.

Por exemplo, talvez você queira ver `SUCCESSES_AND_ERRORS` a lista do que é DataSync excluído em seu local de destino, mas quer ver todo `ERRORS_ONLY` o resto. Neste exemplo, você adicionaria a seguinte opção `Overrides` ao parâmetro `--task-report-config`:

```
"Overrides":{
  "Deleted":{
    "ReportLevel":"SUCCESSES_AND_ERRORS"
  }
}
```

Se você não usar `Overrides`, todo o relatório usará o `ReportLevel` que você especificar.

5. Execute o comando `create-task` para criar sua tarefa.

Você recebe uma resposta como a seguinte, que mostra o ARN da tarefa que você criou. Você precisará desse ARN para executar o comando `start-task-execution`.

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
}
```

6. Copie o seguinte comando `start-task-execution`:

```
aws datasync-task-report start-task-execution \
  --task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

7. Para o parâmetro `--task-arn`, especifique o ARN da tarefa que você está executando. Use o ARN que você recebeu ao executar o comando `create-task`.
8. Execute o comando `start-task-execution`.

Quando sua transferência estiver concluída, você poderá [visualizar seu relatório de tarefa](#).

Visualizando seus relatórios de DataSync tarefas

DataSync cria relatórios de tarefas para cada execução de tarefa. Quando a execução é concluída, você pode encontrar os relatórios de tarefa relacionados no bucket do S3. Os relatórios de tarefas são organizados sob prefixos que incluem suas tarefas e suas execuções. IDs

Para ajudar a localizar relatórios de tarefas em seu bucket do S3, use estes exemplos:

- Relatório de tarefas somente resumido: *reports-prefix/Summary-Reports/task-id-folder/task-execution-id-folder*
- Relatório de tarefas padrão: *reports-prefix/Detailed-Reports/task-id-folder/task-execution-id-folder*

Como os relatórios de tarefa são no formato JSON, você tem várias opções para visualizá-los:

- Visualize um relatório usando o [Amazon S3 Select](#).
- Visualize relatórios usando AWS serviços como AWS Glue Amazon Athena e Amazon. QuickSight
Para obter mais informações sobre visualização de relatórios de tarefa, consulte o [Blog sobre armazenamento da AWS](#).

Monitoramento de transferências de dados com o Amazon CloudWatch Logs

Você pode monitorar sua AWS DataSync transferência usando o CloudWatch Logs. Recomendamos que você configure sua tarefa para, pelo menos, registrar informações básicas (como erros de transferência).

DataSync Permitindo o upload de registros para um grupo de CloudWatch registros

Para [configurar o registro](#) para sua DataSync tarefa, você precisa de um grupo de CloudWatch registros que DataSync tenha permissão para enviar registros para. Você configura esse acesso por meio de uma função AWS Identity and Access Management (IAM). A forma como isso funciona especificamente depende do seu [modo de tarefa](#).

Enhanced mode

Com o modo Avançado, envia DataSync automaticamente os registros de tarefas para um grupo de registros chamado `/aws/datasync`. Se esse grupo de registros não existir no seu Região da AWS, DataSync crie o grupo de registros em seu nome usando uma [função vinculada ao serviço](#) do IAM ao criar sua tarefa.

Basic mode

Há algumas maneiras de configurar um grupo de CloudWatch registros para uma DataSync tarefa usando o modo Básico. No console, você pode criar automaticamente uma função do IAM que, na maioria dos casos, inclui as permissões DataSync necessárias para carregar registros. Lembre-se de que essa função gerada automaticamente pode não atender às suas necessidades do ponto de vista de privilégios mínimos.

Se você quiser usar um grupo de CloudWatch registros existente ou estiver criando suas tarefas programaticamente, você mesmo deverá criar a função do IAM.

O exemplo a seguir é uma política do IAM que concede essas permissões.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataSyncLogsToCloudWatchLogs",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:datasync:region:account-id:task/*"
          ]
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

```
    },  
    "Resource": "arn:aws:logs:region:account-id:log-group:*:*"  
  }  
]  
}
```

A política usa Condition declarações para ajudar a garantir que somente DataSync as tarefas da conta especificada tenham acesso ao grupo de CloudWatch registros especificado. Recomendamos usar as chaves de contexto de condição global [aws:SourceArn](#) e [aws:SourceAccount](#) nessas declarações Condition para se proteger contra o confuso problema do substituto. Para obter mais informações, consulte [Prevenção contra o ataque do “substituto confuso” em todos os serviços](#).

Para especificar a DataSync tarefa ou tarefas, *region* substitua pelo código da região Região da AWS onde as tarefas estão localizadas (por exemplo, *us-west-2*) e *account-id* substitua pela Conta da AWS ID da conta que contém as tarefas. Para especificar o grupo de CloudWatch registros, substitua os mesmos valores. Você também pode modificar a instrução Resource para atingir grupos de logs específicos. Para obter mais informações sobre usar SourceArn e SourceAccount, consulte [Chaves de condição global](#) no Guia do usuário do IAM.

Para aplicar a política, salve essa instrução de política em um arquivo no computador local. Em seguida, execute o AWS CLI comando a seguir para aplicar a política de recursos. Para usar esse exemplo de comando, substitua *full-path-to-policy-file* pelo caminho do arquivo que contém a instrução da política.

```
aws logs put-resource-policy --policy-name trust-datasync --policy-document  
file://full-path-to-policy-file
```

 Note

Execute esse comando usando o mesmo Conta da AWS e Região da AWS onde você ativou seu DataSync agente.

Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch Logs](#).

Configurando o registro para sua tarefa DataSync

Recomendamos que você configure pelo menos algum nível de registro para sua DataSync tarefa.

Antes de começar

DataSync precisa de permissão para carregar registros em um grupo de CloudWatch registros. Para obter mais informações, consulte [DataSync Permitindo o upload de registros para um grupo de CloudWatch registros](#).

Usar o console de DataSync

As instruções a seguir descrevem como configurar o CloudWatch registro ao criar uma tarefa. Você também pode configurar o registro ao editar uma tarefa.

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados, escolha Tarefas e, em seguida, escolha Criar tarefa.
3. Configure os locais de origem e destino da sua tarefa.

Para obter mais informações, consulte [Para onde posso transferir meus dados com AWS DataSync?](#).

4. Na página Definir configurações, escolha um [modo de tarefa](#) e quaisquer outras opções.

Talvez você esteja interessado em algumas das seguintes opções:

- Especifique quais dados transferir usando um [manifesto](#) ou [filtros](#).
 - Configure como [lidar com metadados de arquivos](#) e [verificar a integridade dos dados](#).
5. Em Eventos de log, selecione uma das seguintes opções:
 - Registrar em log informações básicas como erros de transferência: publicar logs apenas com informações básicas (tais como erros de transferência).
 - Registre todos os objetos e arquivos transferidos — publique registros de todos os arquivos ou objetos DataSync transferidos e realize verificações de integridade de dados.
 - Não gere registros
 6. Siga um destes procedimentos, dependendo do modo de tarefa que você está usando para criar ou especificar um grupo de CloudWatch registros:

Enhanced mode

Quando você escolhe Criar tarefa, usa (ou cria) DataSync automaticamente um grupo de registros chamado `/aws/datasync`.

Basic mode

Para grupo de CloudWatch registros, especifique um grupo de registros que DataSync tenha permissão para fazer upload de registros fazendo o seguinte:

- Escolha Geração automática para criar automaticamente um grupo de registros que permita DataSync fazer upload de registros para ele.
- Escolha um grupo de logs existente na sua Região da AWS atual.

Se você escolher um grupo de registros existente, verifique se ele [DataSync tem permissão](#) para fazer upload de registros para esse grupo de registros.

7. Escolha Criar tarefa.

Você está pronto para [iniciar a tarefa](#).

Usando o AWS CLI

1. Copie o seguinte comando `create-task`:

```
aws datasync create-task \
  --source-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --destination-location-arn "arn:aws:datasync:us-east-1:account-id:location/location-id" \
  --task-mode "ENHANCED-or-BASIC" \
  --name "task-name" \
  --options '{"LogLevel": "log-level"}' \
  --cloudwatch-log-group-arn "arn:aws:logs:us-east-1:account-id:log-group:log-group-name:"
```

2. Em `--source-location-arn`, especifique o nome do recurso da Amazon (ARN) do local de origem na transferência.
3. Em `--destination-location-arn`, especifique o ARN do local de destino.

Se você estiver transferindo entre Regiões da AWS nossas contas, verifique se o ARN inclui a outra ID de região ou conta.

4. Para `--task-mode`, especifique `ENHANCED` ou `BASIC`.
5. (Recomendado) Em `--name`, especifique um nome para a tarefa de que você possa se lembrar.
6. Para `LogLevel`, especifique uma das seguintes opções:
 - `BASIC`— Publique registros somente com informações básicas (como erros de transferência).
 - `TRANSFER`— publique registros de todos os arquivos ou objetos que DataSync transferem e realizam verificações de integridade de dados.
 - `NONE`— Não gere registros.
7. Para `--cloudwatch-log-group-arn`, especifique o ARN de um grupo de CloudWatch registros.

 Important

Se `--task-mode` for o seu `ENHANCED`, você não precisa especificar essa opção. Para obter mais informações, consulte [DataSync Permitindo o upload de registros para um grupo de CloudWatch registros](#).

8. Execute o comando `create-task`.

Se o comando for bem-sucedido, você receberá uma resposta que mostra o ARN da tarefa que você criou. Por exemplo:

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Você está pronto para [iniciar a tarefa](#).

Usando a DataSync API

Você pode configurar o CloudWatch registro para sua tarefa usando o `CloudWatchLogGroupArn` parâmetro com qualquer uma das seguintes operações:

- [CreateTask](#)

- [UpdateTask](#)

Visualizando registros de DataSync tarefas

Ao [iniciar sua tarefa](#), você pode visualizar os registros da execução da tarefa usando o CloudWatch console ou AWS CLI (entre outras opções). Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch Logs](#).

DataSync fornece registros estruturados em JSON para tarefas do modo Avançado. As tarefas do modo básico têm registros não estruturados. Os exemplos a seguir mostram como os erros de verificação são exibidos nos registros do modo Avançado em comparação com os registros do modo Básico.

Enhanced mode log example

```
{
  "Action": "VERIFY",
  "Source": {
    "LocationId": "loc-abcdef01234567890",
    "RelativePath": "directory1/directory2/file1.txt"
  },
  "Destination": {
    "LocationId": "loc-05ab2fdc272204a5f",
    "RelativePath": "directory1/directory2/file1.txt",
    "Metadata": {
      "Type": "Object",
      "ContentSize": 66060288,
      "LastModified": "2024-10-03T20:46:58Z",
      "S3": {
        "SystemMetadata": {
          "ContentType": "binary/octet-stream",
          "ETag": "\"1234abcd5678efgh9012ijkl3456mnop\"",
          "ServerSideEncryption": "AES256"
        },
        "UserMetadata": {
          "file-mtime": "1602647222/222919600"
        },
        "Tags": {}
      }
    }
  },
  "ErrorCode": "FileNotAtSource",
```

```
"ErrorDetail": "Verification failed due to file being present at the destination  
but not at the source"  
}
```

Basic mode log example

```
[NOTICE] Verification failed > /directory1/directory2/file1.txt  
[NOTICE] /directory1/directory2/file1.txt    dstMeta: type=R mode=0755 uid=65534  
gid=65534 size=8972938 atime=1728657659/0 mtime=1728657659/0 extAttrsHash=0  
[NOTICE]    dstHash: f9c2cca900301d38b0930367d8d587153154af467da0fdcf1bebc0848ec72c0d
```

Registrando chamadas de AWS DataSync API com AWS CloudTrail

AWS DataSync é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um AWS service (Serviço da AWS) usuário DataSync. CloudTrail captura todas as chamadas de API DataSync como eventos. As chamadas capturadas incluem chamadas do DataSync console e chamadas de código para operações de DataSync API.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para AWS DataSync. 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 DataSync, 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](#).

Trabalhando com DataSync informações em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre em AWS DataSync, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para obter um registro contínuo de eventos na sua Conta da AWS, incluindo eventos para o AWS DataSync, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket

do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as Regiões da AWS na mesma AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para obter mais informações, 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 as DataSync ações são registradas por CloudTrail. (Para obter mais informações, consulte a [referência DataSync da API](#).)

Por exemplo, chamadas para as ListLocations operações CreateAgentCreateTask, e 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 AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para ter mais informações, consulte [CloudTrail userIdentity elemento](#) no Guia do AWS CloudTrail usuário.

Entendendo as entradas do arquivo de DataSync log

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 contém 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 chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a CreateTask operação.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "1234567890abcdef0",
    "arn": "arn:aws:iam::123456789012:user/user1",
    "accountId": "123456789012",
    "accessKeyId": "access key",
    "userName": "user1",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-12-13T14:56:46Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2018-12-13T14:57:02Z",
  "eventSource": "datasync.amazonaws.com",
  "eventName": "CreateTask",
  "awsRegion": "ap-southeast-1",
  "sourceIPAddress": "192.0.2.1",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "cloudWatchLogGroupArn": "arn:aws:logs:ap-southeast-1:123456789012:log-group:MyLogGroup",
    "name": "MyTask-NTIzMzY1",
    "tags": [],
    "destinationLocationArn": "arn:aws:datasync:ap-southeast-1:123456789012:location/loc-abcdef01234567890",
    "options": {
      "bytesPerSecond": -1,
      "verifyMode": "POINT_IN_TIME_CONSISTENT",
      "uid": "INT_VALUE",
      "posixPermissions": "PRESERVE",
      "mtime": "PRESERVE",
      "gid": "INT_VALUE",
      "preserveDevices": "NONE",
      "preserveDeletedFiles": "REMOVE",
      "atime": "BEST_EFFORT"
    }
  }
}
```

```

    },
    "sourceLocationArn": "arn:aws:datasync:ap-southeast-1:123456789012:location/
loc-021345abcdef6789"
  },
  "responseElements": {
    "taskArn": "arn:aws:datasync:ap-southeast-1:123456789012:task/
task-1234567890abcdef0"
  },
  "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}

```

Monitorando eventos usando a Amazon EventBridge

EventBridge Os eventos da Amazon descrevem mudanças nos DataSync recursos. Você pode configurar regras para corresponder a eventos e roteá-los para um ou mais streams ou funções de destino. Os eventos são emitidos com base no melhor esforço.

DataSync eventos de transferência

Os seguintes EventBridge eventos estão disponíveis para DataSync transferências.

Agent state changes

Evento	Descrição
Online	O agente está configurado corretamente e disponível para uso. Esse é o status normal de execução de um agente.
Off-line	O agente esteve fora de contato com o DataSync serviço por cinco minutos ou mais. Isso pode acontecer por alguns motivos. Para obter mais informações, consulte O que eu faço se meu agente estiver off-line? .

Location state changes

Agent state changes

Evento	Descrição
Adicionando	DataSync está adicionando um local.
Available (Disponível)	O local foi criado e está disponível para uso.

Task state changes

Evento	Descrição
Available (Disponível)	A tarefa foi criada e está pronta para ser iniciada.
Em execução	A tarefa está em andamento e funcionando corretamente.
Unavailable (Indisponível)	A tarefa não está configurada corretamente e não pode ser usada. Talvez você veja esse evento quando um agente associado à tarefa ficar off-line.
Enfileirado	Outra tarefa é executar e usar o mesmo agente. DataSync executa tarefas em série (primeiro a entrar, primeiro a sair).

Task execution state changes

Evento	Descrição
Enfileiramento	Outra execução de tarefa é executar e usar o mesmo DataSync agente. Para obter mais informações, consulte Como saber quando a tarefa está na fila .
Launching	DataSync está inicializando a execução da tarefa. Esse status geralmente desaparece rapidamente, mas pode levar até alguns minutos.

Agent state changes

Preparação

DataSync está determinando quais dados transferir.

Essa etapa pode levar apenas alguns minutos ou algumas horas, dependendo do número de arquivos, objetos ou diretórios nos dois locais e de como você configura sua tarefa. A preparação também pode não ser aplicável à sua tarefa. Para obter mais informações, consulte [Como DataSync prepara sua transferência de dados](#).

Em transferência

DataSync está realizando a transferência de dados real.

Verificando

DataSync está realizando uma verificação da integridade dos dados no final da transferência.

Bem-sucedida

A execução da tarefa foi bem-sucedida.

Cancelando

A execução da tarefa está em processo de ser cancelada.

Erro

Houve falha na execução da tarefa.

Monitoramento AWS DataSync com ferramentas manuais

Você pode acompanhar suas AWS DataSync transferências pelo console ou pela linha de comando.

Monitorando sua transferência usando o DataSync console

Você pode monitorar sua DataSync transferência usando o console, que fornece métricas em tempo real, como dados transferidos, taxa de transferência de dados e arquivos e compactação de dados.

Para monitorar sua transferência usando o DataSync console

1. Depois de [iniciar sua DataSync tarefa](#), escolha Ver detalhes da execução.

2. Veja métricas sobre a sua transferência.

Monitorando sua transferência usando o AWS CLI

Você pode monitorar sua DataSync transferência usando o AWS Command Line Interface (AWS CLI).

Copie o seguinte comando `describe-task-execution`: Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
aws datasync describe-task-execution \
  --task-execution-arn 'arn:aws:datasync:region:account-id:task/task-id/execution/task-
  execution-id'
```

Esse comando retornará informações sobre a execução da tarefa, semelhantes às mostradas a seguir.

```
{
  "BytesCompressed": 3500,
  "BytesTransferred": 5000,
  "BytesWritten": 5000,
  "EstimatedBytesToTransfer": 5000,
  "EstimatedFilesToDelete": 10,
  "EstimatedFilesToTransfer": 100,
  "FilesDeleted": 10,
  "FilesSkipped": 0,
  "FilesTransferred": 100,
  "FilesVerified": 100,
  "Result": {
    "ErrorCode": "??????",
    "ErrorDetail": "??????",
    "PrepareDuration": 100,
    "PrepareStatus": "SUCCESS",
    "TransferDuration": 60,
    "TransferStatus": "AVAILABLE",
    "VerifyDuration": 30,
    "VerifyStatus": "SUCCESS"
  },
  "StartTime": 1532660733.39,
  "Status": "SUCCESS",
  "OverrideOptions": {
    "Atime": "BEST_EFFORT",
```

```

    "BytesPerSecond": "1000",
    "Gid": "NONE",
    "Mtime": "PRESERVE",
    "PosixPermissions": "PRESERVE",
    "PreserveDevices": "NONE",
    "PreserveDeletedFiles": "PRESERVE",
    "Uid": "NONE",
    "VerifyMode": "POINT_IN_TIME_CONSISTENT"
  },
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccdddf/execution/exec-1234abcd1234abcd1",
  "TaskReportConfig": {
    "Destination": {
      "S3": {
        "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-datasync-
role",
        "S3BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Subdirectory": "reports"
      }
    },
    "ObjectVersionIds": "INCLUDE",
    "OutputType": "STANDARD",
    "Overrides": {
      "Deleted": {
        "ReportLevel": "ERRORS_ONLY"
      },
      "Skipped": {
        "ReportLevel": "SUCCESSSES_AND_ERRORS"
      },
      "Transferred": {
        "ReportLevel": "ERRORS_ONLY"
      },
      "Verified": {
        "ReportLevel": "ERRORS_ONLY"
      }
    },
    "ReportLevel": "ERRORS_ONLY"
  }
}

```

- Se a execução da tarefa for bem-sucedida, o valor de Status será alterado para SUCCESS (Êxito). Para obter informações sobre o significado dos elementos de resposta, consulte [DescribeTaskExecution](#).

- Se ocorrer uma falha na execução da tarefa, o resultado envia os códigos de erros que podem ajudar a solucionar os problemas. Para obter informações sobre os códigos de erro, consulte [TaskExecutionResultDetail](#).

Monitorando sua transferência usando o utilitário **watch**

Para monitorar o andamento da execução da tarefa em tempo real na linha de comando, você pode usar o utilitário `watch` do padrão do Unix. Os valores da duração da execução da tarefa são medidos em milissegundos.

O `watch` utilitário não reconhece o DataSync alias. O exemplo a seguir mostra como invocar a CLI diretamente. Para usar esse exemplo de comando, substitua os *user input placeholders* por suas próprias informações.

```
# pass '-n 1' to update every second and '-d' to highlight differences
$ watch -n 1 -d \ "aws datasync describe-task-execution --task-execution-arn
'arn:aws:datasync:region:account-id:task/task-id/execution/task execution-id'"
```


Gerenciando AWS DataSync recursos

Aprenda a gerenciar seus AWS DataSync recursos, como agentes, locais e tarefas.

Gerenciando seu DataSync agente

Depois de ativar um DataSync agente, AWS gerencia o agente para você (incluindo atualizações de software). [Saiba mais](#)

Testando a conectividade e os recursos do sistema do seu DataSync agente

Embora AWS gerencie seu DataSync agente depois de implantado e ativado, pode haver casos em que você precise alterar as configurações do agente ou solucionar um problema. [Saiba mais](#)

Substituindo seu DataSync agente

Para substituir um DataSync agente, você deve criar um novo agente e atualizar todos os locais que estão usando o agente antigo. [Saiba mais](#)

Limpando DataSync recursos

Se você usou DataSync para um teste ou simplesmente não precisa mais de seus recursos, exclua esses recursos para que você não seja cobrado por eles. [Saiba mais](#)

Reutilizando a infraestrutura de um DataSync agente

Depois de excluir um recurso do agente DataSync, você ainda pode usar a máquina virtual do agente ou a EC2 instância da Amazon para ativar um novo agente. [Saiba mais](#)

Gerenciando seu AWS DataSync agente

Depois de [ativar um AWS DataSync agente](#), AWS gerencia o dispositivo de máquina virtual (VM) para você.

Atualizações de software de agente

AWS atualiza automaticamente o software do seu agente, incluindo o sistema operacional subjacente e os pacotes DataSync de software relacionados.

DataSync atualiza seu agente somente quando ele está ocioso. Por exemplo, seu agente não será atualizado até que sua transferência seja concluída.

O agente pode ficar off-line brevemente após as atualizações. Isso pode acontecer, por exemplo, logo após a [ativação do agente](#), quando a AWS atualiza o agente.

Important

- DataSync corrige agentes de forma automática e regular para manter sua segurança e estabilidade. DataSync os agentes usam o Amazon Linux 2 como seu sistema operacional básico. Você pode ver o status atual dos problemas detectados de vulnerabilidades e exposições comuns (CVE) no [Amazon](#) Linux Security Center. Os patches CVE são aplicados automaticamente dentro de 30 dias da data de lançamento, conforme indicado no Amazon Linux Security Center. A aplicação de patches ocorre desde que seu agente esteja on-line e não esteja executando ativamente a execução de uma tarefa.
- DataSync não suporta a atualização manual de um EC2 agente da Amazon com as diretivas cloud-init. Se você atualizar um agente dessa forma, poderá encontrar problemas de interoperabilidade com a DataSync impossibilidade de ativar ou usar o agente.

Status de agentes

A tabela a seguir descreve o status dos DataSync agentes.

Status do agente	Significado
Online	O agente está configurado corretamente e disponível para uso. Esse é o status normal de execução de um agente.
Off-line	O agente esteve fora de contato com o DataSync serviço por

Status do agente	Significado
	cinco minutos ou mais. Isso pode acontecer por alguns motivos. Para obter mais informações, consulte O que eu faço se meu agente estiver off-line? .

Solução de problemas de seu agente

Enquanto AWS gerencia o DataSync agente para você, há situações em que talvez você precise trabalhar novamente diretamente com ele. Por exemplo, se o seu agente ficar off-line ou perder a conexão com sistema de armazenamento on-premises, você pode tentar resolver esses problemas no [console local do agente](#).

Para obter mais informações, consulte [DataSync agentes de solução de problemas](#).

Manutenção do agente

Embora AWS gerencie seu AWS DataSync agente depois de implantado e ativado, pode haver casos em que você precise alterar as configurações do agente ou solucionar um problema. Aqui estão alguns exemplos de por que você trabalharia com seu agente por meio do console local:

- Atribuir manualmente um endereço IP ao agente.
- Verifique os recursos de sistema do agente.

Important

Você não precisa usar o console local do agente para obter a DataSync funcionalidade padrão.

Acesso ao console local do agente

A maneira como você acessa o console local depende do tipo de agente que você está usando.

Acessando o console local (VMware ESXiLinux KVM ou Microsoft Hyper-V)

Por motivos de segurança, você não pode se conectar remotamente ao console local da máquina virtual (VM) do DataSync agente.

- Se for a primeira vez que você usa o console local, faça login com as credenciais padrão. O nome de usuário padrão é **admin** e a senha é **password**.

Note

É recomendável alterar a senha padrão. Para fazer isso, no menu principal do console, digite **5** (ou **6** para VMware VMs) e execute o `passwd` comando para alterar a senha.

Acessando o console local (Amazon EC2)

Para se conectar ao console local de um EC2 agente da Amazon, você deve usar SSH.

Antes de começar: certifique-se de que o grupo de segurança da sua EC2 instância permita acesso com SSH (porta TCP 22).

1. Abra um terminal e copie o seguinte comando `ssh`:

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-ip-address
```

- Para `/path/key-pair-name`, especifique o caminho e o nome do arquivo (.pem) da chave privada necessária para se conectar à sua instância.
 - Em `instance-user-name`, especifique `admin`.
 - Para `instance-public-ip-address`, especifique o endereço IP público da sua instância.
2. Execute o comando `ssh` para se conectar à instância.

Uma vez conectado, o menu principal do console local do agente é exibido.

Configuração das definições de DHCP e DNS do agente

A configuração de rede padrão do agente é Dynamic Host Configuration Protocol (DHCP). Com o DHCP, um endereço IP é atribuído automaticamente ao seu agente. Em alguns casos, pode ser necessário atribuir manualmente o IP do agente como endereço IP estático, tal como descrito a seguir.

1. Faça login no console local do agente.
2. No menu principal AWS DataSync Ativação - Configuração, insira **1** para começar a configurar sua rede.
3. No menu Configuração de rede, escolha uma das opções a seguir.

Para	Faça o seguinte
Obter informações sobre seu adaptador de rede	Digite 1. Uma lista de nomes de adaptador é exibida, e você é então solicitado a digitar um nome de adaptador, por exemplo eth0. Se o adaptador especificado estiver em uso, serão exibidas as seguintes informações sobre o adaptador: • O endereço de controle de acesso de mídia (MAC) • Endereço IP • Máscara de rede • Endereço IP do agente • Status de DHCP habilitado Você pode usar o mesmo nome de adaptador ao configurar um endereço IP estático (opção 3), tal como você define o adaptador de rota padrão do agente (opção 5).
Configurar o DHCP	Digite 2. Você é solicitado a configurar a interface de rede para usar o DHCP.

Para	Faça o seguinte
Configurar um endereço IP estático para o agente	Digite 3. Você será solicitado a inserir o nome do adaptador de rede.  Important Se seu agente já tiver sido ativado, você deverá desligá-lo e reiniciá-lo a partir do DataSync console para que as configurações entrem em vigor.
Redefinir todas as configurações de rede do agente para DHCP	Digite 4. Todas as interfaces de rede são definidas para usar DHCP.  Important Se seu agente já tiver sido ativado, você deverá desligá-lo e reiniciá-lo a partir do DataSync console para que as configurações entrem em vigor.

Para	Faça o seguinte
Configurar o adaptador de rota padrão do agente	Digite 5. Os adaptadores disponíveis para seu agente são exibidos e você é solicitado a escolher um dos adaptadores, por exemplo eth0.
Edite a configuração do sistema de nomes de domínio (DNS) do seu agente	Digite 6. Os adaptadores disponíveis dos servidores de DNS primário e secundário são exibidos. O novo endereço IP será solicitado.
Exibir a configuração de DNS do agente	Digite 7. Os adaptadores disponíveis dos servidores de DNS primário e secundário são exibidos.  Note Para algumas versões do VMware hipervisor, você pode editar a configuração do adaptador nesse menu.
Visualizar tabelas de roteamento	Digite 8. A rota padrão do agente é exibida.

Verificando os recursos do sistema do seu agente

Quando você faz login no console do agente, os núcleos de CPU virtual, o tamanho do volume raiz e a RAM são verificados automaticamente. Se houver algum erro ou aviso, ele será sinalizado na tela do menu do console com um banner que fornece detalhes sobre esses erros ou avisos.

Se não houver erros ou avisos ao iniciar o console, o menu exibirá texto em branco. A opção Exibir verificação de recursos do sistema exibirá (0 Errors).

Se houver erros ou avisos, o menu do console exibirá o número de erros e avisos, em vermelho e amarelo, respectivamente, em um banner na parte superior do menu. Por exemplo, (1 ERROR, 1 WARNING).

Para verificar os recursos do sistema do seu agente

1. Faça login no console local do agente.
2. No menu principal AWS DataSync Ativação - Configuração, insira **4** para ver os resultados da verificação de recursos do sistema.

O console exibe uma mensagem [OK], [AVISO] ou [FALHA] para cada recurso, tal como descrito na tabela a seguir.

Para EC2 instâncias da Amazon, a verificação de recursos do sistema verifica se o tipo de instância é uma das instâncias recomendadas para uso com DataSync. Se o tipo de instância corresponder a essa lista, um único resultado será exibido em texto verde, da seguinte forma.

[OK] Instance Type Check

Se a EC2 instância da Amazon não estiver na lista recomendada, a verificação de recursos do sistema verificará os seguintes recursos.

- Verificação dos núcleos da CPU: São necessários pelo menos quatro núcleos.
- Verificação do tamanho do disco: é necessário um mínimo de 80 GB de espaço em disco disponível.
- Verificação RAM:
 - 32 GB de RAM atribuídos à instância para execuções de tarefas trabalhando com até 20 milhões de arquivos, objetos ou diretórios.
 - 64 GB de RAM atribuídos à instância para execuções de tarefas trabalhando com mais de 20 milhões de arquivos, objetos ou diretórios.
- Verificação de sinalizadores de CPU: a CPU da VM do agente deve ter um sinalizador SSSE3 ou um conjunto de SSE4 instruções.

Se a EC2 instância da Amazon não estiver na lista de instâncias recomendadas DataSync, mas tiver recursos suficientes, o resultado da verificação de recursos do sistema exibirá quatro resultados, todos em texto verde.

Os mesmos recursos são verificados para agentes implantados no Hyper-V, na Máquina Virtual Baseada em Kernel Linux (KVM) e VMware VMs

VMware os agentes também são verificados quanto à versão compatível; versões sem suporte causam um erro de banner vermelho. As versões suportadas incluem VMware as versões 6.5 e 6.7.

Sincronizando a hora em seu agente VMware

Se você estiver usando um [VMware agente](#), poderá visualizar ou editar a configuração do servidor Network Time Protocol (NTP) e sincronizar a hora do agente com o host do VMware hipervisor.

1. Faça login no [console local do agente](#).
2. No menu principal AWS DataSync Ativação - Configuração, digite 5.
3. No menu Gerenciamento de hora do sistema escolha uma das seguintes opções:

Para	Faça o seguinte
Exibir e sincronizar o horário da sua VM com o horário do servidor NTP.	Digite 1. A hora atual do agente é exibida. O agente determina a diferença entre a hora do agente e a hora do servidor NTP, e instrui você a sincronizar as horas. Em algumas situações, pode haver um desvio de hora no agente. Por exemplo, pode ser que haja uma interrupção prolongada da rede e que o host do hipervisor e o agente não recebam atualizações de hora e, por isso, a hora do agente fique diferente da hora

Para	Faça o seguinte
	real. Quando há um desvio de hora como esse, ocorre uma discrepância entre a hora declarada das operações (como snapshots) e a hora real em que as operações ocorrem.
Editar a configuração do seu servidor NTP	Digite 2 . Você será solicitado a fornecer a configuração de um servidor NTP.
Exibir a configuração do seu servidor NTP	Digite 3 . A configuração do servidor NTP é exibida.

Execução de comandos relacionados à manutenção para agente

No console local do seu DataSync agente, você pode realizar algumas tarefas de manutenção e diagnosticar problemas com seu agente.

Para executar um comando de configuração ou diagnóstico no console local do seu agente

1. Faça login no [console local do agente](#).
2. No menu principal AWS DataSync Ativação - Configuração, digite **5** (ou para **6** uma VMware VM) no prompt de comando.
3. Use os comandos a seguir para executar as tarefas a seguir com seu agente.

Comando	Descrição
dig	Procure informações de DNS sobre o host.
diskclean	Execute a limpeza do disco.
exit	Retorne ao menu de configuração do console.
h	Exibe uma lista dos comandos disponíveis.

Comando	Descrição
ifconfig	Exibir ou configurar interfaces de rede.
ip	Exiba ou configure roteamento, dispositivos e túneis.
iptables	Configure e mantenha a filtragem de IPv4 pacotes e a tradução de endereços de rede (NAT).
ncport	Teste a conectividade com uma porta TCP de rede específica.
nping	Obtenha informações para solucionar problemas de rede.
save-iptables	Salve as regras de firewall da tabela IP permanentemente.
save-routing-table	Salve uma entrada da tabela de roteamento recém-adicionada.
sslcheck	Verifique se um certificado SSL é válido.
tcptraceroute	Colete saída traceroute do tráfego TCP para um destino.

4. Siga as instruções da tela.

Substituindo seu AWS DataSync agente

Para substituir um AWS DataSync agente, você deve criar um novo agente e atualizar todos os locais de transferência que estejam usando o agente antigo.

Criar um novo agente

Para criar seu novo DataSync agente, siga o mesmo processo quando você criou seu agente antigo:

1. [Implante um agente](#) em seu ambiente de armazenamento.

2. [Escolha um endpoint de serviço](#) que o agente use para se comunicar AWS.
3. [Configure sua rede](#) para que o agente possa se comunicar com seu armazenamento AWS e.
4. [Ative seu agente](#).
5. Depois de ativado, anote o nome do recurso da Amazon (ARN) do agente.

Você precisa desse ARN ao atualizar sua DataSync localização para usar o novo agente.

Atualizando sua localização com o novo agente

Depois de criar um novo agente, você pode atualizar um DataSync local existente para usar esse agente. Na maioria dos casos, você também precisa inserir as credenciais de acesso novamente para atualizar o local. Isso ocorre porque DataSync armazena as credenciais de localização de uma forma que somente seu agente possa usá-las.

Usando o DataSync console

As instruções a seguir descrevem como atualizar locais com um novo agente usando o DataSync console.

NFS

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e, em seguida, escolha Locais.
3. Escolha o local que você deseja atualizar e, em seguida, escolha Editar.
4. Em Agentes, escolha seu novo agente.

Você pode escolher mais de um agente se estiver substituindo [vários agentes](#) em um local.

5. Escolha Salvar alterações.

SMB

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e, em seguida, escolha Locais.
3. Escolha o local que você deseja atualizar e, em seguida, escolha Editar.
4. Em Agentes, escolha seu novo agente.

Você pode escolher mais de um agente se estiver substituindo [vários agentes](#) em um local.

5. Em Password (Senha), insira a senha do usuário que pode montar o servidor de arquivos SMB e tenha permissão para acessar os arquivos e pastas envolvidos na sua transferência.
6. Escolha Salvar alterações.

HDFS

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e, em seguida, escolha Locais.
3. Escolha o local que você deseja atualizar e, em seguida, escolha Editar.
4. Em Agentes, escolha seu novo agente.

Você pode escolher mais de um agente se estiver substituindo [vários agentes](#) em um local.

5. Se você estiver usando a autenticação Kerberos, faça o upload do seu arquivo Keytab e do arquivo de configuração do Kerberos.
6. Escolha Salvar alterações.

Object storage

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e, em seguida, escolha Locais.
3. Escolha o local que você deseja atualizar e, em seguida, escolha Editar.
4. Em Agentes, escolha seu novo agente.

Você pode escolher mais de um agente se estiver substituindo [vários agentes](#) em um local.

5. Se sua localização exigir credenciais, insira a chave secreta que permite DataSync acessar seu bucket de armazenamento de objetos.
6. Escolha Salvar alterações.

Azure Blob Storage

Faça o seguinte para atualizar seu Microsoft Azure Blob Storage localização:

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e, em seguida, escolha Locais.
3. Escolha o local que você deseja atualizar e, em seguida, escolha Editar.
4. Em Agentes, escolha seu novo agente.

Você pode escolher mais de um agente se estiver substituindo [vários agentes](#) em um local.

5. Para o token SAS, insira o [token de assinatura de acesso compartilhado \(SAS\)](#) que permite DataSync acessar seu armazenamento de blobs.
6. Escolha Salvar alterações.

Usando o AWS CLI

As instruções a seguir descrevem como atualizar locais com um novo agente usando o AWS CLI. (Você também pode fazer isso usando a [DataSync API](#).)

NFS

1. Copie o seguinte comando [update-location-nfs](#):

```
aws datasync update-location-nfs \
  --location-arn datasync-nfs-location-arn \
  --on-prem-config AgentArns=new-datasync-agent-arn
```

2. Para o parâmetro `--location-arn`, especifique o ARN do local do NFS que você está atualizando.
3. Para a opção `--on-prem-config` do parâmetro `AgentArns`, especifique o ARN do seu novo agente.

Você pode especificar mais de um ARN se estiver substituindo [vários agentes](#) em um local.

4. Execute o comando `update-location-nfs` para atualizar o local.

SMB

1. Copie o seguinte comando [update-location-smb](#):

```
aws datasync update-location-smb \
```

```
--location-arn datasync-smb-location-arn \  
--agent-arns new-datasync-agent-arn \  
--password smb-file-server-password
```

2. Para o parâmetro `--location-arn`, especifique o ARN do local do SMB que você está atualizando.
3. Para o parâmetro `--agent-arns`, especifique o ARN do seu novo agente.

Você pode especificar mais de um ARN se estiver substituindo [vários agentes](#) em um local.

4. Para o parâmetro `--password`, especifique a senha do usuário que pode montar o servidor de arquivos SMB e tenha permissão para acessar os arquivos e pastas envolvidos na sua transferência.
5. Execute o comando `update-location-smb` para atualizar o local.

HDFS

1. Copie o seguinte comando [update-location-hdfs](#):

```
aws datasync update-location-hdfs \  
--location-arn datasync-hdfs-location-arn \  
--agent-arns new-datasync-agent-arn \  
--kerberos-keytab keytab-file \  
--kerberos-krb5-conf krb5-conf-file
```

2. Para o parâmetro `--location-arn`, especifique o ARN do local do HDFS que você está atualizando.
3. Para o parâmetro `--agent-arns`, especifique o ARN do seu novo agente.

Você pode especificar mais de um ARN se estiver substituindo [vários agentes](#) em um local.

4. Se você estiver usando a autenticação Kerberos, inclua os parâmetros `--kerberos-keytab` e `--kerberos-krb5-conf`:

- Para o parâmetro `--kerberos-keytab`, a tabela de chaves Kerberos (keytab) que contém mapeamentos entre a entidade principal Kerberos definida e as chaves criptografadas.

Você pode carregar o arquivo keytab fornecendo o endereço do arquivo.

- Para o parâmetro `--kerberos-krb5-conf`, especifique o arquivo que contém a configuração do seu realm Kerberos.

Você pode especificar o arquivo `krb5.conf` fornecendo o endereço do arquivo.

Se você estiver usando uma autenticação simples, não precisará incluir esses parâmetros relacionados ao Kerberos no seu comando.

5. Execute o comando `update-location-hdfs` para atualizar o local.

Object storage

1. Copie o seguinte comando [update-location-object-storage](#):

```
aws datasync update-location-object-storage \  
  --location-arn datasync-object-storage-location-arn \  
  --agent-arns new-datasync-agent-arn \  
  --secret-key bucket-secret-key
```

2. Para o parâmetro `--location-arn`, especifique o ARN do local de armazenamento do objeto que você está atualizando.
3. Para o parâmetro `--agent-arns`, especifique o ARN do seu novo agente.

Você pode especificar mais de um ARN se estiver substituindo [vários agentes](#) em um local.

4. Faça o seguinte, dependendo de se o local de armazenamento de objetos exige credenciais de acesso:
 - Se sua localização exigir credenciais — Para o `--secret-key` parâmetro, especifique a chave secreta que permite DataSync acessar seu bucket de armazenamento de objetos.
 - Se o local exigir credenciais: especifique strings vazias para os parâmetros `--access-key` e `--secret-key`. Veja um exemplo de comando :

```
aws datasync update-location-object-storage \  
  --location-arn arn:aws:datasync:us-east-2:111122223333:location/  
loc-abcdef01234567890 \  
  --agent-arns arn:aws:datasync:us-east-2:111122223333:agent/  
agent-1234567890abcdef0 \  
  --access-key "" \  
  --secret-key ""
```

5. Execute o comando `update-location-object-storage` para atualizar o local.

Azure Blob Storage

1. Copie o seguinte comando [update-location-azure-blob](#):

```
aws datasync update-location-azure-blob \  
  --location-arn datasync-azure-blob-storage-location-arn \  
  --agent-arns new-datasync-agent-arn \  
  --sas-configuration '{  
    "Token": "sas-token-for-azure-blob-storage"  
  }'
```

2. Para o `--location-arn` parâmetro, especifique o ARN do Azure Blob Storage local que você está atualizando.
3. Para o parâmetro `--agent-arns`, especifique o ARN do seu novo agente.

Você pode especificar mais de um ARN se estiver substituindo [vários agentes](#) em um local.

4. Para a Token opção do `--sas-configuration` parâmetro, especifique o [token SAS](#) que permite DataSync acessar seu armazenamento de blobs.
5. Execute o comando `update-location-azure-blob` para atualizar o local.

Próximas etapas

1. [Exclua seu agente antigo](#). Se você tiver alguma DataSync tarefa em execução usando esse agente, espere até que essas tarefas terminem antes de excluí-la.
2. Se você precisar substituir agentes em vários locais, repita as etapas anteriores.
3. Quando terminar, você pode retomar a [execução das tarefas](#).

Note

Substituição de agentes para tarefas agendadas: se substituir um agente para uma [tarefa agendada](#), inicie a tarefa manualmente se o novo agente estiver usando um tipo de [endpoint de serviço](#) diferente do antigo. Se você não executar a tarefa manualmente antes da execução agendada, haverá falha na tarefa.

Por exemplo, se o agente antigo usava um endpoint de serviço público, mas o novo agente usa um endpoint da VPC, inicie a tarefa manualmente usando o console ou a operação `StartTaskExecution`. Depois disso, a execução da tarefa será retomada segundo o agendamento.

Recursos de filtragem AWS DataSync

Você pode filtrar seus AWS DataSync locais e tarefas usando as operações `ListLocations` e `ListTasks` da API no AWS CLI. Por exemplo, recupere uma lista de suas tarefas mais recentes.

Parâmetros para filtragem

Você pode usar filtros de API para refinar a lista de recursos retornados por `ListTasks` e `ListLocations`. Por exemplo, para recuperar todos os seus locais do Amazon S3, você pode usar o `ListLocations` com o nome do filtro `LocationType S3` e `Operator Equals`.

Para filtrar os resultados da API, você deve especificar o nome, o operador e o valor do filtro.

- **Name:** nome do filtro que está sendo usado. Cada chamada de API é compatível com uma lista de filtros que estão disponíveis para ela (por exemplo, `LocationType` para `ListLocations`).
- **Values:** os valores que você deseja filtrar. Por exemplo, talvez você queira exibir somente locais do Amazon S3.
- **Operator:** operador usado para comparar valores de filtro (por exemplo, `Equals` ou `Contains`).

A tabela a seguir lista os operadores disponíveis.

Operador	Tipos de chave
<code>Equals</code>	String, número
<code>NotEquals</code>	String, número
<code>LessThan</code>	Número
<code>LessThanOrEqualTo</code>	Número
<code>GreaterThan</code>	Número
<code>GreaterThanOrEqualTo</code>	Número
<code>In</code>	String
<code>Contains</code>	String

Operador	Tipos de chave
NotContains	String
BeginsWith	String

Filtrando por local

ListLocations fornece suporte aos seguintes nomes de filtro:

- **LocationType**: filtra no tipo de localização:
 - SMB
 - NFS
 - HDFS
 - OBJECT_STORAGE
 - S3
 - OUTPOST_S3
 - FSX_WINDOWS
 - FSX_LUSTRE
 - FSX_OPENZFS_NFS
 - FSX_ONTAP_NFS
 - FSX_ONTAP_SMB
- **LocationUri**: filtra o identificador uniforme de recursos (URI) atribuído ao local, conforme retornado pela chamada da API DescribeLocation* (por exemplo, `s3://bucket-name/your-prefix` para locais do Amazon S3).
- **CreationTime**: filtra no horário em que a localização foi criada. O formato de entrada é yyyy-MM-dd:mm:ss, em Universal Coordinated Time (UTC – Tempo universal coordenado).

O AWS CLI exemplo a seguir lista todos os locais do tipo Amazon S3 que têm um URI de localização começando com a string `"s3://amzn-s3-demo-bucket"` e que foram criados em ou após 15/12/2019 às 17:15:20 UTC.

```
aws datasync list-locations \
```

```
--filters [{Name=LocationType, Values=["S3"], Operator=Equals},
{Name=LocationUri, Values=["s3://amzn-s3-demo-bucket"], Operator=BeginsWith},
{Name=CreationTime, Values=["2019-12-15 17:15:20"], Operator=GreaterThanOrEqual}]
```

Esse comando retorna uma saída semelhante à seguinte:

```
{
  "Locations": [
    {
      "LocationArn": "arn:aws:datasync:us-east-1:111122223333:location/loc-3333333333abcdef0",
      "LocationUri": "s3://amzn-s3-demo-bucket1/"
    },
    {
      "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/loc-987654321abcdef0",
      "LocationUri": "s3://amzn-s3-demo-bucket2/"
    }
  ]
}
```

Filtrando por tarefa

ListTasks oferece suporte aos seguintes nomes de filtro.

- **LocationId**: filtra nos locais de origem e destino nos valores do nome do recurso da Amazon (ARN).
- **CreationTime**: filtra no horário em que a tarefa foi criada. O formato de entrada é yyyy-MM-dd:mm:ss em UTC.

O AWS CLI exemplo a seguir mostra a sintaxe durante a filtragem. LocationId

```
aws datasync list-tasks \
  --filters Name=LocationId,Values=arn:aws:datasync:us-east-1:your-account-id:location/your-location-id,Operator=Contains
```

A saída deste comando é parecida com o exemplo a seguir.

```
{
  "Tasks": [
```

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:your-account-id:task/your-task-id",
  "Status": "AVAILABLE",
  "Name": "amzn-s3-demo-bucket"
}
```

Limpendo seus AWS DataSync recursos

Se você usou AWS DataSync para um teste ou não precisa dos AWS recursos que criou, exclua-os para não ser cobrado pelos recursos que não planeja usar.

Note

Se você tiver DataSync recursos em uma [região opcional](#) que você desabilita, esses recursos não serão excluídos automaticamente. Os recursos ainda estarão lá se você habilitar essa região novamente.

Excluindo um agente DataSync

Quando você exclui um agente de AWS DataSync, o recurso do agente não está mais associado ao seu Conta da AWS e não pode ser desfeito.

Lembre-se de que excluir um agente de DataSync não remove sua máquina virtual (VM) ou EC2 instância da Amazon do seu ambiente de armazenamento. Você pode excluir a VM ou a instância ou reutilizá-la para ativar um novo agente.

Pré-requisitos

Não exclua um agente até que você atualize ou remova os DataSync recursos que dependem dele. Se você estiver substituindo um agente, [atualize seus locais de transferência](#) com o novo agente. Se você não estiver substituindo um agente, exclua primeiro as [tarefas](#) e os [locais](#) de transferência usando esse agente.

Exclusão do agente

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação à esquerda, escolha Agentes.

3. Escolha o agente que você deseja excluir.
4. Escolha Excluir, digite **delete** na caixa de texto exibida e selecione Excluir.
5. Se você não planeja [reutilizar a infraestrutura do agente](#) para outras DataSync atividades, exclua a VM do agente ou a EC2 instância da Amazon para removê-la do seu ambiente de armazenamento.

Reutilizando a infraestrutura de um DataSync agente

Você pode excluir um recurso de agente DataSync e ainda usar a VM subjacente do agente ou a EC2 instância da Amazon para ativar um novo agente.

Para reutilizar a infraestrutura de um agente

1. [Teste a conexão do agente com AWS](#) o. Se os testes de rede forem aprovados, vá para a próxima etapa.

É necessária a aprovação nos testes de rede antes de você poder passar para a próxima etapa.

2. [Exclua o recurso do agente](#) DataSync , mas não exclua a VM do agente ou a EC2 instância da Amazon.
3. Repita a etapa 1 para testar AWS novamente a conexão do agente. Se os testes de rede forem aprovados, vá para a próxima etapa.
4. Cerca de três minutos após excluir o recurso do agente DataSync, verifique se a porta 80 está aberta na VM do agente ou na instância da Amazon EC2 . Se estiver, vá para a próxima etapa.
5. [Ative um novo agente](#) com a VM existente ou a EC2 instância da Amazon.

Você pode ativar o novo agente em um [endpoint diferente Região da AWS e com outro tipo de terminal de serviço](#). Conta da AWS Se você usar um outro tipo de endpoint de serviço, precisará ajustar a [configuração de rede](#).

Excluindo um local DataSync

Como prática recomendada, remova os AWS DataSync locais que você não precisa mais.

Para remover um local usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.

2. No painel de navegação esquerdo, expanda Transferência de dados e, em seguida, escolha Locais.
3. Escolha o local que deseja remover.
4. Escolha Excluir. Confirme a exclusão inserindo **delete** e, em seguida, escolha Excluir.

Excluindo uma tarefa DataSync

Se você não precisar mais de uma AWS DataSync tarefa, poderá excluí-la e seus AWS recursos relacionados.

Pré-requisitos

Quando você executa uma tarefa, cria e gerencia DataSync automaticamente [interfaces de rede](#) para tráfego de transferência de dados. Ao excluir uma tarefa, você também exclui suas interfaces de rede relacionadas, desde que tenha as seguintes permissões:

- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`

Essas permissões estão disponíveis na política AWS gerenciada `AWSDataSyncFullAccess`. Para obter mais informações, consulte [AWS políticas gerenciadas para AWS DataSync](#).

Excluindo a tarefa

Depois de excluir uma tarefa, você não poderá restaurá-la.

Usando o DataSync console

1. Abra o AWS DataSync console em <https://console.aws.amazon.com/datasync/>.
2. No painel de navegação esquerdo, expanda Transferência de dados e selecione Tarefas.
3. Selecione a tarefa que você deseja excluir.
4. Escolha Ações e Excluir.
5. Na caixa de diálogo , , escolha Delete.

Usando o AWS CLI

1. Copie o seguinte comando `delete-task`:

```
aws datasync delete-task \  
    --task-arn "task-to-delete"
```

2. Para o parâmetro `--task-arn`, especifique o nome do recurso da Amazon (ARN) da tarefa que você está excluindo (por exemplo, `arn:aws:datasync:us-east-2:123456789012:task/task-012345678abcd0123`).
3. Execute o comando `delete-task`.

Segurança em AWS DataSync

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.

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos [programas de conformidade da AWS](#). Para saber mais sobre os programas de conformidade que se aplicam ao AWS DataSync, consulte [Serviços da AWS no escopo por programa de conformidade](#).
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e normas aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar DataSync. Os tópicos a seguir mostram como configurar para atender DataSync aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus DataSync recursos.

Tópicos

- [Proteção de dados em AWS DataSync](#)
- [Gerenciamento de identidade e acesso em AWS DataSync](#)
- [Validação de conformidade para AWS DataSync](#)
- [Resiliência em AWS DataSync](#)
- [Segurança da infraestrutura em AWS DataSync](#)
- [Protegendo as credenciais do local de armazenamento](#)

Proteção de dados em AWS DataSync

AWS DataSync transfere dados com segurança entre sistemas de armazenamento autogerenciados e serviços de AWS armazenamento e também entre AWS serviços de armazenamento. A forma como seus dados de armazenamento são criptografados em trânsito depende, em parte, dos locais envolvidos na transferência.

Após a conclusão da transferência, os dados são criptografados em repouso pelo sistema ou serviço que os armazena (não DataSync).

Tópicos

- [AWS DataSync criptografia em trânsito](#)
- [AWS DataSync criptografia em repouso](#)
- [Privacidade do tráfego entre redes](#)

AWS DataSync criptografia em trânsito

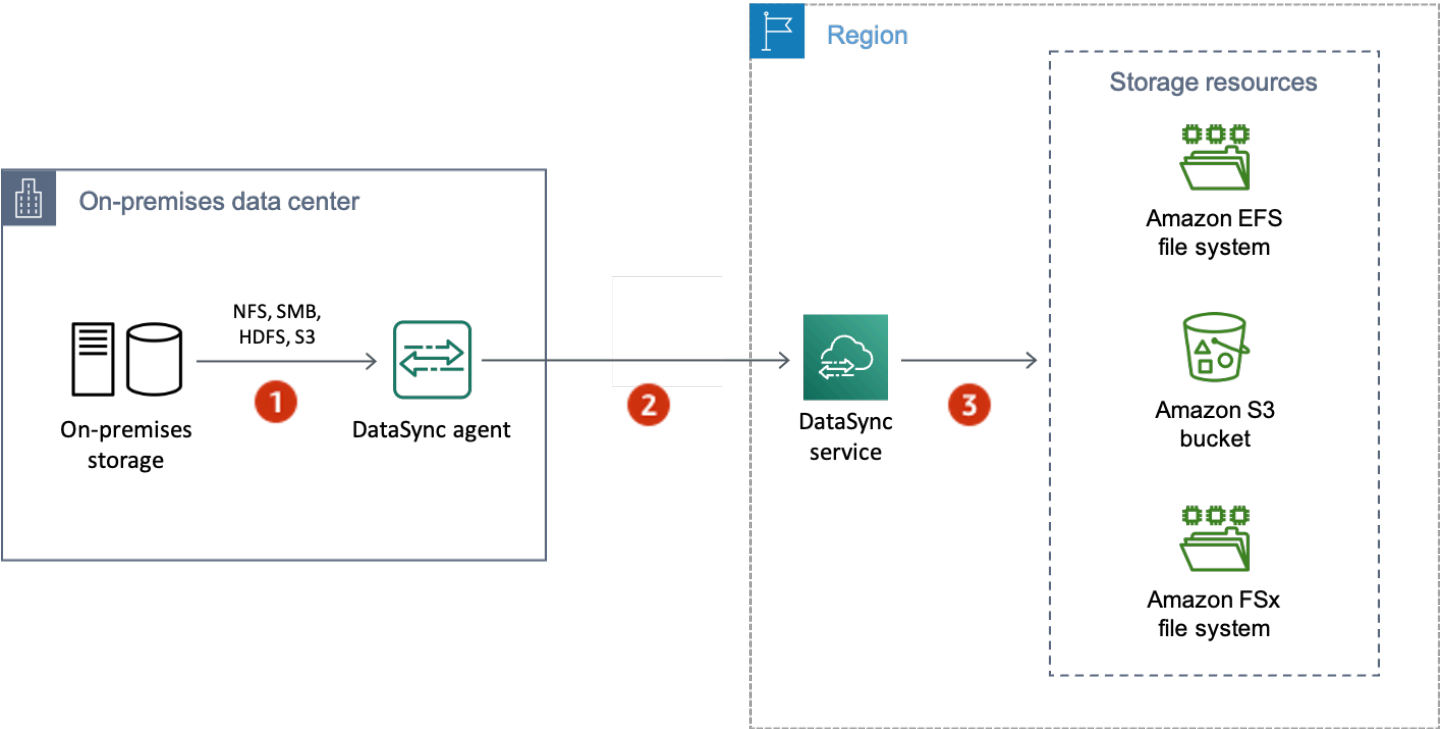
Seus dados de armazenamento (incluindo metadados) são criptografados em trânsito, mas a forma como são criptografados durante a transferência depende dos seus locais de origem e destino.

Ao se conectar a um local, DataSync usa as opções mais seguras fornecidas pelo protocolo de acesso a dados desse local. Por exemplo, ao se conectar a um sistema de arquivos usando o Server Message Block (SMB), DataSync usa os recursos de segurança fornecidos pelo SMB.

Conexões de rede em uma transferência

DataSync requer três conexões de rede para copiar dados: uma conexão para ler dados de um local de origem, outra para transferir dados entre locais e outra para gravar dados em um local de destino.

O diagrama a seguir é um exemplo das conexões de rede DataSync usadas para transferir dados de um sistema de armazenamento local para um serviço AWS de armazenamento. Para entender onde as conexões acontecem e como os dados são protegidos enquanto passam por cada conexão, use a tabela associada.



Referência	Conexões de rede	Descrição
1	Leitura de dados do local de origem	DataSync se conecta usando o protocolo do sistema de armazenamento para acessar dados (por exemplo, SMB ou a API do Amazon S3). Para essa conexão, os dados são protegidos usando os recursos de segurança do sistema de armazenamento, a menos que DataSync não ofereça suporte a esses recursos. Por exemplo, DataSync atualmente não oferece suporte à autenticação Kerberos com servidores de arquivos NFS ou ao usar a criptografia TDE com HDFS.
2	Transferência de dados entre locais	Para essa conexão, DataSync criptografa todo o tráfego de rede

Referência	Conexões de rede	Descrição
		com o Transport Layer Security (mTLS) 1.3 mútuo.
3	Gravação de dados no local de destino	Assim como no local de origem, DataSync conecta-se usando o protocolo do sistema de armazenamento para acessar os dados. Os dados são novamente protegidos usando os recursos de segurança do sistema de armazenamento, a menos que DataSync não ofereça suporte a esses recursos.

Saiba como seus dados são criptografados em trânsito quando DataSync conectados aos seguintes serviços AWS de armazenamento:

- [Amazon EFS](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)
- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)
- [Amazon S3](#)

Cifras TLS

Ao transferir dados entre locais, DataSync usa cifras TLS diferentes. A cifra TLS depende do tipo de endpoint de serviço que seu agente usa para se comunicar. DataSync (Para ter mais informações, consulte [Escolha de um endpoint de serviço para o agente do AWS DataSync.](#))

Sumário

- [Endpoints públicos ou da VPC](#)
- [Endpoints do FIPS](#)

Endpoints públicos ou da VPC

Para endpoints de serviço de nuvem privada pública e virtual (VPC), DataSync use uma das seguintes cifras TLS:

- TLS_ECDHE_RSA_COM_AES_256_GCM_ (ecdh_x25519) SHA384
- TLS_ECDHE_RSA_COM_0_05_ (CHACHA2ecdh_x25519) POLY13 SHA256
- TLS_ECDHE_RSA_COM_AES_128_GCM_ (ecdh_x25519) SHA256

Endpoints do FIPS

Para endpoints de serviço do Federal Information Processing Standard (FIPS), DataSync usa a seguinte cifra TLS:

- SHA256 TLS_AES_128_GCM_ (secp256r1)

AWS DataSync criptografia em repouso

Por ser AWS DataSync um serviço de transferência, ele geralmente não gerencia seus dados de armazenamento em repouso. Os serviços e sistemas de armazenamento que DataSync oferecem suporte são responsáveis por proteger os dados nesse estado. No entanto, há alguns dados relacionados ao serviço que são DataSync gerenciados em repouso.

O que é criptografado?

Os únicos dados tratados DataSync em repouso estão relacionados aos detalhes necessários para concluir sua transferência. DataSync armazena os seguintes dados com criptografia total em repouso no Amazon DynamoDB:

- Configurações de tarefas (por exemplo, detalhes sobre os locais em sua transferência).
- Credenciais de usuário que permitem que seu DataSync agente se autentique com um local. Essas credenciais são criptografadas usando as chaves públicas do seu atendente. O atendente pode descriptografar essas chaves conforme necessário com suas chaves privadas.

Para obter mais informações, consulte [Criptografia DynamoDB em repouso](#), no Guia do desenvolvedor do Amazon DynamoDB.

Gerenciamento de chaves

Você não pode gerenciar as chaves de criptografia DataSync usadas para armazenar informações no DynamoDB relacionadas à execução da sua tarefa. Essas informações incluem suas configurações de tarefas e as credenciais que os atendentes usam para se autenticar em um local de armazenamento.

O que não é criptografado?

Embora DataSync não controle como seus dados de armazenamento são criptografados em repouso, ainda recomendamos configurar seus locais com o mais alto nível de segurança suportado por eles. Por exemplo, você pode criptografar objetos com chaves de criptografia gerenciadas do Amazon S3 (SSE-S3) AWS Key Management Service ou chaves (KMS) (AWS SSE-KMS).

Saiba mais sobre como os serviços AWS de armazenamento criptografam dados em repouso:

- [Amazon S3](#)
- [Amazon EFS](#)
- [Servidor FSx de arquivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)
- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Privacidade do tráfego entre redes

Recomendamos configurar seus locais de origem e destino com o mais alto nível de segurança compatível com cada um deles. Ao se conectar a um local, AWS DataSync funciona com a versão mais segura do protocolo de acesso a dados que o sistema de armazenamento usa. Além disso, considere limitar o tráfego de sub-rede a protocolos e serviços conhecidos.

DataSync protege a conexão entre locais — inclusive entre Contas da AWS, e zonas de disponibilidade — usando o Regiões da AWS Transport Layer Security (TLS) 1.3.

Gerenciamento de identidade e acesso em AWS DataSync

AWS usa credenciais de segurança para identificá-lo e conceder acesso aos seus AWS recursos. Você pode usar os recursos do AWS Identity and Access Management (IAM) para permitir que

outros usuários, serviços e aplicativos usem seus AWS recursos de forma total ou limitada, sem compartilhar suas credenciais de segurança.

Por padrão, as identidades do IAM (usuários, grupos e funções) não têm permissão para criar, visualizar ou modificar AWS recursos. Para permitir que usuários, grupos e funções acessem AWS DataSync recursos e interajam com o DataSync console e a API, recomendamos que você use uma política do IAM que conceda a eles permissão para usar os recursos específicos e as ações de API de que precisarão. Depois, associe a política à identidade do IAM que requer acesso. Para obter uma visão geral dos elementos básicos de uma política, consulte [Gerenciamento de acesso para AWS DataSync](#).

Tópicos

- [Gerenciamento de acesso para AWS DataSync](#)
- [AWS políticas gerenciadas para AWS DataSync](#)
- [Políticas gerenciadas pelo cliente do IAM para o AWS DataSync](#)
- [Usar perfis vinculados a serviço do DataSync](#)
- [Permissões para marcar DataSync recursos durante a criação](#)
- [Prevenção contra o ataque do “substituto confuso” em todos os serviços](#)

Gerenciamento de acesso para AWS DataSync

Cada AWS recurso é de propriedade de um Conta da AWS. As permissões para criar ou acessar um recurso são regidas por políticas de permissões. Um administrador da conta pode anexar políticas de permissões às identidades AWS Identity and Access Management (IAM). Alguns serviços (como AWS Lambda) também oferecem suporte à anexação de políticas de permissões aos recursos.

Note

Um administrador da conta é um usuário com privilégios de administrador em um Conta da AWS. Para obter mais informações, consulte [Práticas recomendadas do IAM](#) no Guia do usuário do IAM.

Tópicos

- [DataSync recursos e operações](#)
- [Informações sobre propriedade de recursos](#)

- [Gerenciar acesso aos recursos da](#)
- [Especificar elementos da política: ações, efeitos, recursos e entidades principais](#)
- [Especificar condições em uma política](#)

DataSync recursos e operações

Em DataSync, os recursos principais são agente, localização, tarefa e execução de tarefas.

Esses recursos têm nomes de recursos exclusivos da Amazon (ARNs) associados a eles, conforme mostrado na tabela a seguir.

Tipo de recurso	Formato ARN
ARN do agente	arn:aws:datasync: <i>region:account-id</i> :agent/ <i>agent-id</i>
ARN do local	arn:aws:datasync: <i>region:account-id</i> :location/ <i>location-id</i>
Nome de região da Amazon (ARN) da tarefa	arn:aws:datasync: <i>region:account-id</i> :task/ <i>task-id</i>
ARN da execução da tarefa	arn:aws:datasync: <i>region:account-id</i> :task/ <i>task-id</i> /executio n/ <i>exec-id</i>

Para conceder permissões para operações específicas da API, como criar uma tarefa, DataSync defina um conjunto de ações que você pode especificar em uma política de permissões. Uma operação de API pode exigir permissões para mais de uma ação.

Informações sobre propriedade de recursos

O proprietário do recurso é Conta da AWS quem criou o recurso. Ou seja, o proprietário do recurso é a Conta da AWS entidade principal (por exemplo, uma função do IAM) que autentica a solicitação que cria o recurso. Os exemplos a seguir mostram como isso funciona:

- Se você usar as credenciais da sua conta raiz Conta da AWS para criar uma tarefa, você Conta da AWS é o proprietário do recurso (em DataSync, o recurso é a tarefa).
- Se você criar uma função do IAM em sua Conta da AWS e conceder permissões para a `CreateTask` ação a esse usuário, o usuário poderá criar uma tarefa. No entanto, sua Conta da AWS, à qual o usuário pertence, é proprietária do recurso de tarefa.
- Se você criar uma função do IAM Conta da AWS com permissões para criar uma tarefa, qualquer pessoa que possa assumir a função poderá criar uma tarefa. Seu Conta da AWS, ao qual a função pertence, é proprietário do recurso da tarefa.

Gerenciar acesso aos recursos da

A política de permissões descreve quem tem acesso a quê. A seção a seguir explica as opções disponíveis para a criação de políticas de permissões.

Note

Esta seção discute o uso do IAM no contexto de DataSync. Não são fornecidas informações detalhadas sobre o serviço IAM. Para ver a documentação completa do IAM, consulte [O que é o IAM?](#) no Guia do usuário do IAM. Para obter mais informações sobre a sintaxe e as descrições da política do IAM, consulte a [Referência de política do AWS Identity and Access Management](#) do Guia do usuário do IAM.

As políticas anexadas a uma identidade do IAM são chamadas de políticas baseadas em identidade (políticas do IAM) e as políticas anexadas a um recurso são chamadas de políticas baseadas em recursos. DataSync suporta somente políticas baseadas em identidade (políticas do IAM).

Tópicos

- [Políticas baseadas em identidade](#)
- [Políticas baseadas em recursos](#)

Políticas baseadas em identidade

Você pode gerenciar o acesso aos DataSync recursos com as políticas do IAM. Essas políticas podem ajudar um Conta da AWS administrador a fazer o seguinte com DataSync:

- Conceda permissões para criar e gerenciar DataSync recursos — Crie uma política do IAM que permita que uma função do IAM em você Conta da AWS crie e gerencie DataSync recursos, como agentes, locais e tarefas.
- Conceder permissões a uma função em outra Conta da AWS ou em uma AWS service (Serviço da AWS) — Crie uma política do IAM que conceda permissões a uma função do IAM em uma função diferente Conta da AWS ou em uma AWS service (Serviço da AWS). Por exemplo:
 1. Um administrador da Conta A cria um perfil do IAM e anexa uma política de permissões ao perfil que concede permissões em recursos da Conta A.
 2. O administrador da conta A anexa uma política de confiança ao perfil que identifica a conta B como a entidade principal, que pode assumir a função.

Para conceder AWS service (Serviço da AWS) permissões para assumir a função, o administrador da Conta A pode especificar a AWS service (Serviço da AWS) como principal na política de confiança.

3. O administrador da conta B pode delegar permissões para que usuários ou grupos da conta B assumam o perfil. Isso permite que os usuários na conta B criem ou acessem recursos na conta A.

Para obter mais informações sobre o uso do IAM para delegar permissões, consulte [Gerenciamento de acesso](#) no Manual do usuário do IAM.

Veja a seguir um exemplo de política que concede permissões para todas as ações `List*` em todos os recursos. Essa ação é somente para leitura e não permite a modificação de recursos.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllListActionsOnAllResources",
      "Effect": "Allow",
      "Action": [
```

```
        "datasync:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Para obter mais informações sobre o uso de políticas baseadas em identidade com DataSync, consulte políticas gerenciadas e [políticas AWS gerenciadas pelo cliente](#). Para obter informações sobre identidades do IAM, consulte o [Guia do usuário do IAM](#).

Políticas baseadas em recursos

Outros serviços, como Amazon S3, também dão suporte a políticas de permissões baseadas em recursos. Por exemplo, você pode anexar uma política a um bucket do Amazon S3 para gerenciar permissões de acesso a esse bucket. No entanto, DataSync não oferece suporte a políticas baseadas em recursos.

Especificar elementos da política: ações, efeitos, recursos e entidades principais

Para cada DataSync recurso, o serviço define um conjunto de operações de API (consulte [Ações](#)). Para conceder permissões para essas operações de API, DataSync defina um conjunto de ações que você pode especificar em uma política. Por exemplo, para o DataSync recurso, as seguintes ações são definidas: `CreateTaskDeleteTask`, `DescribeTask` e. A execução de uma operação de API pode exigir permissões para mais de uma ação.

Estes são os elementos de política mais básicos:

- **Recurso:** em uma política, você usa um Amazon Resource Name (ARN – Nome do recurso da Amazon) para identificar o recurso a que a política se aplica. Para os recursos do DataSync, você pode usar o caractere curinga (`*`) nas políticas do IAM. Para obter mais informações, consulte [DataSync recursos e operações](#).
- **Ação:** você usa palavras-chave de ação para identificar operações de recursos que deseja permitir ou negar. Por exemplo, dependendo do `Effect` elemento especificado, a `datasync:CreateTask` permissão permite ou nega ao usuário permissões para realizar a DataSync `CreateTask` operação.
- **Efeito:** você especifica o efeito quando o usuário solicita a ação específica, que pode ser `Allow` ou `Deny`. Se você não conceder explicitamente acesso a um recurso (`Allow`), o acesso estará implicitamente negado. Você também pode negar explicitamente o acesso a um recurso, para ter

certeza de que um usuário não consiga acessá-lo, mesmo que uma política diferente conceda acesso. Para ter mais informações, consulte [Autorização](#) no Guia do usuário do IAM.

- Entidade principal: em políticas baseadas em identidade (políticas do IAM), o usuário ao qual a política é anexada é a entidade principal implícita. Para políticas baseadas em recursos, você especifica o usuário, a conta, o serviço ou outra entidade que deseja receber permissões (aplica-se somente às políticas baseadas em recursos). DataSync não oferece suporte a políticas baseadas em recursos.

Para saber mais sobre a sintaxe e as descrições da política do IAM, consulte a [Referência da política do AWS Identity and Access Management](#) no Guia do usuário do IAM.

Especificar condições em uma política

Ao conceder permissões, você pode usar a linguagem da política do IAM para especificar as condições sobre quando uma política relativa à concessão de permissões deverá entrar em vigor. Por exemplo, é recomendável aplicar uma política somente após uma data específica. Para obter mais informações sobre como especificar condições em uma linguagem de política, consulte [Condição](#) no Guia do usuário do IAM.

Para expressar condições, você usa chaves de condição predefinidas. Não existem chaves de condição específicas do DataSync. No entanto, existem chaves AWS de condição amplas que você pode usar conforme apropriado. Para obter uma lista completa de chaves AWS largas, consulte [Chaves disponíveis](#) no Guia do usuário do IAM.

AWS políticas gerenciadas para AWS DataSync

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar [políticas gerenciadas pelo cliente do IAM](#) que fornecem 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 políticas AWS gerenciadas, consulte [políticas AWS gerenciadas](#) no Guia do usuário do IAM.

Serviços da AWS manter e atualizar 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 Serviços da AWS os 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: `AWSDataSyncReadOnlyAccess`

É possível anexar a política `AWSDataSyncReadOnlyAccess` às identidades do IAM.

Essa política concede permissões somente de leitura para. DataSync

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DataSyncReadOnlyAccessPermissions",
    "Effect": "Allow",
    "Action": [
      "datasync:Describe*",
      "datasync:List*",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "elasticfilesystem:DescribeFileSystems",
      "elasticfilesystem:DescribeMountTargets",
      "fsx:DescribeFileSystems",
      "iam:GetRole",
      "iam:ListRoles",
      "logs:DescribeLogGroups",
```

```

        "logs:DescribeResourcePolicies",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
    ],
    "Resource": "*"
}]
}
```

AWS política gerenciada: AWSDataSyncFullAccess

É possível anexar a política AWSDataSyncFullAccess às identidades do IAM.

Essa política concede permissões administrativas DataSync e é necessária para o AWS Management Console acesso ao serviço. AWSDataSyncFullAccess fornece acesso total às operações de DataSync API e às operações que interagem com recursos relacionados (como buckets do Amazon S3, sistemas de arquivos Amazon EFS, AWS KMS chaves e segredos do Secrets Manager). A política também concede permissões para a Amazon CloudWatch, incluindo a criação de grupos de registros e a criação ou atualização de uma política de recursos.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DataSyncFullAccessPermissions",
    "Effect": "Allow",
    "Action": [
      "datasync:*",
      "ec2:CreateNetworkInterface",
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRegions",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcEndpoints",
      "ec2:ModifyNetworkInterfaceAttribute",
      "fsx:DescribeFileSystems",
      "fsx:DescribeStorageVirtualMachines",
      "elasticfilesystem:DescribeAccessPoints",
      "elasticfilesystem:DescribeFileSystems",

```

```

        "elasticfilesystem:DescribeMountTargets",
        "iam:GetRole",
        "iam:ListRoles",
        "logs:CreateLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeResourcePolicies",
        "outposts:ListOutposts",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3-outposts:ListAccessPoints",
        "s3-outposts:ListRegionalBuckets",
        "secretsmanager:ListSecrets",
        "kms:ListAliases",
        "kms:DescribeKey"
    ],
    "Resource": "*"
},
{
    "Sid": "DataSyncPassRolePermissions",
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "datasync.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "DataSyncCreateSLRPermissions",
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/
datasync.amazonaws.com/AWSServiceRoleForDataSync",
    "Condition": {
        "StringEquals": {

```

```

        "iam:AWSServiceName": "datasync.amazonaws.com"
    }
}
},
{
    "Sid": "DataSyncSecretsManagerCreateAccess",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:CreateSecret"
    ],
    "Resource": [
        "arn:*:secretsmanager:*:secret:aws-datasync!*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid": "DataSyncSecretsManagerAccess",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:DeleteSecret",
        "secretsmanager:UpdateSecret",
        "secretsmanager:PutSecretValue"
    ],
    "Resource": [
        "arn:aws:secretsmanager:*:secret:aws-datasync!*"
    ],
    "Condition": {
        "StringEquals": {
            "secretsmanager:ResourceTag/
aws:secretsmanager:owningService": "aws-datasync",
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
}
]
}

```


AWS política gerenciada: AWSDDataSyncServiceRolePolicy

É possível anexar a política `AWSDDataSyncServiceRolePolicy` a suas identidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite DataSync realizar ações em seu nome. Para obter mais informações, consulte [Usar perfis vinculados a serviço do DataSync](#).

Essa política concede permissões administrativas que permitem que a função vinculada ao serviço crie CloudWatch registros da Amazon para DataSync tarefas usando o modo Avançado.

Atualizações da política

Alteração	Descrição	Data
AWSDDataSyncFullAccess: alteração	DataSync declarações de permissão modificadas para <code>AWSDDataSyncFullAccess</code> : As instruções atualizadas removem as condições de marcação das permissões DataSync usadas para criar segredos do Secrets Manager.	13 de maio de 2025
AWSDDataSyncFullAccess: alteração	DataSync adicionou novas permissões para <code>AWSDDataSyncFullAccess</code> : • <code>secretsmanager:CreateSecret</code> • <code>secretsmanager:PutSecretValue</code> • <code>secretsmanager:DeleteSecret</code> • <code>secretsmanager:UpdateSecret</code>	7 de maio de 2025

Alteração	Descrição	Data
	Essas permissões permitem DataSync criar, editar e excluir AWS Secrets Manager segredos.	
<u>AWSDDataSyncFullAccess:</u> alteração	DataSync adicionou novas permissões para <code>AWSDDataSyncFullAccess</code> : • <code>secretsmanager:ListSecrets</code> • <code>kms:ListAliases</code> • <code>kms:DescribeKey</code> Essas permissões permitem DataSync recuperar metadados sobre seus AWS Secrets Manager segredos e AWS KMS chaves, incluindo quaisquer aliases associados às suas chaves.	23 de abril de 2025

Alteração	Descrição	Data
AWSDataSyncServiceRolePolicy : alteração	DataSync adicionou novas permissões à <code>AWSDataSyncServiceRolePolicy</code> política usada pela função DataSync vinculada ao serviço: <code>AWSServiceRoleForDataSync</code> • <code>secretsmanager:DescribeSecret</code> • <code>secretsmanager:GetSecretValue</code> Essas permissões permitem DataSync ler metadados e valores de segredos gerenciados pelo AWS Secrets Manager.	15 de abril de 2025
AWSDataSyncServiceRolePolicy – Nova política	DataSync adicionou uma política que é usada pela função DataSync vinculada ao serviço. <code>AWSServiceRoleForDataSync</code> Essa nova política gerenciada cria automaticamente CloudWatch registros da Amazon para suas DataSync tarefas que usam o modo Avançado.	30 de outubro de 2024

Alteração	Descrição	Data
<u>AWSDataSyncFullAccess:</u> alteração	DataSync adicionou uma nova permissão paraAWSDataSyncFullAccess : • iam:CreateServiceLinkedRole Essa permissão permite DataSync criar funções vinculadas a serviços para você.	30 de outubro de 2024
<u>AWSDataSyncFullAccess:</u> alteração	DataSync adicionou uma nova permissão paraAWSDataSyncFullAccess : • ec2:DescribeRegions Essa permissão permite que você escolha regiões opcionais ao criar uma DataSync tarefa para transferências entre Regiões da AWS elas.	22 de julho de 2024

Alteração	Descrição	Data
AWSDataSyncFullAccess : alteração	DataSync adicionou uma nova permissão paraAWSDataSy ncFullAccess : • s3:ListBucketVersi ons Essa permissão permite que você escolha uma versão específica do seu DataSync manifesto.	16 de fevereiro de 2024

Alteração	Descrição	Data
<u>AWSDataSyncFullAccess:</u> alteração	DataSync adicionou novas permissões para <code>AWSDataSyncFullAccess</code> : • <code>ec2:DescribeVpcEndpoints</code> • <code>elasticfilesystem:DescribeAccessPoints</code> • <code>fsx:DescribeStorageVirtualMachines</code> • <code>outposts:ListOutposts</code> • <code>s3:GetBucketLocation</code> • <code>s3-outposts:ListAccessPoints</code> • <code>s3-outposts:ListRegionalBuckets</code> Essas permissões ajudam você a criar DataSync agentes e locais para Amazon EFS, Amazon FSx for NetApp ONTAP, Amazon S3 e S3 on Outposts.	2 de maio de 2023
DataSync começou a rastrear as alterações	DataSync começou a rastrear as mudanças em suas políticas AWS gerenciadas.	1.º de março de 2021

Políticas gerenciadas pelo cliente do IAM para o AWS DataSync

Além das políticas AWS gerenciadas, você também pode criar suas próprias políticas baseadas em identidade AWS DataSync e anexá-las às identidades AWS Identity and Access Management (IAM) que exigem essas permissões. Políticas gerenciadas pelo cliente são políticas autônomas que você administra na sua própria Conta da AWS.

Important

Antes de começar, recomendamos que você conheça os conceitos básicos e as opções para gerenciar o acesso aos seus DataSync recursos. Para obter mais informações, consulte [Gerenciamento de acesso para AWS DataSync](#).

Ao criar uma política gerenciada pelo cliente, você inclui declarações sobre DataSync operações que podem ser usadas em determinados AWS recursos. A política de exemplo a seguir tem duas declarações (observe os elementos `Action` e `Resource` em ambas as declarações):

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsSpecifiedActionsOnAllTasks",
      "Effect": "Allow",
      "Action": [
        "datasync:DescribeTask",
      ],
      "Resource": "arn:aws:datasync:us-east-2:111222333444:task/*"
    },
    {
      "Sid": "ListAllTasks",
      "Effect": "Allow",
      "Action": [
        "datasync:ListTasks"
      ],
      "Resource": "*"
    }
  ]
}
```

As declarações da política fazem o seguinte:

- A primeira declaração concede permissões para realizar a ação `datasync:DescribeTask` em determinados recursos da tarefa de transferência especificando um nome do recurso da Amazon (ARN) com um caractere curinga (*).
- A segunda instrução concede permissões para realizar a ação `datasync:ListTasks` em todas as tarefas especificando apenas um caractere curinga (*).

Exemplos de políticas gerenciadas pelo cliente

O exemplo a seguir de políticas gerenciadas pelo cliente concede permissões para várias DataSync operações. As políticas funcionam se você estiver usando o AWS Command Line Interface (AWS CLI) ou um AWS SDK. Para usar essas políticas no console, você também deve usar a política gerenciada `AWSDataSyncFullAccess`.

Tópicos

- [Exemplo 1: Crie uma relação de confiança que permita DataSync acessar seu bucket do Amazon S3](#)
- [Exemplo 2: Permitir DataSync a leitura e gravação em seu bucket do Amazon S3](#)
- [Exemplo 3: Permitir DataSync o upload de registros para grupos de CloudWatch registros](#)

Exemplo 1: Crie uma relação de confiança que permita DataSync acessar seu bucket do Amazon S3

Veja a seguir um exemplo de uma política de confiança que permite DataSync assumir uma função do IAM. Essa função permite DataSync acessar um bucket do Amazon S3. Para evitar o [problema adjunto confuso de vários serviços](#), recomendamos usar as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` na política.

JSON

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



```

        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "123456789012"
            },
            "StringLike": {
                "aws:SourceArn": "arn:aws:datasync:us-east-2:123456789012:*"
            }
        }
    }
}

```

Exemplo 2: Permitir DataSync a leitura e gravação em seu bucket do Amazon S3

O exemplo de política DataSync a seguir concede as permissões mínimas para ler e gravar dados em um bucket do S3 usado como local de destino.

Note

O valor de `aws:ResourceAccount` deve ser o ID da conta que possui o bucket do Amazon S3 especificado na política.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ],
}

```

```
{
  "Action": [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectTagging",
    "s3:GetObjectVersion",
    "s3:GetObjectVersionTagging",
    "s3:ListMultipartUploadParts",
    "s3:PutObject",
    "s3:PutObjectTagging"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "123456789012"
    }
  }
}
```

Exemplo 3: Permitir DataSync o upload de registros para grupos de CloudWatch registros

DataSync requer permissões para poder fazer upload de registros para seus grupos de CloudWatch registros da Amazon. Você pode usar grupos de CloudWatch registros para monitorar e depurar suas tarefas.

Para obter um exemplo de política do IAM que concede essas permissões, consulte [DataSync Permitindo o upload de registros para um grupo de CloudWatch registros](#).

Usar perfis vinculados a serviço do DataSync

AWS DataSync usa funções [vinculadas ao serviço AWS Identity and Access Management](#) (IAM).

Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente

a. DataSync As funções vinculadas ao serviço são predefinidas DataSync e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Tópicos

- [Usando funções para DataSync](#)

Usando funções para DataSync

AWS DataSync usa funções [vinculadas ao serviço AWS Identity and Access Management](#) (IAM).

Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente

a. DataSync As funções vinculadas ao serviço são predefinidas DataSync e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração DataSync porque você não precisa adicionar manualmente as permissões necessárias. DataSync define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só DataSync pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado ao serviço poderá ser excluído somente após excluir seus atributos relacionados. Isso protege seus DataSync recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte [AWS Serviços que funcionam com IAM](#) e procure os serviços que têm Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

Permissões de função vinculadas ao serviço para DataSync

DataSync usa a função vinculada ao serviço chamada `AWSServiceRoleForDataSync`— Permite realizar operações essenciais para DataSync a execução de tarefas de transferência, incluindo a leitura de segredos e a criação de AWS Secrets Manager grupos e eventos de CloudWatch log.

A função `AWSServiceRoleForDataSync` vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `datasync.amazonaws.com`

A função vinculada ao serviço usa a política AWS gerenciada chamada [AWSDataSyncServiceRolePolicy](#), que permite DataSync concluir as seguintes ações nos recursos especificados:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DataSyncCloudWatchLogCreateAccess",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogGroup",
      "logs:CreateLogStream"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/datasync*"
    ]
  },
  {
    "Sid": "DataSyncCloudWatchLogStreamUpdateAccess",
    "Effect": "Allow",
    "Action": [
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/datasync*:log-stream:*"
    ]
  },
  {
    "Sid": "DataSyncSecretsManagerReadAccess",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:DescribeSecret",
      "secretsmanager:GetSecretValue"
    ],
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:aws-datasync!*"
    ],
    "Condition": {
      "StringEquals": {
        "secretsmanager:ResourceTag/
aws:secretsmanager:owningService": "aws-datasync",
        "aws:ResourceAccount": "${aws:PrincipalAccount}"
      }
    }
  }
]
```

```
} ]
```

Você deve configurar permissões para permitir que seus usuários, grupos ou perfis criem, editem ou excluam um perfil vinculado ao serviço. Para ter mais informações, consulte [Permissões de função vinculada a serviços](#) no Guia do usuário do IAM.

Criação de uma função vinculada ao serviço para o DataSync

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria uma DataSync tarefa na AWS Management Console, na ou na AWS API AWS CLI, DataSync cria a função vinculada ao serviço para você.

Na AWS CLI ou na AWS API, você pode criar uma função vinculada ao serviço com o nome do `datasync.amazonaws.com` serviço. Para obter mais informações, consulte [Criar um perfil vinculado a serviço](#) no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, será possível usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria uma DataSync tarefa, DataSync cria a função vinculada ao serviço para você novamente.

Se excluir esse perfil vinculado ao serviço, será possível usar o mesmo processo do IAM para criar o perfil novamente.

Editar um perfil vinculado ao serviço para o DataSync

DataSync não permite que você edite a função `AWSServiceRoleForDataSync` vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar uma função vinculada a serviço](#) no Guia do usuário do IAM.

Excluir um perfil vinculado ao serviço para o DataSync

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar seu perfil vinculado ao serviço para excluí-la manualmente.

Limpar um perfil vinculado ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir qualquer recurso usado pelo perfil.

Note

Se o DataSync serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir DataSync recursos usados pelo AWSService RoleForDataSync

1. [Exclua DataSync os agentes](#) usados pela tarefa (se houver).
2. [Exclua os locais da tarefa](#).
3. [Exclua a tarefa](#).

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSService RoleForDataSync vinculada ao serviço. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Regiões suportadas por perfis vinculados a serviço do DataSync

DataSync suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte [Regiões e endpoints da AWS](#).

Permissões para marcar DataSync recursos durante a criação

Algumas ações de AWS DataSync API de criação de recursos permitem que você especifique tags ao criar o recurso. É possível usar tags de recursos para implantar o controle de acesso por atributo (ABAC). Para obter mais informações, consulte [Para que serve o ABAC?](#) AWS no Guia do usuário do IAM.

Para permitir que os usuários marquem recursos na criação, eles devem ter permissões para usar a ação que cria o recurso, como `datasync:CreateAgent` ou `datasync:CreateTask`. Se as tags

forem especificadas na ação de criação de recursos, os usuários também precisarão ter permissões claras para usar a ação `datasync:TagResource`.

A ação `datasync:TagResource` será avaliada somente se as tags forem aplicadas durante a ação `resource-creating`. Portanto, um usuário que tiver permissões para criar um recurso (pressupondo-se que não existam condições de marcação) não precisa de permissão para usar a ação `datasync:TagResource` se nenhuma tag for especificada na solicitação.

Contudo, se o usuário tentar criar um recurso com tags, haverá falha na solicitação se o usuário não tiver permissão para usar a ação `datasync:TagResource`.

Exemplo de instruções de política do IAM

Use o exemplo de declarações de política do IAM a seguir para conceder `TagResource` permissões aos usuários que criam DataSync recursos.

A declaração a seguir permite que os usuários DataSync marquem um agente ao criar o agente.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "datasync:TagResource",
      "Resource": "arn:aws:datasync:region:account-id:agent/*"
    }
  ]
}
```

A declaração a seguir permite que os usuários DataSync marquem um local ao criá-lo.

JSON

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

```

        "Action": "datasync:TagResource",
        "Resource": "arn:aws:datasync:region:account-id:location/*"
    }
]
}

```

A declaração a seguir permite que os usuários DataSync marquem uma tarefa ao criá-la.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "datasync:TagResource",
      "Resource": "arn:aws:datasync:region:account-id:task/*"
    }
  ]
}

```

Prevenção contra o ataque do “substituto confuso” em todos os serviços

“Confused deputy” é um problema de segurança no qual uma entidade sem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A personificação entre serviços 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.

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 AWS DataSync concede outro serviço ao recurso. Se você utilizar ambas as chaves de contexto de condição global e o valor de `aws:SourceArn` contiver o ID da conta, o valor de `aws:SourceAccount` e a conta no valor de `aws:SourceArn` deverão utilizar o mesmo ID de conta quando utilizados na mesma declaração da política. Use `aws:SourceArn` se quiser que apenas um

recurso seja associado ao acesso entre serviços. Use `aws:SourceAccount` se quiser que qualquer recurso nessa conta seja associado ao uso entre serviços.

O valor de `aws:SourceArn` deve incluir o ARN do DataSync local com o qual DataSync é permitido assumir a função do IAM.

A maneira mais eficaz de se proteger contra o problema do confused deputy é usar a chave `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo ou estiver especificando vários recursos, use os caracteres curingas (*) para as partes desconhecidas. Aqui estão alguns exemplos de como fazer isso para DataSync:

- Para limitar a política de confiança a um DataSync local existente, inclua o ARN completo do local na política. DataSync assumirá a função do IAM somente ao lidar com aquele local específico.
- Ao criar um local do Amazon S3 para DataSync, você não sabe o ARN do local. Nesses cenários, use o seguinte formato para a chave `aws:SourceArn`: `arn:aws:datasync:us-east-2:123456789012:*`. Este formato valida a partição (aws), o ID da conta e a região.

O exemplo completo a seguir mostra como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves de contexto em uma política de confiança para evitar o problema confuso do substituto com DataSync.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:datasync:us-east-2:123456789012:*"
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

Para obter mais exemplos de políticas que mostram como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e com DataSync, consulte os tópicos a seguir:

- [Crie uma relação de confiança que permita DataSync acessar seu bucket do Amazon S3](#)
- [Configurar um perfil do IAM para acessar o bucket do Amazon S3](#)

Validação de conformidade para AWS DataSync

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. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Governança e conformidade de segurança](#): esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- [Referência de serviços qualificados para HIPAA](#): lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a HIPAA.
- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).

- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#)— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- [AWS Audit Manager](#)— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência em AWS DataSync

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.

Note

Se uma zona de disponibilidade para a qual você está migrando dados falhar durante a execução de uma DataSync tarefa, a tarefa também falhará.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte [infraestrutura AWS global](#).

Segurança da infraestrutura em AWS DataSync

Como serviço gerenciado, AWS DataSync 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 DataSync pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

Protegendo as credenciais do local de armazenamento

DataSync usa [locais](#) para acessar seus recursos de armazenamento localizados no local, em outras nuvens ou em AWS. Alguns tipos de localização exigem que você forneça credenciais, como chave de acesso e chave secreta ou nome de usuário e senha, para se autenticar no sistema de armazenamento. Ao criar um DataSync local que exige credenciais para autenticação, você pode escolher uma das seguintes opções para controlar como o segredo de suas credenciais é armazenado:

- Armazene o segredo AWS Secrets Manager usando um segredo gerenciado pelo serviço criptografado com uma chave padrão.
- Armazene o segredo AWS Secrets Manager usando um segredo gerenciado pelo serviço criptografado com uma AWS KMS chave que você gerencia.
- Armazene o segredo AWS Secrets Manager usando um segredo e uma chave que você cria e gerencia. DataSync acessa esse segredo usando uma função do IAM fornecida por você.

Em todos os casos, o segredo do Secrets Manager é armazenado em sua conta, permitindo que você atualize o segredo conforme necessário, independentemente do DataSync serviço. Você é cobrado apenas pelo uso de segredos que você cria fora do DataSync. Segredos criados e gerenciados por DataSync têm o prefixo `aws-datasync`.

Usando um segredo gerenciado pelo serviço criptografado com uma chave padrão

Ao criar sua DataSync localização, basta fornecer a string secreta. DataSync cria um recurso secreto AWS Secrets Manager para armazenar o segredo que você fornece e criptografa o segredo com a chave KMS padrão do Secrets Manager para sua conta. Você pode alterar o valor secreto diretamente no Secrets Manager ou atualizando o local usando o DataSync console ou o SDK. AWS CLI Quando você exclui o recurso de localização ou o atualiza para usar um segredo personalizado, DataSync exclui o recurso secreto automaticamente.

Note

Para criar, modificar e excluir recursos secretos no Secrets Manager, é necessário ter as permissões apropriadas. Para obter mais informações, consulte [Políticas gerenciadas pela AWS para DataSync](#).

Usando um segredo gerenciado pelo serviço criptografado com uma chave personalizada AWS KMS

Ao criar sua DataSync localização, você fornece o segredo e o ARN da sua AWS KMS chave. DataSync cria automaticamente um recurso secreto AWS Secrets Manager para armazenar o segredo que você fornece e o criptografa usando sua AWS KMS chave. Você pode alterar o valor secreto diretamente no Secrets Manager ou atualizando o local usando o DataSync console ou o SDK. AWS CLI Quando você exclui o recurso de localização ou o atualiza para usar um segredo personalizado, DataSync exclui o recurso secreto automaticamente.

Note

Sua AWS KMS chave deve usar criptografia simétrica com o tipo de `ENCRYPT_DECRYPT` chave. Para obter mais informações, consulte [Como escolher uma AWS Key Management Service chave](#) no Guia AWS Secrets Manager do usuário.

Para criar, modificar e excluir recursos secretos no Secrets Manager, é DataSync necessário ter as permissões apropriadas. Para obter mais informações, consulte [Políticas gerenciadas pela AWS : AWSDataSyncFullAccess](#).

Além de usar a política DataSync gerenciada correta, você também precisa das seguintes permissões:

```
{
  "Sid": "DataSyncKmsPermissions",
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "your-kms-key-arn",
  "Condition": {
    "StringLike": {
      "kms:ViaService": "secretsmanager.*.amazonaws.com"
    }
  }
}
```

your-kms-key-arn Substitua pelo ARN da sua chave KMS.

Para recuperar e descriptografar o valor secreto, DataSync use uma função vinculada ao serviço (SLR) para acessar sua chave. AWS KMS Para garantir que DataSync você possa usar sua chave KMS, adicione o seguinte à declaração de política da chave:

```
{
  "Sid": "Allow DataSync to use the key for decryption",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::accountid:role/aws-service-role/
datasync.amazonaws.com/AWSServiceRoleForDataSync"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}
```

accountid Substitua pelo seu Conta da AWS ID.

Usando um segredo que você gerencia

Antes de criar sua DataSync localização, [crie uma entrada secreta AWS Secrets Manager](#). O valor do segredo deve conter somente a própria string secreta em texto simples. Ao criar sua DataSync localização, você fornece o ARN do seu segredo e uma função do IAM que DataSync usa para acessar seu segredo e a AWS KMS chave usada para criptografá-lo. Para criar uma função do IAM com as permissões apropriadas, faça o seguinte:

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação esquerdo, em Gerenciamento de acesso, escolha Perfis e, em seguida, escolha Criar perfil.
3. Na página Selecionar entidade confiável, em Tipo de entidade confiável, escolha AWS serviço.
4. Para Caso de uso, escolha na DataSync lista suspensa. Escolha Próximo.
5. Na página Adicionar permissões, escolha Próximo. Insira um nome para sua função e escolha Criar função.
6. Na página Perfis, procure o perfil que você acabou de criar e escolha seu nome.
7. Na página Detalhes da função, escolha a guia Permissões. Escolha Adicionar permissões e, em seguida, Criar política em linha.
8. Escolha a guia JSON e adicione as seguintes permissões ao editor de políticas:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": "your-secret-arn"
    }
  ]
}
```

your-secret-arn Substitua pelo ARN do seu segredo do Secrets Manager.

9. Escolha Próximo. Insira um nome para sua política e escolha Criar política.
10. (Recomendado) Para evitar o [problema “confused deputy” entre serviços](#), faça o seguinte:
 - a. Na página Detalhes da função, escolha a guia Relações de confiança. Escolha Editar política de confiança.
 - b. Atualize a política de confiança usando o exemplo a seguir, que inclui as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount`:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:datasync:region:account-
id:*"
        }
      }
    }
  ]
}
```

- c. Escolha Atualizar política.

Você pode especificar essa função ao criar sua localização. Se seu segredo usa uma AWS KMS chave gerenciada pelo cliente para criptografia, você também precisará atualizar a política da chave para permitir o acesso da função que você criou no procedimento anterior. Para atualizar a política, adicione o seguinte à declaração de política da sua AWS KMS chave:


```
{
  "Sid": "Allow DataSync use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam accountid:role/your-role-name"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}
```

accountid Substitua pelo seu Conta da AWS ID e *your-role-name* pelo nome da função do IAM que você criou no procedimento anterior.

 Note

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

AWS DataSync cotas

Saiba mais sobre cotas e limites de recursos ao trabalhar com AWS DataSync.

Limites do sistema de armazenamento, arquivos e objetos

A tabela a seguir descreve os limites DataSync que existem ao trabalhar com sistemas de armazenamento, arquivos e objetos.

Descrição	Limite
Tamanho máximo total do caminho do arquivo	4,096 bytes
Tamanho máximo do componente do caminho do arquivo (nome do arquivo, diretório ou subdiretório)	255 bytes
Tamanho máximo do domínio do Windows	253 caracteres
Tamanho máximo do nome do host do servidor	255 caracteres
Tamanho máximo do nome do objeto do Amazon S3	1.024 caracteres UTF-8

DataSync cotas

A tabela a seguir descreve as cotas de DataSync recursos em uma região específica Conta da AWS .

Recurso	Quota	Ajustável
Número máximo de tarefas que você pode criar	100	Sim
(Tarefas do modo aprimorado) Número máximo de objetos de origem e destino com os quais DataSync podem trabalhar por execução de tarefa	Praticamente ilimitado	N/D

Recurso	Quota	Ajustável
Para obter mais informações, consulte Como DataSync transfere arquivos, objetos e diretório S.		

Recurso	Quota	Ajustável
(Tarefas do modo básico) Número máximo de arquivos, objetos e diretórios de origem e destino que DataSync podem funcionar por execução de tarefa entre serviços locais, autogerenciados ou outros serviços de armazenamento e armazenamento em nuvem AWS Para obter mais informações, consulte Como DataSync transfere arquivos, objetos e diretórios.	50 milhões  Important Lembre-se do seguinte sobre essa cota: - Se você transferir objetos do Amazon S3 com prefixos, os prefixos serão tratados como diretórios e contabilizados na cota. Por exemplo, DataSync consideraria <code>s3://bucket/foo/bar.txt</code> como dois diretórios (<code>./e./foo/</code>) e um objeto (<code>bar.txt</code>). - Se sua tarefa estiver trabalhando com mais de 20 milhões de arquivos, objetos ou diretórios, certifique-se de alocar um mínimo de 64 GB de RAM para seu DataSync agente. Para obter mais informações, consulte os requisitos do agente para	Sim  Tip Em vez de solicitar um aumento, você pode criar tarefas focadas em diretórios específicos usando filtros de inclusão e exclusão. Para obter mais informações, consulte como filtrar os

Recurso	Quota	Ajustável
	<u>DataSync transferências.</u>	<u>dados transferidos por DataSync.</u>

Recurso	Quota	Ajustável
(Tarefas do modo básico) Número máximo de arquivos, objetos e diretórios de origem e destino que DataSync podem funcionar por execução de tarefa entre os serviços AWS de armazenamento Para obter mais informações, consulte Como DataSync transfere arquivos, objetos e diretório.	25 milhões  Important Se você transferir objetos do Amazon S3 com prefixos, os prefixos serão tratados como diretórios e contabilizados na cota. Por exemplo, DataSync consideraria <code>s3://bucket/foo/bar.txt</code> como dois diretórios (<code>./e./foo/</code>) e um objeto (<code>bar.txt</code>).	Sim  Tip Em vez de solicitar um aumento, você pode criar tarefas focadas em diretórios específicos usando filtros de inclusão e exclusão. Para obter mais informações, consulte filtrar os

Recurso	Quota	Ajustável
		dados transferidos por DataSync.
Taxa de transferência máxima por tarefa (para transferências que usam um DataSync agente)	10 Gbps	Não
Taxa de transferência máxima por tarefa (para transferências que não usam um DataSync agente)	5 Gbps	Não
Número máximo de caracteres que você pode incluir em um filtro de tarefas	102,400 caracteres	Não
	 Note Se você estiver usando o DataSync console, esse limite inclui todos os caracteres combinados em seus padrões de inclusão e exclusão.	
Número máximo de execuções em fila para uma única tarefa	50	Não
Número máximo de execuções simultâneas de tarefas no modo Avançado	120	Não
Número máximo de dias durante os quais o histórico de execução de tarefas é mantido	30	Não

Solicitar um aumento da cota

Você pode solicitar um aumento para algumas DataSync cotas. Os aumentos não são concedidos imediatamente e podem levar alguns dias para entrarem em vigor.

Para solicitar um aumento da cota

1. Abra o console do Service Quotas em <https://console.aws.amazon.com/servicequotas/>.
2. No painel de navegação, escolha Services da AWS e depois AWS DataSync.
3. Escolha a cota que você deseja aumentar e depois escolha Solicitar aumento ao nível da conta.
4. Insira o valor total da cota que você deseja e escolha Solicitar.

Se você precisa aumentar uma cota diferente, preencha uma solicitação separada.

Solução de AWS DataSync problemas

Use as informações a seguir para solucionar AWS DataSync problemas e erros.

Tópicos

- [Solução de problemas com DataSync agentes](#)
- [Solução de problemas com DataSync locais](#)
- [Solução de problemas com DataSync tarefas](#)
- [Solução de problemas de verificação de dados](#)
- [Solução de problemas de custos de armazenamento S3 acima do esperado com DataSync](#)

Solução de problemas com DataSync agentes

Use as informações a seguir para ajudá-lo a solucionar problemas com AWS DataSync agentes.

Alguns desses problemas podem incluir:

- Problemas na conexão com o console local de um EC2 agente da Amazon
- Falha ao recuperar a chave de ativação de um agente
- Problemas ao ativar um agente com um endpoint de serviço VPC
- Descobrir que um agente está off-line

Como faço para me conectar ao console local de um EC2 agente da Amazon?

Para se conectar ao console local de um EC2 agente da Amazon, você deve usar SSH. Certifique-se de que o grupo de segurança da sua EC2 instância permita acesso com SSH (porta TCP 22).

Em um terminal, execute o seguinte comando `ssh` para se conectar à instância:

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-ip-address
```

- Para `/path/key-pair-name`, especifique o caminho e o nome do arquivo (`.pem`) da chave privada necessária para se conectar à sua instância.

- Em *instance-user-name*, especifique admin.
- Para *instance-public-ip-address*, especifique o endereço IP público da sua instância.

O que significa o erro Falha ao recuperar a chave de ativação do agente?

Ao ativar seu DataSync agente, o agente se conecta ao endpoint de serviço que você especifica para solicitar uma chave de ativação. Esse erro provavelmente significa que suas configurações de segurança de rede estão bloqueando a conexão.

Medida a ser tomada

Se você estiver usando um endpoint de serviço de nuvem privada virtual (VPC), verifique se as configurações do grupo de segurança permitem que o agente se conecte ao endpoint da VPC. Para obter informações sobre as portas necessárias, consulte [Requisitos de rede para endpoints de serviço da VPC](#).

Se você estiver usando um endpoint público ou Federal Information Processing Standard (FIPS), verifique se as configurações de firewall e roteador permitem que o agente se conecte ao endpoint. Para mais informações, consulte [Requisitos de rede para endpoints de serviço públicos ou FIPS](#).

Ainda não consigo ativar um agente usando um endpoint de serviço VPC

Se você ainda estiver tendo problemas para ativar um DataSync agente com um endpoint de serviço VPC, consulte [Não sei o que está acontecendo com meu agente. Alguém pode me ajudar?](#)

O que eu faço se meu agente estiver off-line?

Seu DataSync agente pode estar off-line por alguns motivos, mas talvez você consiga colocá-lo novamente on-line. Antes de excluir o agente e criar um novo, consulte a lista de verificação a seguir para ajudar você a entender o que pode ter acontecido.

- Entre em contato com sua equipe de backup: se seu agente estiver off-line porque sua máquina virtual (VM) foi restaurada a partir de um snapshot ou backup, talvez seja necessário [substituir o agente](#).
- Verifique se a VM do agente ou a EC2 instância da Amazon está desativada — dependendo do tipo de agente que você está usando, tente reativar a VM ou a EC2 instância se ela estiver desativada. Quando estiver ligado novamente, [teste a conectividade de rede do seu agente](#) com AWS o.

- Verifique se seu agente atende aos requisitos mínimos de hardware — Seu agente pode estar off-line porque a configuração da VM ou da EC2 instância foi alterada acidentalmente desde que o agente foi ativado. Por exemplo, se sua VM não tiver mais a memória ou o espaço mínimos necessários, o agente poderá aparecer como off-line. Para obter mais informações, consulte [Requisitos para AWS DataSync agentes](#).
- Aguarde a conclusão das atualizações de software relacionadas ao agente: seu agente pode ficar off-line brevemente após as [atualizações de software fornecidas pela AWS](#). Se você acredita que é por isso que o agente está off-line, aguarde um curto período e verifique se o agente está online novamente.
- Verifique suas configurações de VPC Service Endpoint — [Se seu agente off-line estiver usando um endpoint de serviço público e também na mesma VPC em que você criou um endpoint de serviço VPC DataSync, talvez seja necessário desativar o suporte de DNS privado para esse VPC endpoint](#).

Se nenhum desses parece ser o motivo pelo qual o agente está off-line, você provavelmente precisará [substituí-lo](#).

Não sei o que está acontecendo com meu agente. Alguém pode me ajudar?

Você pode permitir AWS Support o acesso ao seu DataSync agente e ajudar a solucionar problemas relacionados ao agente. Você deve habilitar esse acesso usando o console local do agente.

Para fornecer Suporte acesso ao seu agente

1. [Faça login no console local do agente](#).
2. No prompt, digite **5** para abrir o prompt de comando (para VMware VMs, use **6**).
3. Insira **h** para abrir a janela COMANDOS DISPONÍVEIS.
4. Na janela COMANDOS DISPONÍVEIS, digite o seguinte para se conectar ao Suporte:

open-support-channel

Se você estiver usando o agente com VPC endpoints, deverá fornecer um endereço IP de VPC endpoint para seu canal de suporte, da seguinte forma:

open-support-channel *vpc-ip-address*

Seu firewall deve permitir que a porta TCP de entrada 22 inicie um canal de suporte para. AWS Quando você se conecta Suporte, DataSync atribui a você um número de suporte. Anote seu número de suporte.

 Note

O número do canal não é um número de porta TCP/UDP. Na verdade, ele faz uma conexão SSH (TCP 22) com os servidores e fornece o canal de suporte para a conexão.

5. Quando o canal de suporte for estabelecido, forneça seu número de serviço de suporte para Suporte que eles possam fornecer assistência na solução de problemas.
6. Quando a sessão de suporte for concluída, pressione **Enter** para finalizá-la.
7. Digite **exit** para sair do console DataSync local.
8. Siga as instruções para sair do console local.

Solução de problemas com DataSync locais

Use as informações a seguir para ajudá-lo a solucionar problemas com AWS DataSync locais. Alguns desses problemas podem incluir:

- Permissões e erros de montagem com locais NFS
- Problemas de propriedade do arquivo
- Problemas ao acessar locais de pequenas e médias empresas que usam a autenticação Kerberos
- Problemas de permissão e acesso com armazenamento de objetos, como localizações de Amazon S3 e Microsoft Azure Blob

Falha na minha tarefa com um erro de permissões do NFS negadas

Você pode obter a mensagem de erro “permissões negadas” se configurar o servidor de arquivos NFS com `root_squash` ou `all_squash` ativado e nem todos seus arquivos têm acesso de leitura.

Medida a ser tomada

Para corrigir esse problema, configure a exportação de NFS com `no_root_squash` ou tenha certeza de que as permissões para todos os arquivos que você deseja transferir permitem acesso de leitura para todos os usuários.

DataSync Para acessar os diretórios, você também deve habilitar o acesso a todas as execuções. Para garantir que o diretório possa ser montado, primeiro conecte-se a qualquer computador que tenha a mesma configuração de rede que o agente. Depois execute o seguinte comando da CLI:

```
mount -t nfs -o nfsvers=<your-nfs-server-version> <your-nfs-server-name>:<nfs-export-path-you-specified> <new-test-folder-on-your-computer>
```

Se o problema ainda não tiver sido resolvido, entre em contato com a [Central AWS Support](#).

Falha na minha tarefa com um erro de montagem do NFS

Você pode ver o seguinte erro ao executar uma DataSync tarefa que envolve uma localização de servidor de arquivos NFS:

Falha na tarefa ao acessar o local loc-1111222233334444a: x40016: mount.nfs: tempo limite de conexão expirado

Medidas a serem tomadas

Faça o seguinte até o erro ser resolvido:

1. Verifique se o servidor de arquivos NFS e a exportação especificados em seu DataSync local são válidos. Se não forem, exclua o local e a tarefa e crie um local e uma tarefa novos que usem um servidor de arquivos e uma exportação NFS válidos. Para obter mais informações, consulte [Usar o console de DataSync](#).
2. Verifique a configuração do firewall entre o agente e o servidor de arquivos NFS. Para obter mais informações, consulte [Requisitos de rede para armazenamento on-premises, autogerenciado, em outra nuvem e a na borda](#).
3. Certifique-se de que seu agente possa acessar o servidor de arquivos NFS e montar a exportação. Para obter mais informações, consulte [Fornecendo DataSync acesso aos servidores de arquivos NFS](#).
4. Se o erro persistir, abra um canal de suporte com Suporte. Para obter mais informações, consulte [Não sei o que está acontecendo com meu agente. Alguém pode me ajudar?](#).

Falha na minha tarefa com um erro de montagem do Amazon EFS

Você pode ver o seguinte erro ao executar uma DataSync tarefa que envolve uma localização do Amazon EFS:

Falha na tarefa ao acessar o local loc-1111222233334444a: x40016: falha ao se conectar ao destino de montagem do EFS com IP: 10.10.1.0.

Isso pode acontecer se o caminho de montagem do sistema de arquivos Amazon EFS que você configura com sua localização for atualizado ou excluído. DataSync não está ciente dessas mudanças no sistema de arquivos.

Ação a realizar

Exclua o local e a tarefa e [crie um novo local do Amazon EFS](#) com o novo caminho de montagem.

A propriedade do arquivo não é mantida com a transferência do NFS

Após a transferência, você pode notar que os arquivos em seu local de DataSync destino têm usuário IDs (UIDs) ou grupo IDs (GIDs) diferente dos mesmos arquivos em seu local de origem. Por exemplo, os arquivos no destino podem ter um UID de 65534, 99 ou nobody.

Isso pode acontecer se um sistema de arquivos envolvido na sua transferência usar o mapeamento de ID NFS versão 4, um recurso que DataSync não é compatível.

Ação a realizar

Você tem algumas opções para contornar esse problema:

- Criar um novo local para o sistema de arquivos que use o NFS versão 3 em vez da versão 4.
- Desativar o mapeamento de ID do NFS versão 4 no sistema de arquivos.

Repetir a transferência. Qualquer uma das opções deve resolver o problema.

Minha tarefa não consegue acessar um local SMB que usa Kerberos

DataSync erros em locais SMB que usam a [autenticação Kerberos](#) geralmente estão relacionados a incompatibilidades entre sua localização e as configurações do Kerberos. Também pode haver um problema de rede.

Falha ao acessar o local

O erro a seguir indica que pode haver problemas de configuração com sua localização SMB ou com a configuração do Kerberos:

```
Task failed to access location
```

Verifique o seguinte:

- O servidor de arquivos SMB que você especifica para sua localização é um nome de domínio. Para Kerberos, você não pode especificar o endereço IP do servidor de arquivos.
- O principal do Kerberos que você especifica para sua localização corresponde ao principal usado para criar o arquivo da tabela de chaves do Kerberos (keytab). Os nomes principais diferenciam maiúsculas de minúsculas.
- A senha de usuário mapeada do diretor do Kerberos não mudou desde que você criou o arquivo keytab. Se a senha mudar (devido à rotação da senha ou por algum outro motivo), a execução da tarefa poderá falhar com o seguinte erro:

Falha na tarefa ao acessar o local loc-1111222233334444a: x40015: kinit: a pré-autenticação falhou ao obter as credenciais iniciais

Não consigo entrar em contato com o reino KDC

O erro a seguir indica um problema de rede:

```
kinit: Cannot contact any KDC for realm 'MYDOMAIN.ORG' while getting initial credentials"
```

Verifique o seguinte:

- O arquivo de configuração Kerberos (`krb5.conf`) que você forneceu DataSync tem as informações corretas sobre sua região Kerberos. Para ver um exemplo de `krb5.conf` arquivo, consulte Pré-requisitos de [autenticação Kerberos](#).
- A porta do servidor Kerberos Key Distribution Center (KDC) está aberta. A porta KDC é normalmente a porta TCP 88.
- A configuração do DNS na sua rede.

Minha tarefa falhou com um erro de entrada/saída

Você pode receber uma input/output error message if your storage system fails I/O solicitação do DataSync agente. Motivos comuns para isso incluem falha no disco do servidor, alterações na configuração do firewall ou falha do roteador de rede.

Se o erro envolver um servidor de arquivos NFS ou em um cluster do Sistema de Arquivos Distribuído do Hadoop (HDFS), use as etapas a seguir para resolver o erro.

Medidas a serem tomadas (NFS)

Primeiro, verifique os logs e as métricas do servidor NFS para determinar se o problema foi originado no servidor NFS. Se sim, resolva esse problema.

e verifique se a configuração de rede não foi alterada. Para verificar se o servidor de arquivos NFS está configurado corretamente e se DataSync pode acessá-lo, faça o seguinte:

1. Configure outro cliente NFS na mesma sub-rede da rede que o agente do .
2. Monte o compartilhamento nesse cliente.
3. Valide se o cliente pode ler e gravar no compartilhamento com êxito.

Medidas a serem tomadas (HDFS)

Faça o seguinte até resolver o erro:

1. Certifique-se de que seu cluster HDFS permita que seu DataSync agente se comunique com o cluster NameNode e as DataNode portas.

Na maioria dos clusters, você pode encontrar os números de porta que o cluster usa nos seguintes arquivos de configuração:

- Para encontrar a NameNode porta, consulte o `core-site.xml` arquivo sob a `fs.default.name` propriedade `fs.default` ou (dependendo da distribuição do Hadoop).
 - Para encontrar a DataNode porta, consulte o `hdfs-site.xml` arquivo abaixo da `dfs.datanode.address` propriedade.
2. No arquivo `hdfs-site.xml`, verifique se a propriedade `dfs.data.transfer.protection` tem apenas um valor. Por exemplo:

```
<property>
  <name>dfs.data.transfer.protection</name>
  <value>privacy</value>
</property>
```

Erro: **FsS3UnableToConnectToEndpoint**

DataSync não consigo se conectar à sua localização [do Amazon S3](#). Isso pode significar que o bucket S3 do local não está acessível ou que o local não está configurado corretamente.

Faça o seguinte até resolver o problema:

- Verifique se DataSync consegue [acessar seu bucket do S3](#).
- Certifique-se de que a localização esteja configurada corretamente usando o DataSync console ou a operação do [DescribeLocationS3](#).

Erro: **FsS3HeadBucketFailed**

DataSync não consegue acessar o bucket do S3 para o qual você está transferindo ou do qual você está transferindo. Verifique se DataSync tem permissão para acessar o bucket usando a operação Amazon S3 [HeadBucket](#). Se você precisar ajustar as permissões, consulte [Fornecendo DataSync acesso aos buckets do S3](#).

A tarefa falha com um **Unable to list Azure Blobs on the volume root** erro

Se sua tarefa de DataSync transferência falhar com um Unable to list Azure Blobs on the volume root erro, pode haver um problema com seu token de assinatura de acesso compartilhado (SAS) ou com seu Azure rede da conta de armazenamento.

Medidas a serem tomadas

Tente o seguinte e execute sua tarefa novamente até corrigir o problema:

- Certifique-se de que seu [token SAS](#) tenha as permissões corretas para acessar seu Microsoft Azure Blob Storage.
- Se você estiver dirigindo seu DataSync agente em Azure, configure sua conta de armazenamento para permitir o acesso da rede virtual em que seu agente reside.
- Se você estiver executando seu agente na Amazon EC2, configure seu Azure firewall de armazenamento para permitir o acesso a partir do endereço IP público do agente.

Para obter informações sobre como configurar seu Azure rede da conta de armazenamento, consulte o [Azure Blob Storage documentação](#).

Erro: **FsAzureBlobVolRootListBlobsFailed**

O token de assinatura de acesso compartilhado (SAS) DataSync usado para acessar seu Microsoft Azure Blob Storage não tem a permissão Lista.

Para resolver o problema, [atualize o local](#) com um token que tenha a permissão de List e tente executar a tarefa novamente.

Erro: **SrcLocHitAccess**

DataSync não consegue acessar sua localização de origem. Verifique se DataSync tem permissão para acessar o local e tente executar sua tarefa novamente.

Erro: **SyncTaskErrorLocationNotAdded**

DataSync não consigo acessar sua localização. Verifique se DataSync tem permissão para acessar o local e tente executar sua tarefa novamente.

A tarefa com o local de origem do S3 falha **HeadObject** ou **GetObjectTagging** erro

Se você estiver transferindo objetos com uma versão específica IDs de um bucket do S3, talvez veja um erro relacionado a HeadObject ou. GetObjectTagging Por exemplo, aqui está um erro relacionado a GetObjectTagging:

```
[WARN] Failed to read metadata for file /picture1.png (versionId: 111111): S3 Get
Object Tagging Failed
[ERROR] S3 Exception: op=GetObjectTagging photos/picture1.png, code=403, type=15,
exception=AccessDenied,
msg=Access Denied req-hdrs: content-type=application/xml, x-amz-api-version=2006-03-01
rsp-hdrs: content-type=application/xml,
date=Wed, 07 Feb 2024 20:16:14 GMT, server=AmazonS3, transfer-encoding=chunked,
x-amz-id-2=IOWQ4fDEXAMPLEQM+ey7N9WgVhSnQ6JEXAMPLEZb7hSQDASK+Jd1vEXAMPLEa3Km, x-amz-
request-id=79104EXAMPLEB723
```

Se você ver algum desses erros, valide se a função do IAM DataSync usada para acessar seu local de origem do S3 tem as seguintes permissões:

- s3:GetObjectVersion
- s3:GetObjectVersionTagging

Se você precisar atualizar o perfil com essas permissões, consulte [Criação de uma função do IAM DataSync para acessar sua localização no Amazon S3](#).

Solução de problemas com DataSync tarefas

Use as informações a seguir para ajudá-lo a solucionar problemas com AWS DataSync tarefas e execuções de tarefas. Esses problemas podem incluir problemas de configuração de tarefas, execuções de tarefas paralisadas e dados não transferidos conforme o esperado.

Erro: SyncOption valor inválido. Opção:

TransferModePreserveDeletedFiles,, Valor: TUDO, REMOVER.

Esse erro ocorre quando você está criando ou editando sua DataSync tarefa e seleciona a opção Transferir todos os dados e desmarca a opção Manter arquivos excluídos.

Quando você transfere todos os dados, DataSync não escaneia sua localização de destino e não sabe o que excluir.

A execução da tarefa falha com um EniNotFound erro

Esse erro ocorre se você excluir uma das interfaces de rede da tarefa em sua nuvem privada virtual (VPC). Se sua tarefa estiver agendada ou em fila, ela falhará se não tiver uma [interface de rede necessária para transferir seus dados](#).

Medidas a serem tomadas

Você tem as seguintes opções para contornar esse problema:

- Reiniciar manualmente a tarefa. Ao fazer isso, DataSync criará todas as interfaces de rede ausentes necessárias para executar a tarefa.
- Se você precisar limpar recursos em sua VPC, certifique-se de não excluir interfaces de rede relacionadas a uma DataSync tarefa que você ainda está usando.

Para ver as interfaces de rede alocadas para a tarefa, siga um destes procedimentos:

- Use a operação [DescribeTask](#). Você pode visualizar as interfaces de rede nos elementos de resposta SourceNetworkInterfaceArns e DestinationNetworkInterfaceArns.
- No EC2 console da Amazon, pesquise seu ID de tarefa (comotask-f012345678abcdef0) para encontrar suas interfaces de rede.
- Considere não executar suas tarefas automaticamente. Isso pode incluir a desativação do enfileiramento ou agendamento de tarefas (por meio DataSync de automação personalizada).

A execução da tarefa falha com um erro Não é possível alocar memória

Quando sua DataSync tarefa falha com o erro Não é possível alocar memória, isso pode significar algumas coisas diferentes.

Ação a realizar

Tente o seguinte até que você não veja mais o problema:

- Se sua transferência envolver um agente, certifique-se de que o agente atenda aos requisitos da [máquina virtual \(VM\)](#) ou [da EC2 instância da Amazon](#).
- Divida sua transferência em várias tarefas usando [filtros](#). É possível que você esteja tentando transferir mais arquivos ou objetos do que [uma DataSync tarefa pode suportar](#).
- Se você ainda encontrar o problema, [entre em contato com o Suporte](#).

A execução da tarefa tem um status de lançamento, mas nada parece estar acontecendo

Sua DataSync tarefa pode ficar paralisada com o status de Inicialização, normalmente porque o agente está desligado ou perdeu a conectividade com a rede.

Ação a realizar

Certifique-se de que o status do seu agente esteja ONLINE. Se o agente estiver OFFLINE, certifique-se de ativá-lo.

Se o agente estiver ativado e a tarefa ainda estiver paralisada no status Iniciando, o mais provável é que haja um problema de conectividade de rede entre o agente e o AWS. Para obter informações sobre como testar a conectividade de rede, consulte [Verificando a conexão do seu agente com o serviço DataSync](#).

Se você ainda estiver com esse problema, consulte [Não sei o que está acontecendo com meu agente. Alguém pode me ajudar?](#).

A execução da tarefa parece paralisada no status de preparação

O tempo em que sua tarefa de DataSync transferência tem o status Preparando depende da quantidade de dados na origem e no destino da transferência e do desempenho desses sistemas de armazenamento.

Quando uma tarefa é iniciada, DataSync executa uma listagem recursiva de diretórios para descobrir todos os arquivos, objetos, diretórios e metadados em sua origem e destino. DataSync usa essas listas para identificar diferenças entre sistemas de armazenamento e determinar o que copiar. Esse processo pode levar alguns minutos ou até algumas horas.

Medida a ser tomada

Você não deveria ter que fazer nada. Continue aguardando até que o status da tarefa mude para Transferindo. Se o status ainda não mudar, entre em contato com a [Central AWS Support](#).

A execução da tarefa é interrompida antes que a transferência termine

Se a execução da DataSync tarefa for interrompida mais cedo, a configuração da tarefa poderá incluir uma Região da AWS que esteja desativada no seu Conta da AWS.

Medidas a serem tomadas

Faça o seguinte para executar a tarefa novamente:

1. Verifique o [status de adesão opcional](#) das regiões da tarefa e certifique-se de que estejam habilitadas.
2. [Inicie a tarefa](#) novamente.

A execução da tarefa falha ao transferir de um bucket do Google Cloud Storage

Como DataSync se comunica com o Google Cloud Storage usando a API Amazon S3, há uma limitação que pode fazer com que DataSync sua transferência falhe se você tentar copiar tags de objetos. A seguinte mensagem relacionada ao problema aparece em seus CloudWatch registros:

[AVISO] Falha ao ler os metadados do arquivo/*your-bucket/your-object*: Falha na marcação de objetos do S3: prosseguindo sem marcação

Para evitar isso, desmarque a opção Copiar tags de objeto ao definir as configurações da tarefa de transferência.

Há incompatibilidades entre os registros de data e hora da execução da tarefa

Ao examinar o DataSync console ou os CloudWatch registros da Amazon, você pode perceber que os horários de início e término da execução da DataSync tarefa não coincidem com os registros de data e hora que você vê em outras ferramentas de monitoramento. Isso ocorre porque o console e CloudWatch os registros levam em consideração o tempo gasto pela execução de uma tarefa nos [estados](#) de inicialização ou enfileiramento, enquanto outras ferramentas não.

Você pode notar essa discrepância ao comparar os timestamps de execução entre o DataSync console ou os CloudWatch registros e os seguintes locais:

- Registros do sistema de arquivos envolvido na sua transferência
- A data da última modificação em um objeto do Amazon S3 que DataSync foi gravado em
- Tráfego de rede DataSync proveniente do agente
- EventBridge Eventos da Amazon

A execução da tarefa falha com **NoMem** erro

O conjunto de dados que você está tentando transferir pode ser muito grande DataSync. Se você receber esse erro, entre em contato com o [AWS Support Center](#).

Falha na transferência do objeto para Azure Blob Storage com **user metadata key** erro

Ao transferir de um bucket S3 para Azure Blob Storage, você pode ver o seguinte erro:

```
[ERROR] Failed to transfer file /user-metadata/file1: Azure Blob user metadata key must be a CSharp identifier
```

Isso significa que */user-metadata/file1* inclui metadados do usuário que não usam um identificador C# válido. Para obter mais informações, consulte a [Documentação da Microsoft](#).

Há uma **/.aws-datasync** pasta no local de destino

DataSync cria uma pasta chamada **/.aws-datasync** em seu local de destino para ajudar a facilitar a transferência de dados.

Embora DataSync normalmente exclua essa pasta após a transferência, pode haver situações em que isso não aconteça.

Ação a realizar

Exclua essa pasta a qualquer momento, desde que você não tenha uma tarefa em execução copiando para esse local.

Não é possível transferir links simbólicos entre locais usando SMB

Quando a execução da tarefa for concluída, você verá o seguinte erro:

```
Transfer and verification completed. Selected files transferred except for files
skipped due to errors. If no skipped files are listed in Cloud Watch Logs, please
contact AWS Support for further assistance.
```

Ao transferir entre sistemas de armazenamento SMB (como um servidor de arquivos SMB e o sistema de arquivos Amazon FSx para Windows File Server), você pode ver os seguintes avisos e erros em seus registros: CloudWatch

```
[WARN] Failed to read metadata for file /appraiser/symlink: No data available
[ERROR] Failed to read metadata for directory /appraiser/symlink: No data available
```

Ação a realizar

DataSync não suporta a transferência de links simbólicos (ou links físicos) ao transferir entre esses tipos de localização. Para obter mais informações, consulte [Links e diretórios copiados pelo AWS DataSync](#).

Erros do relatório de tarefas

Você pode se deparar com um dos seguintes erros ao tentar monitorar sua DataSync transferência com um relatório de tarefas.

Mensagem de erro	Solução temporária
O caminho do arquivo excede o comprimento máximo de 4.096 caracteres. Não é possível gravar no relatório de tarefas	N/A (não é DataSync possível transferir um arquivo com um caminho que exceda 4.096 bytes)

Mensagem de erro	Solução temporária
	Para obter mais informações, consulte Limites do sistema de armazenamento, arquivos e objetos .
Falha no upload do(s) relatório(s) de tarefas para o S3 devido a um bucket ou perfil do IAM inválidos	Verifique se a função DataSync do IAM tem as permissões corretas para carregar um relatório de tarefas no seu bucket do S3.
Ocorreu um erro de execução antes da geração de qualquer relatório de tarefas	Verifique seus CloudWatch registros para identificar por que a execução da tarefa falhou.

Solução de problemas de verificação de dados

Por padrão, AWS DataSync [verifica a integridade](#) dos seus dados ao final de uma transferência. Use as informações a seguir para ajudá-lo a diagnosticar erros e avisos comuns de verificação, como arquivos sendo modificados ou excluídos antes de DataSync concluir a verificação dos dados.

Com problemas de verificação, muitas vezes é útil revisar seus [CloudWatch registros](#) (ou [relatórios de tarefas](#)), além do erro de execução da tarefa que você está vendo. DataSync fornece registros estruturados em JSON para tarefas do modo Avançado, enquanto as tarefas do modo Básico têm registros não estruturados.

Há incompatibilidades entre o conteúdo de um arquivo

Quando a execução da tarefa for concluída, você verá o seguinte erro:

```
Transfer and verification completed. Verification detected mismatches. Files with mismatches are listed in Cloud Watch Logs
```

Em seus CloudWatch registros, você pode notar falhas nas verificações de conteúdos que diferem entre os locais de origem e de destino. Isso pode acontecer se os arquivos forem modificados durante a transferência.

Por exemplo, os registros a seguir mostram que `file1.txt` tem `dstHash` valores de `mtimesrcHash`, e diferentes:

Exemplo de registro do modo básico

```
[NOTICE] Verification failed <> /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt  srcMeta: type=R mode=0755 uid=65534
gid=65534 size=534528 atime=1633100003/684349800 mtime=1602647222/222919600
extAttrsHash=0
[NOTICE]  srcHash: 0c506c26bd1e43bd3ac346734f1a9c16c4ad100d1b43c2903772ca894fd24e44
[NOTICE] /directory1/directory2/file1.txt  dstMeta: type=R mode=0755 uid=65534
gid=65534 size=511001 atime=1633100003/684349800 mtime=1633106855/859227500
extAttrsHash=0
[NOTICE]  dstHash: dbd798929f11a7c0201e97f7a61191a83b4e010a449dfc79fbb8233801067c46
```

Em DataSync, `mtime` representa a última vez em que um arquivo foi gravado antes da [preparação](#). Ao verificar as transferências, DataSync compara `mtime` os valores entre os locais de origem e destino. Uma falha de verificação como essa ocorre se o `mtime` arquivo não for o mesmo para os dois locais. As diferenças entre `srcHash` e `dstHash` indicam que o conteúdo do arquivo não coincidem nos dois locais.

Medidas a serem tomadas

Faça o seguinte:

1. Use um conversor de época para determinar se o arquivo ou objeto de origem ou destino foi modificado mais recentemente. Isso pode ajudar a identificar qual versão é atual.
2. Para evitar esse erro novamente, [agende sua tarefa](#) para ser executada durante uma janela de manutenção quando não houver atividade na origem e no destino.

Há uma incompatibilidade entre os metadados SMB de um arquivo

Quando a execução da tarefa for concluída, você verá o seguinte erro:

```
Transfer and verification completed. Verification detected mismatches. Files with
mismatches are listed in Cloud Watch Logs
```

Ao transferir entre sistemas de armazenamento que suportam o protocolo Server Message Block (SMB), você pode ver esse erro quando os atributos SMB estendidos de um arquivo não coincidem entre origem e destino.

Por exemplo, os registros a seguir mostram que `file1.txt` tem um `extAttrHash` valor diferente entre os locais, indicando que o conteúdo do arquivo é idêntico, mas os atributos estendidos não foram definidos no destino:

Exemplo de registro do modo básico

```
[NOTICE] Verification failed <> /directory1/directory2/file1.txt
[NOTICE] /directory1/directory2/file1.txt   srcMeta: type=R mode=0755 uid=65534
gid=65534 size=1469752 atime=1631354985/174924200 mtime=1536995541/986211400
extAttrHash=2272191894
[NOTICE]   srcHash: 38571d42b646ac8f4034b7518636b37dd0899c6fc03cdaa8369be6e81a1a2bb5
[NOTICE] /directory1/directory2/file1.txt   dstMeta: type=R mode=0755 uid=65534
gid=65534 size=1469752 atime=1631354985/174924200 mtime=1536995541/986211400
extAttrHash=3051150340
[NOTICE]   dstHash: 38571d42b646ac8f4034b7518636b37dd0899c6fc03cdaa8369be6e81a1a2bb5
```

Você também pode ver uma mensagem de erro relacionada sobre atributos estendidos:

```
[ERROR] Deferred error: WriteFileExtAttr2 failed to setextattrlist(filename="/
directory1/directory2/file1.txt"): Input/output error
```

Ação a realizar

Esse erro geralmente ocorre quando não há permissões suficientes para copiar listas de controle de acesso (ACLs) para o destino. Para resolver esse problema, consulte os seguintes guias de configuração com base no seu tipo de destino:

- [Permissões necessárias](#) FSx para sistemas de arquivos do Windows File Server
- [Permissões necessárias](#) FSx para sistemas de arquivos ONTAP que usam SMB

Os arquivos a serem transferidos não estão mais no local de origem

Quando a execução da tarefa for concluída, você verá o seguinte erro:

```
Transfer and verification completed. Selected files transferred except for files
skipped due to errors. If no skipped files are listed in Cloud Watch Logs, please
contact AWS Support for further assistance.
```

Em seus registros, você pode ver erros indicando que os arquivos não estão no local de origem. Isso pode acontecer se os arquivos (como `file1.dll` e `file2.dll`) forem excluídos após a [preparação](#), mas antes de DataSync transferi-los:

Exemplo de registro do modo básico

```
[ERROR] Failed to open source file /file1.dll: No such file or directory
[ERROR] Failed to open source file /file2.dll: No such file or directory
```

Ação a realizar

Para evitar essas situações, [programe sua tarefa](#) para ser executada quando não houver atividade no local de origem.

Por exemplo, você pode executar sua tarefa durante uma janela de manutenção quando os usuários e aplicativos não estão trabalhando ativamente com esse local.

Em alguns casos, talvez você não veja os registros associados a esse erro. Se isso acontecer, entre em contato com a [AWS Support Central de](#) contatos.

DataSync não é possível verificar os dados de destino

Quando a execução da tarefa for concluída, você verá o seguinte erro:

```
Transfer and verification completed. Verification detected mismatches. Files with
mismatches are listed in Cloud Watch Logs
```

Em seus registros, você pode perceber que não é DataSync possível verificar determinadas pastas ou arquivos no local de destino. Esses erros podem ter a seguinte aparência:

Exemplo de registro do modo básico

```
[ERROR] Failed to read metadata for destination file /directory1/directory2/
file1.txt: No such file or directory
```

Para arquivos, você pode ver falhas de verificação como estas:

Exemplo de registro do modo básico

[illegible]

Ação a realizar

Esses registros indicam que os dados de destino foram excluídos após a transferência, mas antes da verificação. (Os registros parecem semelhantes quando os dados são enviados para um local de origem durante o mesmo período.)

Para evitar essas situações, [programe sua tarefa](#) para ser executada quando não houver atividade no local de destino.

Por exemplo, você pode executar sua tarefa durante uma janela de manutenção quando os usuários e aplicativos não estão trabalhando ativamente com esse local.

DataSync não consigo ler os metadados do objeto

Quando a execução da tarefa for concluída, você verá o seguinte erro:

Transfer and verification completed. Selected files transferred except for files skipped due to errors. If no skipped files are listed in Cloud Watch Logs, please contact AWS Support for further assistance.

Em seus registros, você pode notar que não DataSync consegue ler `file1.png` devido a uma falha na solicitação do `Amazon S3HeadObject`. [DataSync faz HeadObject solicitações](#) com os locais do S3 durante a preparação e verificação da tarefa.

Exemplo de registro do modo básico

```
[WARN] Failed to read metadata for file /file1.png: S3 Head Object Failed
```

Medidas a serem tomadas

Para corrigir esse problema, verifique se DataSync tem o nível certo de permissões para trabalhar com seu bucket do S3:

- Certifique-se de que a função do IAM DataSync usada para acessar seus locais do Amazon S3 permita a `s3:GetObject` permissão. Para obter mais informações, consulte [Permissões obrigatórias](#).
- Se seu bucket do S3 usa criptografia do lado do servidor, verifique se ele DataSync tem permissão para acessar os objetos nesse bucket. Para obter mais informações, consulte [Acessar buckets do S3 usando criptografia no lado do servidor](#).

Há uma incompatibilidade nos metadados definidos pelo sistema de um objeto

Quando a execução da tarefa no modo Avançado entre buckets do S3 terminar, você verá o seguinte erro:

```
Verification failed due to a difference in metadata
```

Você pode notar em seus registros uma incompatibilidade nos metadados definidos pelo sistema Amazon [S3](#) de um objeto. Neste exemplo específico, o objeto de origem não tem Content-Type metadados, mas o objeto de destino tem. Isso aconteceu porque o bucket do S3 de destino aplicou automaticamente `"ContentType": "application/octet-stream"` os metadados ao objeto quando o DataSync transferiu para lá.

Exemplo de registro do modo aprimorado

```
{
  "Action": "VERIFY",
  "Source": {
    "LocationId": "loc-0b3017fc4ba4a2d8d",
    "RelativePath": "encoding/content-null",
    "Metadata": {
      "Type": "Object",
      "ContentSize": 24,
      "LastModified": "2024-12-23T15:48:15Z",
      "S3": {
        "SystemMetadata": {
          "ETag": "\"68b9c323bb846841ee491481f576ed4a\""
        }
      }
    }
  }
}
```

```

        "UserMetadata": {},
        "Tags": {}
    }
},
"Destination": {
    "LocationId": "loc-abcdef01234567890",
    "RelativePath": "encoding/content-null",
    "Metadata": {
        "Type": "Object",
        "ContentSize": 24,
        "LastModified": "2024-12-23T16:00:03Z",
        "S3": {
            "SystemMetadata": {
                "ContentType": "application/octet-stream",
                "ETag": "\"68b9c323bb846841ee491481f576ed4a\""
            },
            "UserMetadata": {
                "file-mtime": "1734968895000"
            },
            "Tags": {}
        }
    }
},
"TransferType": "CONTENT_AND_METADATA",
"ErrorCode": "MetadataDiffers",
"ErrorDetail": "Verification failed due to a difference in metadata"
}

```

Ação a realizar

Para evitar esse erro, atualize seus objetos de localização de origem para incluir a propriedade de Content-Type metadados.

Entendendo a duração da verificação de dados

DataSync a verificação inclui uma SHA256 soma de verificação do conteúdo do arquivo e uma comparação exata dos metadados do arquivo entre os locais. A duração da verificação depende de vários fatores, incluindo o número de arquivos ou objetos envolvidos, o tamanho dos dados nos sistemas de armazenamento e o desempenho desses sistemas.

Ação a realizar

Considerando os fatores que podem afetar o tempo de verificação, você não precisa fazer nada. No entanto, se a execução da sua tarefa parecer paralisada em um status de [verificação](#), entre em contato com a [AWS Support Central](#) de contatos.

Solução de problemas de custos de armazenamento S3 acima do esperado com DataSync

Se os custos de armazenamento do Amazon S3 forem maiores do que você imaginava após uma transferência AWS DataSync, isso pode ser devido a um ou mais dos seguintes motivos:

- Ao transferir de ou para buckets do S3, você incorre em custos relacionados às solicitações de API do S3 feitas por DataSync
- DataSync usa o recurso de upload de várias partes do Amazon S3 para fazer upload de objetos para buckets do S3. Isso pode resultar em cobranças de armazenamento inesperadas para uploads que não são concluídos com êxito.
- O versionamento de objetos pode estar ativado no bucket do S3. O versionamento de objetos faz com que o Amazon S3 armazene várias cópias de objetos com o mesmo nome.

Medidas a serem tomadas

Nesses casos, você pode executar as seguintes etapas:

- Certifique-se de entender como DataSync usa as solicitações do S3 e como elas podem estar afetando seus custos de armazenamento. Para obter mais informações, consulte [Avaliando os custos de solicitação do S3 ao usar DataSync](#).
- Se o problema estiver relacionado a uploads fracionados, configure uma política de uploads fracionados para o bucket do S3 para limpar uploads fracionados incompletos para reduzir o custo de armazenamento. Para obter mais informações, consulte a postagem do AWS blog [S3 Lifecycle Management Update - Support for Multipart Uploads](#) and Delete Markers.
- Se o problema estiver relacionado ao versionamento de objetos, desative o versionamento de objetos em seu bucket do S3.
- Se precisar de mais ajuda, entre em contato com a [Central AWS Support](#).

AWS DataSync tutoriais

Esses tutoriais orientam você em alguns cenários do mundo real com AWS DataSync.

Tópicos

- [Tutorial: Transferindo dados do armazenamento local para o Amazon S3 em todo Contas da AWS](#)
- [Tutorial: Transferência de dados entre buckets do Amazon S3 entre Contas da AWS](#)

Tutorial: Transferindo dados do armazenamento local para o Amazon S3 em todo Contas da AWS

Ao usar AWS DataSync com armazenamento local, você normalmente transfere dados para um serviço AWS de armazenamento que pertence ao Conta da AWS mesmo que seu DataSync agente. No entanto, há situações em que talvez seja necessário transferir dados para um bucket do Amazon S3 associado a uma conta diferente.

Important

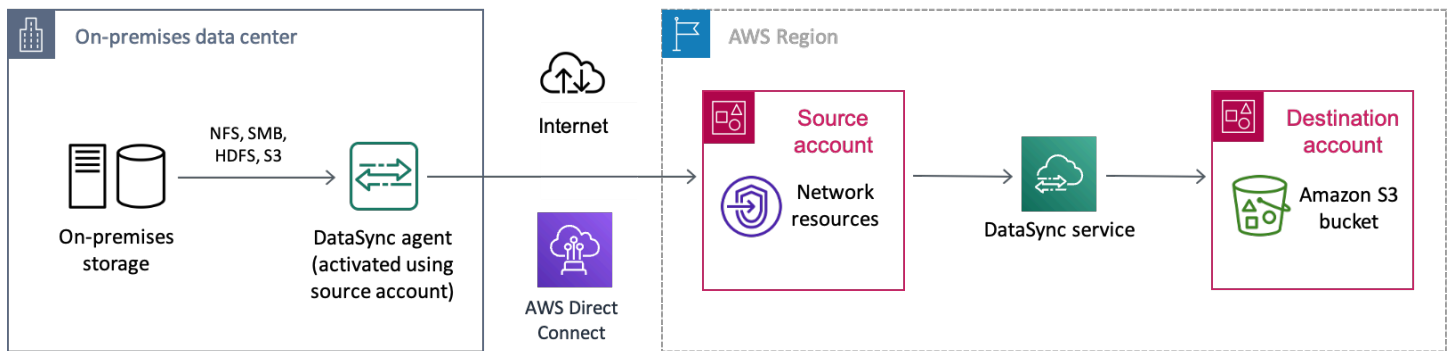
A transferência de dados Contas da AWS usando os métodos deste tutorial funciona somente quando o Amazon S3 é um dos locais de DataSync transferência.

Visão geral

Não é incomum precisar transferir dados entre diferentes Contas da AWS, especialmente se você tiver equipes separadas gerenciando os recursos da sua organização. Veja como DataSync pode ser uma transferência entre contas:

- Conta de origem: A Conta da AWS para gerenciar recursos de rede. Essa é a conta com a qual você ativa seu DataSync agente.
- Conta de destino: a Conta da AWS para gerenciar o bucket do S3 para o qual você precisa transferir dados.

O diagrama a seguir ilustra esse tipo de cenário.



Pré-requisito: permissões necessárias na conta de origem

Para sua fonte Conta da AWS, há dois conjuntos de permissões a serem considerados com esse tipo de transferência entre contas:

- Permissões de usuário que permitem que um usuário trabalhe com DataSync (pode ser você ou seu administrador de armazenamento). Essas permissões permitem criar DataSync locais e tarefas.
- DataSync permissões de serviço que permitem DataSync transferir dados para o bucket da sua conta de destino.

User permissions

Na sua conta de origem, adicione pelo menos as seguintes permissões a uma função do IAM para criar seus DataSync locais e tarefas. Para obter informações sobre como adicionar permissões a um perfil, consulte [criação](#) ou [modificação](#) de um perfil do IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SourceUserRolePermissions",
      "Effect": "Allow",
      "Action": [
        "datasync:CreateLocationS3",
        "datasync:CreateTask",
        "datasync:DescribeLocation*",
        "datasync:DescribeTaskExecution",
        "datasync:ListLocations",
        "datasync:ListTaskExecutions",
```

```

        "datasync:DescribeTask",
        "datasync:CancelTaskExecution",
        "datasync:ListTasks",
        "datasync:StartTaskExecution",
        "iam:CreateRole",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "datasync.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Tip

Para configurar suas permissões de usuário, considere usar [AWSDataSyncFullAccess](#). Essa é uma política AWS gerenciada que fornece ao usuário acesso total DataSync e acesso mínimo às suas dependências.

DataSync service permissions

O DataSync serviço precisa das seguintes permissões em sua conta de origem para transferir dados para o bucket da conta de destino.

Posteriormente neste tutorial, você adiciona essas permissões ao [criar uma função do IAM](#) para DataSync. Você também especifica essa função (*source-datasync-role*) em sua [política de bucket de destino](#) e ao [criar seu local de DataSync destino](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
}
```

Pré-requisito: permissões necessárias na conta de destino

Na sua conta de destino, suas permissões de usuário devem permitir que você atualize a política do bucket de destino e desative suas listas de controle de acesso (ACLs). Para obter mais informações sobre essas permissões específicas, consulte o [Guia de usuário do Amazon S3](#).

Etapa 1: na sua conta de origem, crie um DataSync agente

Para começar, você deve criar um DataSync agente que possa ler do seu sistema de armazenamento local e se comunicar com o DataSync serviço. Esse processo inclui a implantação de um agente no ambiente de armazenamento on-premises e a ativação do agente na Conta da AWS fonte.

Note

As etapas deste tutorial se aplicam a qualquer tipo de agente e endpoint de serviço que você usa.

Para criar um DataSync agente

1. [Implante um DataSync agente](#) em seu ambiente de armazenamento local.
2. [Escolha um endpoint de serviço](#) que o agente usará para se comunicar AWS.
3. [Ative seu agente](#) na sua conta de origem.

Etapa 2: na sua conta de origem, crie uma função DataSync do IAM para acesso ao bucket de destino

Na sua conta de origem, você precisa de uma função do IAM que dê DataSync as permissões para transferir dados para o bucket da sua conta de destino.

Como você está transferindo entre contas, você deve criar a função manualmente. (DataSync pode criar essa função para você no console ao transferir para a mesma conta.)

Crie a DataSync função do IAM

Crie uma função do IAM DataSync como entidade confiável.

Para criar perfil do IAM

1. Faça login no AWS Management Console com sua conta de origem.
2. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
3. No painel de navegação esquerdo, em Gerenciamento de acesso, escolha Perfis e, em seguida, escolha Criar perfil.

4. Na página Selecionar entidade confiável, para Tipo de entidade confiável, escolha AWS service (Serviço da AWS).
5. Em Caso de uso, escolha DataSyncna lista suspensa e selecione. DataSync Escolha Próximo.
6. Na página Adicionar permissões, escolha Próximo.
7. Forneça um nome ao perfil e escolha Criar perfil.

Para obter mais informações, consulte [Criação de uma função para um AWS service \(Serviço da AWS\) \(console\)](#) no Guia do usuário do IAM.

Adicionar permissões à função do DataSync IAM

A função do IAM que você acabou de criar precisa das permissões que permitem DataSync transferir dados para o bucket do S3 na sua conta de destino.

Para adicionar permissões ao perfil do IAM

1. Na página Perfis do console do IAM, procure o perfil que você acabou de criar e escolha seu nome.
2. Na página do perfil, escolha a guia Permissões. Selecione Adicionar permissões e, em seguida, Criar política em linha.
3. Selecione a guia JSON e faça o seguinte:
 - a. Cole o JSON a seguir no editor de política:

Note

O valor de `aws:ResourceAccount` deve ser o ID da conta que possui o bucket do Amazon S3 especificado na política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ]
    }
  ]
}
```

```

    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "123456789012"
    }
  }
},
{
  "Action": [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:GetObject",
    "s3:GetObjectTagging",
    "s3:GetObjectVersion",
    "s3:GetObjectVersionTagging",
    "s3:ListMultipartUploadParts",
    "s3:PutObject",
    "s3:PutObjectTagging"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
  "Condition": {
    "StringEquals": {
      "aws:ResourceAccount": "123456789012"
    }
  }
}
]
}

```

- b. Substitua cada instância do *amzn-s3-demo-destination-bucket* pelo nome do bucket do S3 em sua conta de destino.
4. Escolha Próximo. Digite um nome para a política e escolha Criar política.

Etapa 3: na conta de destino, atualize a política do bucket do S3

Na sua conta de destino, modifique a política de bucket do S3 de destino para incluir a [função DataSync do IAM](#) que você criou na sua conta de origem.

Antes de começar: certifique-se de que tem as [permissões necessárias para conta de destino](#).

Para atualizar a política de bucket do S3 de destino

1. No AWS Management Console, mude para sua conta de destino.
2. Abra o console do Amazon S3 em <https://console.aws.amazon.com/s3/>.
3. No painel de navegação à esquerda, escolha Buckets.
4. Na lista Buckets, escolha o bucket do S3 para o qual você está transferindo dados.
5. Na página do perfil, escolha a guia Permissões.
6. Em Política de bucket, escolha Editar e faça o seguinte para modificar sua política de bucket do S3:
 - a. Atualize o que está no editor para incluir as seguintes declarações de política:

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source-account:role/source-datasync-role"
      },
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

- b. Substitua cada instância *source-account* de pelo ID Conta da AWS da sua conta de origem.
 - c. *source-datasync-role* Substitua pela [função do IAM que você criou DataSync na sua conta de origem](#).
 - d. Substitua cada instância do *amzn-s3-demo-destination-bucket* pelo nome do bucket do S3 em sua conta de destino.
7. Escolha Salvar alterações.

Etapa 4: na sua conta de destino, desative ACLs o bucket do S3

É importante que todos os dados que você copia para o bucket do S3 pertençam à conta de destino. Para garantir que essa conta possua os dados, desative as listas de controle de acesso (ACLs) do bucket. Para obter mais informações, consulte [Controle da propriedade de objetos e desativação ACLs do seu bucket no Guia](#) do usuário do Amazon S3.

Para desativar ACLs para seu bucket de destino

1. Enquanto ainda estiver conectado ao console do S3 com sua conta de destino, escolha o bucket do S3 para o qual você está transferindo dados.
2. Na página do perfil, escolha a guia Permissões.
3. Em Object Ownership, escolha Editar.
4. Se ainda não estiver selecionada, escolha a opção ACLs desativada (recomendada).
5. Escolha Salvar alterações.

Etapa 5: na sua conta de origem, crie um local de DataSync origem para seu armazenamento local

Na sua conta de origem, crie um [local de DataSync origem](#) para o sistema de armazenamento local do qual você está transferindo dados. Esse local deve usar o [agente que você acabou de ativar](#) na conta de origem.

Etapa 6: na sua conta de origem, crie um local de DataSync destino para seu bucket do S3

Ainda na conta de origem, crie um local para o bucket do S3 para o qual você está transferindo dados.

Antes de começar: certifique-se de que tem as [permissões necessárias para conta de origem](#).

Como você não pode criar locais entre contas usando a interface do DataSync console, essas instruções exigem que você execute um `create-location-s3` comando para criar seu local de destino. Recomendamos executar o comando usando AWS CloudShell um shell pré-autenticado baseado em navegador que você inicia diretamente do console. CloudShell permite que você execute AWS CLI comandos `create-location-s3` sem baixar ou instalar ferramentas de linha de comando.

Note

Para concluir as etapas a seguir usando uma ferramenta de linha de comando diferente de CloudShell, certifique-se de que seu [AWS CLI perfil](#) use a mesma função do IAM que inclui as [permissões de usuário necessárias](#) para uso DataSync em sua conta de origem.

Para criar um local de DataSync destino usando CloudShell

1. Enquanto ainda estiver na sua conta de origem, faça o seguinte para iniciar a CloudShell partir do console:
 - Escolha o CloudShell ícone na barra de navegação do console. Ele está à direita da caixa de pesquisa.
 - Use a caixa de pesquisa na barra de navegação do console para pesquisar CloudShelle, em seguida, escolha a CloudShellopção.
2. Copie o seguinte comando:

```
aws datasync create-location-s3 \  
  --s3-bucket-arn arn:aws:s3:::amzn-s3-demo-destination-bucket \  
  --s3-config '{  
    "BucketAccessRoleArn":"arn:aws:iam::source-user-account:role/source-datasync-  
role"
```

```
}'
```

3. Substitua *amzn-s3-demo-destination-bucket* pelo nome de bucket S3 em sua conta de destino.
4. Substitua *source-user-account* pelo ID Conta da AWS da sua conta de origem.
5. *source-datasync-role* Substitua pela [função DataSync do IAM](#) que você criou na sua conta de origem.
6. Execute o comando em CloudShell.

Se o comando retornar um ARN de DataSync localização semelhante a este, você criou o local com sucesso:

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
abcdef01234567890"
}
```

7. No painel de navegação esquerdo, expanda Transferência de dados e, em seguida, escolha Locais.

Na conta de origem, você pode ver o local do bucket do S3 que acabou de criar para o bucket da conta de destino.

Etapa 7: na sua conta de origem, crie e inicie sua DataSync tarefa

Antes de iniciar uma DataSync tarefa para transferir seus dados, vamos recapitular o que você fez até agora:

- Na sua conta de origem, você criou seu DataSync agente. O agente pode ler do seu sistema de armazenamento local e se comunicar com o DataSync serviço.
- Na sua conta de origem, você criou uma função do IAM que permite DataSync transferir dados para o bucket do S3 na sua conta de destino.
- Na sua conta de destino, você configurou seu bucket do S3 para DataSync poder transferir dados para ele.
- Na sua conta de origem, você criou os locais de DataSync origem e destino para sua transferência.

Para criar e iniciar a DataSync tarefa

1. Enquanto ainda estiver usando o DataSync console em sua conta de origem, expanda Transferência de dados no painel de navegação esquerdo e escolha Tarefas e Criar tarefa.
2. Na página Configurar local de origem, selecione Escolher local existente. Escolha o local de origem do qual você está copiando os dados (seu armazenamento on-premises) e, em seguida, Próximo.
3. Na página Configurar local de destino, escolha Escolher um local existente. Escolha o local de destino para o qual você está copiando os dados (o bucket S3 na conta de destino) e, em seguida, Próximo.
4. Na página Definir configurações, dê um nome à tarefa. Conforme necessário, defina configurações adicionais, como especificar um grupo de CloudWatch logs da Amazon. Escolha Próximo.
5. Na página Revisão, revise suas configurações e selecione Criar tarefa.
6. Na página de detalhes da tarefa, escolha Iniciar e, em seguida, escolha uma das seguintes opções:
 - Para executar a tarefa sem modificação, escolha Iniciar com padrões.
 - Para modificar a tarefa antes de executá-la, escolha Iniciar com opções de substituição.

Quando sua tarefa terminar, verifique o bucket do S3 na sua conta de destino. Você deve ver os dados que foram movidos do local de origem.

Recursos relacionados

Para obter mais informações sobre o que você fez neste tutorial, consulte os seguintes tópicos:

- [Criando uma função para um AWS service \(Serviço da AWS\) \(console\)](#)
- [Modificar a política de confiança de um perfil \(console\)](#)
- [Adição de uma política de bucket usando o console do Amazon S3](#)
- [Crie um local S3 com o AWS CLI](#)

Tutorial: Transferência de dados entre buckets do Amazon S3 entre Contas da AWS

Com AWS DataSync, você pode transferir dados entre buckets do Amazon S3 que pertencem a diferentes. Contas da AWS

Important

A transferência de dados Contas da AWS usando os métodos deste tutorial funciona somente com o Amazon S3. Além disso, este tutorial pode ajudar você a transferir dados entre buckets do S3 que também estão em diferentes Regiões da AWS.

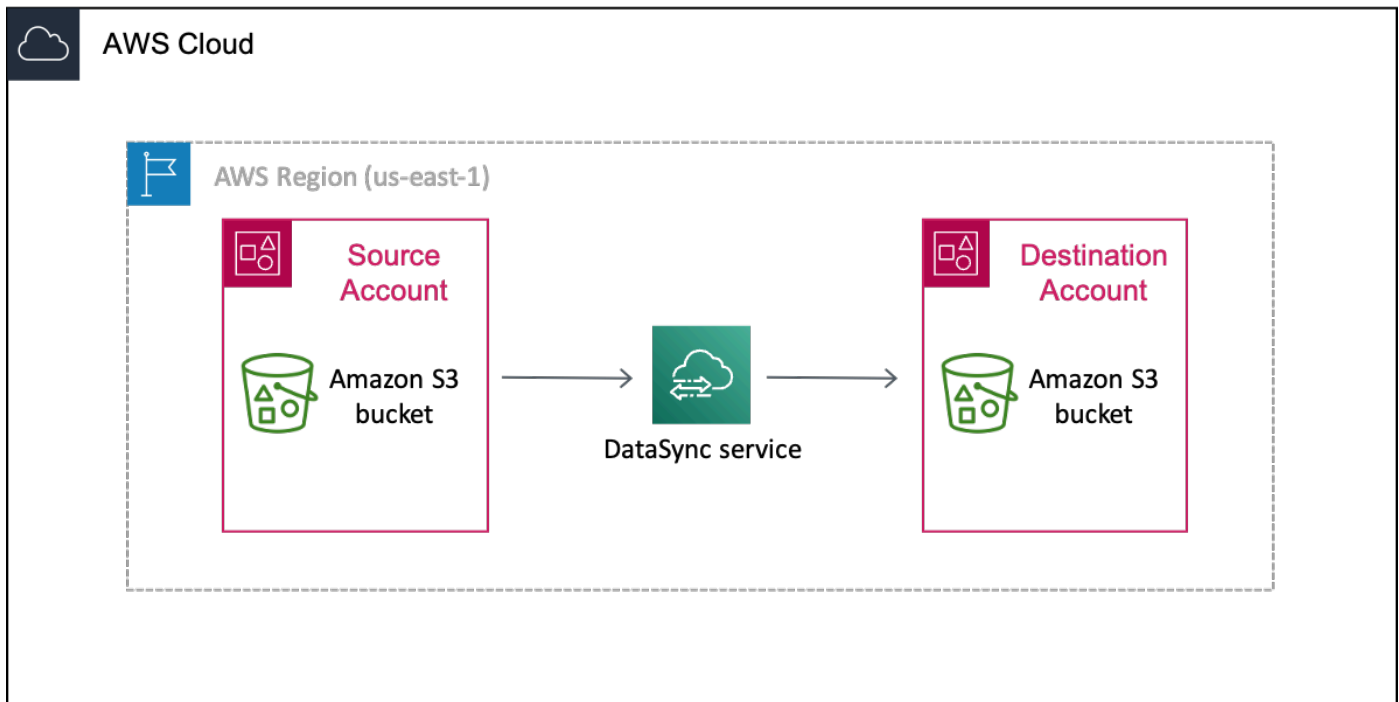
Visão geral

Não é incomum transferir dados entre eles Contas da AWS, especialmente se você tiver equipes separadas gerenciando os recursos da sua organização. Veja como DataSync pode ser uma transferência entre contas:

- Conta de origem: a Conta da AWS para gerenciar o bucket do S3 do qual você precisa transferir dados.
- Conta de destino: a Conta da AWS para gerenciar o bucket do S3 para o qual você precisa transferir dados.

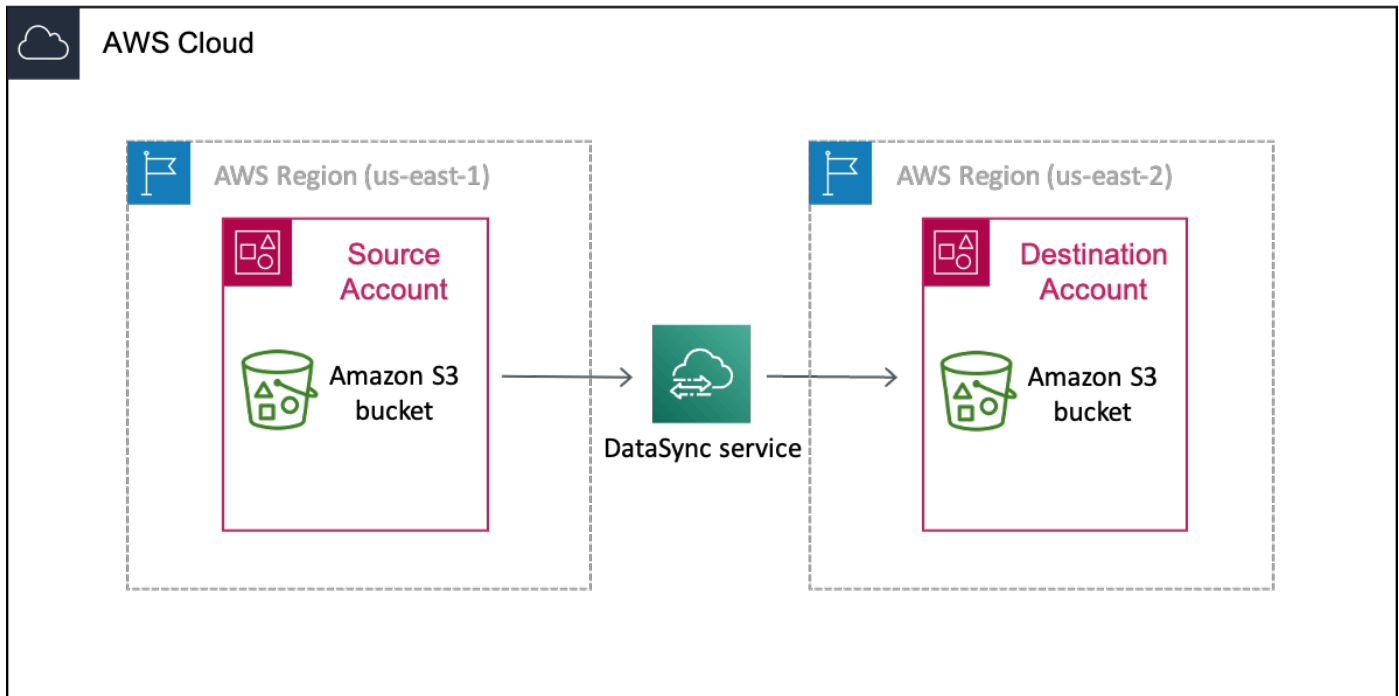
Transfers across accounts

O diagrama a seguir ilustra um cenário em que você transfere dados de um bucket do S3 para outro bucket do S3 que está em outro Conta da AWS.



Transfers across accounts and Regions

O diagrama a seguir ilustra um cenário em que você transfere dados de um bucket do S3 para outro bucket do S3 que está em uma região diferente Conta da AWS .



Pré-requisito: permissões necessárias na conta de origem

Para sua fonte Conta da AWS, há dois conjuntos de permissões a serem considerados com esse tipo de transferência entre contas:

- Permissões de usuário que permitem que um usuário trabalhe com DataSync (pode ser você ou seu administrador de armazenamento). Essas permissões permitem criar DataSync locais e tarefas.
- DataSync permissões de serviço que permitem DataSync transferir dados para o bucket da sua conta de destino.

Permissões do usuário para a conta de origem

Na sua conta de origem, adicione pelo menos as seguintes permissões a uma função do IAM para criar seus DataSync locais e tarefas. Para obter informações sobre como adicionar permissões a um perfil, consulte [criação](#) ou [modificação](#) de um perfil do IAM.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SourceUserRolePermissions",
      "Effect": "Allow",
      "Action": [
        "datasync:CreateLocationS3",
        "datasync:CreateTask",
        "datasync:DescribeLocation*",
        "datasync:DescribeTaskExecution",
        "datasync:ListLocations",
        "datasync:ListTaskExecutions",
        "datasync:DescribeTask",
        "datasync:CancelTaskExecution",
        "datasync:ListTasks",
        "datasync:StartTaskExecution",
        "iam:CreateRole",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
```

```
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "datasync.amazonaws.com"
        ]
      }
    }
  }
]
```

i Tip

Para configurar suas permissões de usuário, considere usar [AWSDataSyncFullAccess](#). Essa é uma política AWS gerenciada que fornece ao usuário acesso total DataSync e acesso mínimo às suas dependências.

DataSync permissões de serviço para sua conta de origem

O DataSync serviço precisa das seguintes permissões em sua conta de origem para transferir dados para o bucket da conta de destino.

Posteriormente neste tutorial, você adiciona essas permissões ao [criar uma função do IAM](#) para DataSync. Você também especifica essa função (*source-datasync-role*) em sua [política de bucket de destino](#) e ao [criar seu local de DataSync destino](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
}
```

Pré-requisito: permissões necessárias na conta de destino

Na sua conta de destino, suas permissões de usuário devem permitir que você atualize a política do bucket de destino e desative suas listas de controle de acesso (ACLs). Para obter mais informações sobre essas permissões específicas, consulte o [Guia de usuário do Amazon S3](#).

Etapa 1: na sua conta de origem, crie uma função DataSync do IAM para acesso ao bucket de destino

Na sua fonte Conta da AWS, você precisa de uma função do IAM que dê DataSync as permissões para transferir dados para o bucket da sua conta de destino.

Como você está transferindo entre contas, você deve criar a função manualmente. (DataSync pode criar essa função para você no console ao transferir para a mesma conta.)

Crie a DataSync função do IAM

Crie uma função do IAM DataSync como entidade confiável.

1. Faça login no AWS Management Console com sua conta de origem.
2. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
3. No painel de navegação esquerdo, em Gerenciamento de acesso, escolha Perfis e, em seguida, escolha Criar perfil.
4. Na página Selecionar entidade confiável, para Tipo de entidade confiável, escolha AWS service (Serviço da AWS).
5. Em Caso de uso, escolha DataSync na lista suspensa e selecione. DataSync Escolha Próximo.
6. Na página Adicionar permissões, escolha Próximo.
7. Forneça um nome ao perfil e escolha Criar perfil.

Para obter mais informações, consulte [Criação de uma função para um AWS service \(Serviço da AWS\) \(console\)](#) no Guia do usuário do IAM.

Adicionar permissões à função do DataSync IAM

A função do IAM que você acabou de criar precisa das permissões que permitem DataSync transferir dados para o bucket do S3 na sua conta de destino.

1. Na página Funções, escolha o nome do perfil que você acabou de criar.
2. Na página do perfil, escolha a guia Permissões. Selecione Adicionar permissões e, em seguida, Criar política em linha.
3. Selecione a guia JSON e faça o seguinte:
 - a. Cole o JSON a seguir no editor de política:

 Note

O valor de `aws:ResourceAccount` deve ser o ID da conta que possui o bucket do Amazon S3 especificado na política.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectTagging"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
      "Condition": {
        "StringEquals": {
```

```

    "aws:ResourceAccount": "123456789012"
  }
}
]
}

```

- b. Substitua cada instância do *amzn-s3-demo-destination-bucket* pelo nome do bucket do S3 em sua conta de destino.
4. Escolha Próximo. Digite um nome para a política e escolha Criar política.

Etapa 2: na conta de destino, atualize a política do bucket do S3

Na sua conta de destino, modifique a política de bucket do S3 de destino para incluir a [função DataSync do IAM](#) que você criou na sua conta de origem.

Antes de começar: certifique-se de que tem as [permissões necessárias para conta de destino](#).

Atualizar a política de bucket do S3 de destino

1. No AWS Management Console, mude para sua conta de destino.
2. Abra o console do Amazon S3 em <https://console.aws.amazon.com/s3/>.
3. No painel de navegação à esquerda, escolha Buckets.
4. Na lista Buckets, escolha o bucket do S3 para o qual você está transferindo dados.
5. Na página do perfil, escolha a guia Permissões.
6. Em Política de bucket, escolha Editar e faça o seguinte para modificar sua política de bucket do S3:
 - a. Atualize o que está no editor para incluir as seguintes declarações de política:

```

{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "DataSyncCreateS3LocationAndTaskAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::source-account:role/source-datasync-role"
      },
      "Action": [

```

```

        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    ]
}
]
}

```

- b. Substitua cada instância *source-account* de pelo Conta da AWS ID da sua conta de origem.
- c. *source-datasync-role* Substitua pela [função do IAM que você criou DataSync na sua conta de origem](#).
- d. Substitua cada instância do *amzn-s3-demo-destination-bucket* pelo nome do bucket do S3 em sua conta de destino.

7. Escolha Salvar alterações.

Etapa 3: na sua conta de destino, desative ACLs o bucket do S3

É importante que todos os dados transferidos para o bucket do S3 pertençam à sua conta de destino. Para garantir que essa conta possua os dados, desative as listas de controle de acesso (ACLs) do bucket. Para obter mais informações, consulte [Controle da propriedade de objetos e desativação ACLs do seu bucket no Guia](#) do usuário do Amazon S3.

Antes de começar: certifique-se de que tem as [permissões necessárias para conta de destino](#).

Desative seu bucket S3 de destino ACLs

1. Enquanto ainda estiver conectado ao console do S3 com sua conta de destino, escolha o bucket do S3 para o qual você está transferindo dados.

2. Na página do perfil, escolha a guia Permissões.
3. Em Object Ownership, escolha Editar.
4. Se ainda não estiver selecionada, escolha a opção ACLs desativada (recomendada).
5. Escolha Salvar alterações.

Etapa 4: na sua conta de origem, crie seus DataSync locais

Na sua conta de origem, crie os DataSync locais para seus buckets S3 de origem e destino.

Antes de começar: certifique-se de que tem as [permissões necessárias para conta de origem](#).

Crie sua localização DataSync de origem

- Na conta de origem, crie um [local](#) para o bucket do S3 do qual você está transferindo dados.

Crie seu local DataSync de destino

Ainda na conta de origem, crie um local para o bucket do S3 para o qual você está transferindo dados.

Como você não pode criar locais entre contas usando a interface do DataSync console, essas instruções exigem que você execute um `create-location-s3` comando para criar seu local de destino. Recomendamos executar o comando usando AWS CloudShell um shell pré-autenticado baseado em navegador que você inicia diretamente do console. CloudShell permite que você execute AWS CLI comandos `create-location-s3` sem baixar ou instalar ferramentas de linha de comando.

Note

Para concluir as etapas a seguir usando uma ferramenta de linha de comando diferente de CloudShell, certifique-se de que seu [AWS CLI perfil](#) use a mesma função do IAM que inclui as [permissões de usuário necessárias](#) para uso DataSync em sua conta de origem.

Para criar um local de DataSync destino usando CloudShell

1. Enquanto ainda estiver na sua conta de origem, faça o seguinte para iniciar a CloudShell partir do console:

- Escolha o CloudShell ícone na barra de navegação do console. Ele está à direita da caixa de pesquisa.
 - Use a caixa de pesquisa na barra de navegação do console para pesquisar CloudShelle, em seguida, escolha a CloudShellopção.
2. Copie o seguinte comando `create-location-s3`:

```
aws datasync create-location-s3 \  
  --s3-bucket-arn arn:aws:s3:::amzn-s3-demo-destination-bucket \  
  --region amzn-s3-demo-destination-bucket-region \  
  --s3-config '{  
    "BucketAccessRoleArn": "arn:aws:iam::source-account-id:role/source-datasync-  
role"  
  }'
```

3. Substitua `amzn-s3-demo-destination-bucket` pelo nome de bucket S3 em sua conta de destino.
4. Se o bucket de destino estiver em uma região diferente do bucket de origem, substitua `amzn-s3-demo-destination-bucket-region` pela região onde o bucket de destino reside (por exemplo, `us-east-2`). Remova essa opção se os buckets estiverem na mesma região.
5. `source-account-id` Substitua pelo Conta da AWS ID de origem.
6. `source-datasync-role` Substitua pela [função DataSync do IAM](#) que você criou na sua conta de origem.
7. Execute o comando em CloudShell.

Se o comando retornar um ARN de DataSync localização semelhante a este, você criou o local com sucesso:

```
{  
  "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-  
abcdef01234567890"  
}
```

8. No painel de navegação esquerdo, expanda Transferência de dados e, em seguida, escolha Locais.
9. Se você criou o local em uma região diferente, escolha essa região no painel de navegação.

Na conta de origem, você pode ver o local do bucket do S3 que acabou de criar para o bucket da conta de destino.

Etapa 5: na sua conta de origem, crie e inicie sua DataSync tarefa

Antes de iniciar uma DataSync tarefa para transferir seus dados, vamos recapitular o que você fez até agora:

- Na sua conta de origem, você criou uma função do IAM que permite DataSync transferir dados para o bucket do S3 na sua conta de destino.
- Na sua conta de destino, você configurou seu bucket do S3 para DataSync poder transferir dados para ele.
- Na sua conta de origem, você criou os locais de DataSync origem e destino para sua transferência.

Crie e inicie sua DataSync tarefa

1. Enquanto ainda estiver usando o DataSync console em sua conta de origem, expanda Transferência de dados no painel de navegação esquerdo e escolha Tarefas e Criar tarefa.
2. Se o bucket na sua conta de destino estiver em uma região diferente do bucket na sua conta de origem, escolha a região do bucket de destino no painel de navegação superior.

Important

Para evitar um erro de conexão de rede, você deve criar sua DataSync tarefa na mesma região do local de destino.

3. Na página Configurar local de origem, faça o seguinte:
 - a. Selecione Escolher um local existente.
 - b. (Para transferências entre regiões) No menu suspenso Região, escolha a região em que o bucket de origem reside.
 - c. Em Locais existentes, escolha o local de origem do bucket do S3 do qual você está transferindo dados e, em seguida, escolha Próximo.
4. Na página Configurar local de destino, faça o seguinte:
 - a. Selecione Escolher um local existente.

- b. Em Locais existentes, escolha o local de destino para o bucket do S3 para o qual você está transferindo dados e, em seguida, escolha Próximo.
5. Na página Definir configurações, escolha um modo de tarefa.

 Tip

Recomendamos usar o modo Avançado. Para obter mais informações, consulte [Escolhendo um modo de tarefa para sua transferência de dados](#).

6. Dê um nome à tarefa e defina configurações adicionais, como especificar um grupo de CloudWatch logs da Amazon. Escolha Próximo.
7. Na página Revisão, revise suas configurações e selecione Criar tarefa.
8. Na página de detalhes da tarefa, escolha Iniciar e, em seguida, escolha uma das seguintes opções:
 - Para executar a tarefa sem modificação, escolha Iniciar com padrões.
 - Para modificar a tarefa antes de executá-la, escolha Iniciar com opções de substituição.

Quando sua tarefa terminar, verifique o bucket do S3 na sua conta de destino. Você deve ver os dados que foram movidos do bucket da sua conta de origem.

Solução de problemas

Consulte as informações a seguir se tiver problemas ao tentar realizar a transferência entre contas.

Erros de conexão

Ao transferir entre buckets do S3 em diferentes regiões Contas da AWS e regiões com tarefas do modo Básico, você pode receber um erro de conexão de rede ao iniciar sua tarefa. DataSync Para resolver isso, use uma tarefa do modo Avançado. Como alternativa, crie uma tarefa do modo Básico na mesma região do seu local de destino e tente executar essa tarefa.

Relacionado: transferências entre contas com buckets S3 usando criptografia no servidor

Se você estiver tentando fazer essa transferência com buckets S3 usando criptografia no servidor, consulte o [Blog da AWS sobre armazenamento](#) para obter instruções.

Executando uma grande migração de dados com AWS DataSync

As migrações de dados em grande escala podem envolver a transferência de volumes significativos de dados que abrangem milhões de arquivos ou objetos em vários formatos. AWS DataSync simplifica essas transferências complexas gerenciando o agendamento, o monitoramento, a criptografia e a verificação de dados.

O que é uma grande migração de dados?

Uma grande migração de dados geralmente envolve a transferência de terabytes ou mais de dados espalhados por várias fontes para um novo ambiente de armazenamento de destino (nesse caso,). AWS Essas migrações exigem planejamento e coordenação cuidadosos em sua organização para mover os dados com sucesso e, ao mesmo tempo, minimizar a interrupção dos negócios.

DataSync podem simplificar essas migrações, que geralmente são de natureza complexa. Alguns benefícios do uso DataSync para sua migração incluem:

- Gerenciamento automatizado dos processos de transferência de dados e da infraestrutura necessária para transferências de dados seguras e de alto desempenho.
- End-to-end segurança, incluindo criptografia e validação da integridade dos dados, para ajudar a garantir que seus dados cheguem com segurança, intactos e prontos para uso.
- Um protocolo de rede específico e uma arquitetura paralela de vários processos para acelerar as migrações.

Estágios principais de uma grande migração de dados

Normalmente, você pode dividir uma grande migração nos seguintes estágios:

- (Etapa 1) Planejando sua migração de dados — Nesse estágio, você está tentando entender por que está migrando e com que tipo de dados está trabalhando. As atividades de planejamento incluem:
 - Entendendo por que você quer migrar
 - Reunir uma equipe para ajudá-lo em todos os aspectos da migração.

- Identificação de locais de dados, formatos e padrões de uso
- Avaliar os recursos de hardware disponíveis e os requisitos de rede (se você estiver migrando de um data center local)
- Executando testes de prova de conceito (POC) DataSync para estimar cronogramas de migração, planejar janelas de transição e ter uma ideia de como você precisa configurar DataSync
- (Etapa 2) Implementando sua migração de dados grandes — Neste momento, você está validando seu plano e iniciando a migração. As atividades de implementação incluem:
 - Validando o plano de migração
 - Executando transições em fases que incluem monitoramento e verificação de suas transferências de dados conforme o esperado
 - Otimizando e ajustando conforme necessário entre cada transição
 - Limpando recursos não utilizados quando estiver pronto

Recursos adicionais

AWS A orientação prescritiva tem os seguintes recursos que podem ajudá-lo a planejar e implementar uma grande migração. Use este guia para entender como DataSync pode funcionar no contexto de processos e atividades comuns de migração.

- [Grandes migrações para a nuvem AWS](#)
- [Estratégia e melhores práticas para AWS grandes migrações](#)
- [Migre sistemas de arquivos compartilhados em uma AWS grande migração](#) — Esse recurso inclui uma pasta de trabalho do SFS-Discovery-Workbook que você pode baixar e usar para planejar uma migração no nível do compartilhamento de arquivos.

Etapa 1: Planejando sua migração de grandes volumes de dados

O planejamento é essencial ao migrar um grande conjunto de dados. Você deve entender os dados que está migrando, suas motivações para a migração e como você AWS DataSync pode ajudá-lo a colocar seus dados onde quiser.

Tópicos

- [Reunindo os requisitos para sua migração](#)

- [Executando uma DataSync prova de conceito](#)
- [Estimando os cronogramas de migração](#)

Reunindo os requisitos para sua migração

A primeira etapa de uma grande migração de dados requer a coleta de uma variedade de informações em toda a organização.

Essas informações ajudam você a criar um [processo](#) de migração que, para grandes migrações, pode incluir várias transferências e procedimentos para cortar as operações (feitas em [ondas](#)) do armazenamento de origem para o destino.

Entendendo por que você quer migrar

Antes de começar a migrar para AWS, você precisa entender claramente por que está migrando seus dados. Isso ajuda a enfrentar desafios comuns de migração, como cumprir prazos, gerenciar recursos e coordenar as equipes.

Se precisar de ajuda para determinar suas motivações para a migração, responda a estas perguntas:

- Você está liberando espaço de armazenamento local?
- Você está cumprindo os prazos dos contratos de suporte de hardware?
- Isso é para a saída de um data center?
- Qual é o seu cronograma de migração?
- Você está transferindo dados de outro armazenamento em nuvem?
- Você está migrando conjuntos de dados parciais ou completos?
- Isso é para arquivamento de dados?
- Os aplicativos ou usuários precisam de acesso regular a esses dados?

Descobrimos a logística

Aborde algumas logísticas básicas sobre seu ambiente de armazenamento, a migração e sua organização:

1. Obtenha uma compreensão básica da sua infraestrutura atual de armazenamento de dados.

2. Verifique se você precisa de um [DataSync agente](#). Por exemplo, você precisa de um agente se estiver transferindo do armazenamento local.
3. Se você precisar de um agente, certifique-se de entender os [requisitos do agente](#):
 - Um agente pode ser executado como uma máquina virtual (VM) em VMware ESXi uma máquina virtual baseada em kernel Linux (KVM) e em hipervisores Microsoft Hyper-V. Você também pode implantar um agente como uma EC2 instância da Amazon dentro AWS.
 - Em geral, grandes migrações consomem muita memória. Certifique-se de que seu agente tenha RAM suficiente.
4. Identifique as principais partes interessadas de seus departamentos de liderança, rede, armazenamento e TI que precisam estar envolvidas na migração. Elas podem incluir:
 - Encontre um [líder único que se](#) dedique ao projeto e seus resultados.
 - Determine quem é responsável pela propriedade e classificação dos dados que você está migrando.
 - Identifique quem gerencia sua fonte e quem eventualmente gerenciará o serviço AWS de armazenamento para o qual você está migrando.
 - Descubra quem criará e gerenciará quaisquer outros processos para seus dados depois que eles entrarem AWS.
5. Estabeleça canais de comunicação entre departamentos.
6. Crie um plano de reversão para contingências.
7. Documente o processo completo de migração, incluindo ondas, validação e procedimentos de transição. Use isso como seu runbook para toda a migração. Você atualizará esse processo ao planejar e implementar a migração.

Analizando os dados que você está migrando

Trabalhe com suas equipes de armazenamento e aplicativos para analisar as características dos dados que você está migrando. Essas informações ajudam a determinar uma estratégia de migração com a qual você pode executar DataSync.

Sumário

- [Determinando padrões de uso de dados](#)
- [Identificação da estrutura e do layout dos dados](#)
- [Documentando compartilhamentos e pastas](#)

- [Analisando tamanhos de arquivos](#)

Determinando padrões de uso de dados

- Para dados usados ativamente com modificações frequentes, planeje várias ondas de transferências incrementais para evitar interromper as operações comerciais.
- Para dados somente para leitura que podem ser considerados arquivados, talvez você não precise planejar ondas.
- Se você tiver uma combinação de padrões de uso de dados, planeje ondas que migrem esses diferentes conjuntos de dados separadamente. Por exemplo, você pode ter uma onda para arquivar dados, com o resto das ondas dedicadas à migração de dados ativos.

Identificação da estrutura e do layout dos dados

- Determine se os dados estão organizados por períodos (ano, mês, dia) ou outros padrões.
- Use essa estrutura organizacional para planejar suas ondas de migração. Por exemplo, você pode migrar o equivalente a um ano de dados arquivados durante uma onda.

Documentando compartilhamentos e pastas

- Crie um inventário de compartilhamentos e pastas (incluindo contagens de arquivos ou objetos para cada um).
- Identifique compartilhamentos e pastas com conjuntos de dados ativos. Isso pode exigir transferências incrementais durante a migração.
- Revise as [DataSync cotas](#). Isso pode ajudar você a planejar como particionar seu conjunto de dados durante a configuração DataSync.

Analisando tamanhos de arquivos

- Espere uma maior taxa de transferência de dados para transferências com arquivos maiores (MB ou GB) em comparação com arquivos menores (KB).
- Se você estiver trabalhando com muitos arquivos menores, espere mais operações de metadados em seu sistema de armazenamento e menor taxa de transferência de dados. DataSync executa essas operações ao comparar e verificar seus locais de origem e destino.

Identificação dos requisitos de armazenamento

Para escolher um serviço AWS de armazenamento compatível para migrar seus dados, você precisa avaliar as características e o desempenho do sistema de armazenamento de origem.

Essas informações também podem ajudá-lo a [programar suas transferências](#) para minimizar o impacto nas operações comerciais durante a migração.

Sumário

- [Determinando o suporte ao armazenamento de origem](#)
- [Analisando os requisitos de preservação de metadados](#)
- [Coletando métricas de desempenho do armazenamento de origem](#)
- [Escolhendo um serviço AWS de armazenamento de destino](#)

Determinando o suporte ao armazenamento de origem

DataSync pode trabalhar com uma variedade de sistemas de armazenamento que permitem acesso por meio de clientes de armazenamento de objetos compatíveis com NFS, SMB, HDFS e S3.

Se você estiver migrando de outro armazenamento em nuvem, verifique se ele DataSync funciona com esse provedor. Para obter uma lista dos locais de origem compatíveis, consulte [Para onde posso transferir meus dados com AWS DataSync?](#)

Analisando os requisitos de preservação de metadados

DataSync pode preservar seus metadados de arquivo ou objeto durante uma transferência. A forma como seus metadados são preservados depende dos locais de transferência e se esses locais usam tipos semelhantes de metadados.

DataSync em alguns casos, precisa de permissões adicionais para preservar os metadados do arquivo, como listas de acesso discrecionário do NTFS (). DACLs

Para obter mais informações, consulte [Entendendo como DataSync manipula metadados de arquivos e objetos](#).

Coletando métricas de desempenho do armazenamento de origem

Meça o IOPS básico e a taxa de transferência de disco durante cargas de trabalho médias e de pico para seu armazenamento de origem. A transferência de dados adiciona sobrecarga de I/O aos sistemas de armazenamento de origem e de destino.

Compare esses dados de desempenho com as especificações do seu sistema de armazenamento para determinar os recursos de desempenho disponíveis.

Escolhendo um serviço AWS de armazenamento de destino

Nesse ponto, você pode ter uma ideia de qual serviço AWS de armazenamento faz sentido para seus dados. Caso contrário, os padrões de uso de dados e o desempenho do armazenamento são algumas áreas a serem consideradas ao decidir. Por exemplo, você pode considerar o Amazon S3 se tiver dados de arquivamento e o Amazon ou o FSx Amazon EFS para dados ativos.

Para ajudá-lo a decidir o armazenamento baseado em objetos ou arquivos certo para seus dados, consulte [Escolha de um serviço AWS de armazenamento](#).

Determinando os requisitos de rede

Para migrar seus dados com DataSync, você deve estabelecer conexões de rede entre o armazenamento de origem, o agente e AWS. Você também precisa planejar a largura de banda e a infraestrutura de rede suficientes.

Trabalhe com seus engenheiros de rede e administradores de armazenamento para reunir os seguintes requisitos de rede.

Sumário

- [Avaliando sua largura de banda de rede disponível](#)
- [Considerando as opções para conectar sua rede a AWS](#)
- [Escolhendo um endpoint de serviço para comunicação com agentes](#)
- [Planejando uma infraestrutura de rede suficiente](#)

Avaliando sua largura de banda de rede disponível

Sua largura de banda de rede disponível influencia suas velocidades de transferência e o tempo geral de migração. Se você estiver transferindo de um sistema de armazenamento local, faça o seguinte:

- Trabalhe com sua equipe de rede para determinar a utilização média e máxima da largura de banda.
- Identifique as janelas em que você pode transferir dados e evite interromper as operações diárias. Isso informará quando suas ondas de migração e transições acontecerem.

Você pode controlar a quantidade de largura de banda DataSync usada. Para obter mais informações, consulte [Definir limites de largura de banda para a tarefa de AWS DataSync](#).

Como as transferências de outro armazenamento em nuvem geralmente acontecem pela Internet pública, geralmente há menos restrições e considerações de largura de banda com essas transferências.

Considerando as opções para conectar sua rede a AWS

Considere as seguintes opções para estabelecer a conectividade de rede para sua DataSync transferência:

- AWS Direct Connect- Analise os [exemplos de arquitetura e roteamento](#) para usar o Direct Connect with DataSync. Você pode monitorar a atividade do Direct Connect usando a [Amazon CloudWatch](#).
- VPN - [AWS Site-to-Site VPN](#) oferece taxa de transferência de até 1,25 Gbps por túnel.
- Internet pública - Entre em contato com seu provedor de serviços de Internet para obter dados de uso da rede.

Escolhendo um endpoint de serviço para comunicação com agentes

DataSync os agentes usam [endpoints de serviço](#) para se comunicarem com o DataSync serviço. O tipo de endpoint que você usa depende de como você está se conectando à AWS sua rede.

Planejando uma infraestrutura de rede suficiente

Para cada tarefa de transferência que você cria, gera e gerencia DataSync automaticamente a infraestrutura de rede para suas transferências de dados. Essa infraestrutura é conhecida como interfaces de rede ou interfaces de rede elásticas, que são componentes lógicos de rede em uma nuvem privada virtual (VPC) da Amazon que representam placas de rede virtuais. Para obter mais informações, consulte o [Guia EC2 do usuário da Amazon](#).

Cada interface de rede usa um único endereço IP na sub-rede VPC de destino. Para garantir que você tenha infraestrutura de rede suficiente para sua migração, faça o seguinte:

- Observe o número de [interfaces de rede](#) que DataSync serão criadas para seu local de DataSync destino.
- Certifique-se de que sua sub-rede tenha endereços IP suficientes para suas DataSync tarefas. Por exemplo, uma tarefa que usa um agente exige quatro endereços IP. Se você criar quatro tarefas

para sua migração, isso significa que você precisa de 16 endereços IP disponíveis na sua sub-rede.

Executando uma DataSync prova de conceito

Executar uma prova de conceito (POC) AWS DataSync ajuda você a validar os seguintes aspectos do seu planejamento de migração de dados:

- Verifique a conectividade de rede entre os locais de origem e destino.
- Valide sua configuração inicial de DataSync tarefas.
- Avalie o desempenho da transferência de dados.
- Estime os cronogramas de migração.
- Defina critérios de sucesso com as principais partes interessadas que trabalham na migração.

Começando com sua prova de conceito

1. Crie seu DataSync agente:
 1. [Implante seu agente](#).
 2. [Escolha um endpoint de serviço](#) para seu agente.
 3. [Ative o agente](#).
 4. [Verifique as conexões de rede do seu agente](#).
2. Selecione um pequeno subconjunto de dados que represente os dados que você está migrando.

Por exemplo, se o armazenamento de origem tiver uma mistura de arquivos grandes e pequenos, o subconjunto de dados que você transfere na sua POC deve refletir isso. Isso fornece uma compreensão preliminar do desempenho dos sistemas de armazenamento, de sua rede DataSync e.
3. Crie um local DataSync de origem para seu sistema de armazenamento [local](#) ou [outro sistema de armazenamento em nuvem](#).
4. Crie um local de DataSync destino para seu [serviço AWS de armazenamento](#).
5. [Crie uma tarefa DataSync de transferência](#) com um [filtro](#) que transfere somente seu subconjunto de dados.
6. [Comece sua DataSync tarefa](#).
7. Colete métricas de desempenho de transferência monitorando o seguinte:

- A taxa de transferência de dados e arquivos da execução da sua tarefa. Você pode fazer isso por meio do DataSync console ou da [DescribeTaskExecution](#) operação. Se você usa `DescribeTaskExecution`, veja como calcular essas métricas:
 - Taxa de transferência de dados: `Divida BytesWritten por TransferDuration`
 - Taxa de transferência de arquivos: `Divida FilesTransferred por TransferDuration`
 - Utilização do armazenamento na origem e no destino. Trabalhe em estreita colaboração com seus administradores de armazenamento para obter essas informações.
 - Uso da rede.
8. Verifique os dados transferidos em seu local de destino:
- Analise seus CloudWatch registros em busca de erros de execução de tarefas.
 - Verifique se as permissões e os metadados estão preservados no local de destino.
 - Confirme se os aplicativos e os usuários podem acessar os dados de destino conforme o esperado.
 - Resolva todos os problemas que você encontrar. Para obter mais informações, consulte [Solução de AWS DataSync problemas](#).
9. Execute sua tarefa mais algumas vezes para ter uma ideia de quanto tempo é necessário DataSync para preparar, transferir e verificar seus dados. (Para ter mais informações, consulte [Status de execução de tarefa](#).)

Se você executar uma tarefa mais de uma vez, DataSync por padrão, executará uma transferência incremental e copiará somente os dados que foram alterados em relação à execução anterior da tarefa.

Embora o tempo de transferência provavelmente seja menor para transferências incrementais, sempre DataSync preparará sua transferência da mesma forma, examinando e comparando seus locais para identificar o que transferir. Você pode usar esses tempos de preparação para [estimar os cronogramas de transição](#) para sua migração.

10. Se necessário, atualize seu plano de migração com base no que você aprendeu durante o POC.

Estimando os cronogramas de migração

Usando as informações que você coletou até agora, você pode estimar quanto tempo a migração levará usando AWS DataSync.

Estimando cronogramas de transferência de dados

Você pode estimar quanto tempo leva DataSync para transferir seus dados com base nas seguintes informações coletadas durante a coleta dos requisitos de migração e na sua DataSync prova de conceito (POC):

- Sua largura de [banda de rede disponível](#)
- Métricas de utilização do armazenamento na origem e no destino
- Métricas de desempenho do seu [DataSync POC](#)

Para estimar um cronograma de transferência de dados

1. Compare a taxa de transferência de dados e arquivos do seu POC com a largura de banda de rede disponível.
2. Se sua taxa de transferência for menor que a largura de banda disponível (como 300 MiB/s para taxa de transferência com 10 Gbps de largura de banda de rede), considere particionar seu conjunto de dados em várias tarefas para maximizar o uso da largura de banda.

DataSync tem algumas opções para particionar seu conjunto de dados. Para obter mais informações, consulte [Acelerando sua migração com particionamento de dados](#).

3. Calcule quantos dias uma transferência leva usando a seguinte fórmula, que fornece um tempo mínimo teórico de transferência:

```
(DATA_SIZE * 8 bits per byte)/(CIRCUIT * NETWORK_UTILIZATION percentage * 3600  
seconds per hour * AVAILABLE_HOURS) = Number of days
```

Ao usar essa fórmula, substitua o seguinte pelos seus próprios valores:

- DATA_SIZE: a quantidade de dados que você está migrando (expressa em bytes).
- CIRCUIT: Sua largura de banda de rede disponível (expressa em bits por segundo).
- NETWORK_UTILIZATION: Qual porcentagem da sua rede está sendo usada.
- AVAILABLE_HOURS: O número de horas operacionais disponíveis em cada dia.

Por exemplo, você calcularia uma migração com 100 TB de dados, uma conexão de internet de 1 Gbps, 80% de utilização da rede e disponibilidade de 24 horas por dia da seguinte forma:

$$(100,000,000,000,000 \text{ bytes} * 8) / (1,000,000,000 \text{ bps} * 0.80 * 3600 * 24) = 11.57 \text{ days}$$

Nesse caso, a migração levaria quase 12 dias antes de considerar as condições do mundo real.

4. Ajuste a duração calculada da transferência de acordo com as condições do mundo real:

- Flutuações no desempenho da rede
- Variações de desempenho de armazenamento
- Tempo de inatividade entre as ondas de migração

Estimando cronogramas de transição

Se você estiver migrando conjuntos de dados ativos, provavelmente precisará de transferências para não interromper as operações comerciais.

Não subestime quanto tempo as transições demoram. Com grandes migrações, não é incomum que as atividades de transição ocupem até 30% do tempo total de migração.

1. Avalie se você precisa realizar transições em ondas para reduzir a quantidade de dados digitalizados em busca de alterações incrementais.

Uma estratégia para fazer isso é cortar os conjuntos de dados que você particiona com base em compartimentos, pastas ou sistemas de armazenamento.

2. Analise quanto tempo geralmente é necessário DataSync para preparar, transferir e verificar seus dados durante o POC.

Observe, em particular, as durações de preparação das execuções de suas tarefas. Para encontrar essas informações, execute a [DescribeTaskExecution](#) operação e verifique o valor do tempo [PrepareDuration](#) de duração (em milissegundos).

3. Estime quanto tempo uma transição pode levar medindo o delta de tempo em tarefas paralelas.

Para obter mais informações sobre tarefas paralelas, consulte [Acelerando sua migração com particionamento de dados](#).

4. Use sua estimativa de transição para agendar suas transições. Basicamente, essas são janelas de manutenção em que seus dados de origem não podem ser modificados.

Próximas etapas

Depois de estimar seus cronogramas, você está pronto para começar a implementar sua migração.

Etapa 2: Implementando sua migração de dados grandes

Com as informações coletadas durante o planejamento, você pode começar a usá-las AWS DataSync para migrar para seu novo sistema de armazenamento. Se você ainda não o fez, recomendamos revisar os [recursos de orientação AWS prescritiva para](#) grandes migrações.

Tópicos

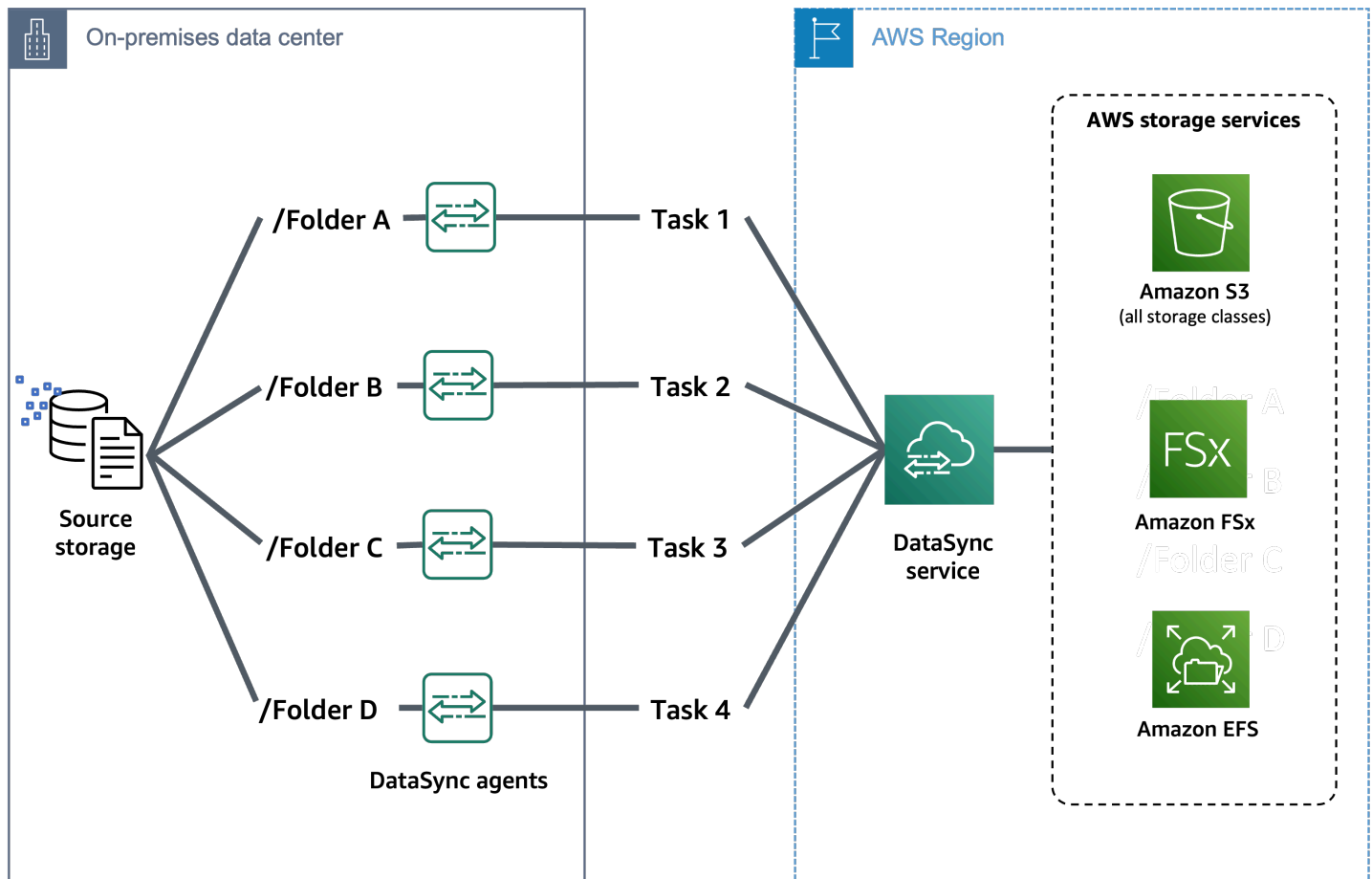
- [Acelerando sua migração com particionamento de dados](#)
- [Executando suas tarefas DataSync de transferência](#)
- [Monitorando suas transferências](#)

Acelerando sua migração com particionamento de dados

Com uma grande migração, recomendamos particionar seu conjunto de dados com várias tarefas. DataSync Particionar seus dados de origem em várias tarefas (e possivelmente em agentes) permite paralelizar suas transferências e reduzir o cronograma de migração.

O particionamento também ajuda você a permanecer dentro das DataSync [cotas](#) e simplifica o monitoramento e a depuração de suas tarefas.

O diagrama a seguir mostra como você pode usar várias DataSync tarefas e agentes para transferir dados do mesmo local de armazenamento de origem. Nesse cenário, cada tarefa se concentra em uma pasta específica no local de origem. Para obter mais informações e exemplos sobre essas abordagens, consulte [Como acelerar suas transferências de dados com arquiteturas de AWS DataSync expansão](#) horizontal.



Particionar seu conjunto de dados por pasta ou prefixo

Ao criar seu local de DataSync origem, você pode especificar uma pasta, diretório ou prefixo que seja DataSync lido. Por exemplo, se você estiver migrando um compartilhamento de arquivos com diretórios de nível superior, poderá criar vários locais que especificam um caminho de diretório diferente. Em seguida, você pode usar esses locais para executar várias DataSync tarefas durante a migração.

Particionando seu conjunto de dados com filtros

Você pode aplicar [filtros](#) para incluir ou excluir dados do seu local de origem em uma transferência. No contexto de uma grande migração, os filtros podem ajudar você a definir o escopo das tarefas para partes específicas do seu conjunto de dados.

Por exemplo, se você estiver migrando dados de arquivamento organizados por ano, poderá criar um filtro de inclusão que corresponda a um ano específico ou a vários anos. Você também pode modificar o filtro sempre que executar a tarefa para corresponder a um ano diferente.

Particionando seu conjunto de dados com manifestos

Um [manifesto](#) é uma lista de arquivos ou objetos que você DataSync deseja transferir. Com um manifesto, DataSync não é necessário ler tudo em um local de origem para determinar o que transferir.

Você pode criar manifestos a partir de inventários de seu armazenamento de origem ou por meio de abordagens orientadas por eventos (por exemplo, consulte [Implementação AWS DataSync com centenas de milhões de objetos](#)). Você também pode usar um manifesto diferente cada vez que inicia uma tarefa, permitindo transferir diferentes conjuntos de dados com a mesma tarefa.

Executando suas tarefas DataSync de transferência

Durante cada uma das ondas de migração, sua transferência de dados geralmente segue o mesmo processo geral:

1. Execute uma transferência inicial completa dos seus dados.
2. Verifique os dados no destino.
3. Execute transferências incrementais para quaisquer dados que possam ter sido alterados desde a transferência inicial.
4. Reduza as operações para o local de destino.
5. Analise os resultados da transição.

Executando suas tarefas

Provavelmente, você precisará executar suas tarefas de DataSync transferência durante o horário comercial para minimizar o tempo geral de migração. É comum nessas situações executar uma transferência inicial completa seguida por transferências incrementais que contabilizam as alterações feitas por usuários e aplicativos em seu local de origem.

Para evitar problemas relacionados à rede durante o horário comercial, você pode limitar a quantidade de largura de banda que suas tarefas usam. Para obter mais informações, consulte [Definir limites de largura de banda para a tarefa de AWS DataSync](#).

1. Execute uma transferência inicial completa:
 - a. [Inicie sua DataSync tarefa](#) (ou tarefas se você estiver executando tarefas em paralelo).

- b. Monitore o progresso e o desempenho de suas execuções de tarefas.
 - c. Verifique se seus dados foram transferidos da maneira esperada (por exemplo, os metadados do arquivo foram preservados).
2. Execute transferências incrementais:
 - a. [Agende suas tarefas](#) para serem executadas periodicamente.
 - b. Monitore suas execuções de tarefas e corrija erros, se encontrados.

Executando uma transição

Após as transferências iniciais e incrementais, você pode iniciar o processo de transferir as operações para o local de destino.

1. Inicie a janela de manutenção programada.
2. Atualize seu sistema de armazenamento de origem para que seja lido somente por aplicativos e usuários.
3. Execute as transferências incrementais finais para copiar os deltas restantes entre seus locais de origem e destino.
4. Conduza uma validação completa dos dados (por exemplo, revisando CloudWatch registros e [relatórios de tarefas](#)).
5. Mude seus aplicativos e usuários para o novo ambiente do seu local de destino.
6. Teste a funcionalidade do aplicativo e certifique-se de que os usuários possam acessar os dados em seu local de destino.
7. Agende uma reunião retrospectiva para analisar a transferência com as equipes de migração. Faça os seguintes exemplos de perguntas de sondagem:
 - A transição foi bem-sucedida? Se não, qual foi o problema?
 - Usamos toda a largura de banda disponível?
 - O armazenamento de origem e de destino foi totalmente utilizado?
 - Podemos obter mais produtividade de dados com tarefas adicionais?
 - Precisamos planejar uma janela de manutenção mais longa?
8. Se necessário, atualize seu plano de migração antes de iniciar a próxima onda.

Monitorando suas transferências

AWS DataSync fornece várias opções de monitoramento para ajudá-lo a validar e depurar sua transferência.

Monitorando suas transferências com CloudWatch métricas

Você pode criar CloudWatch painéis personalizados com métricas de suas execuções de DataSync tarefas. Para obter mais informações, consulte [Monitoramento de transferências de dados com CloudWatch métricas da Amazon](#).

Monitorando suas transferências com relatórios de tarefa

Se você estiver transferindo milhões de arquivos ou objetos, considere usar relatórios de tarefas. Os relatórios de tarefas fornecem informações detalhadas sobre quais DataSync tentativas transferir, ignorar, verificar e excluir durante a execução de uma tarefa. Para obter mais informações, consulte [Monitorando suas transferências de dados com relatórios de tarefas](#).

Você também pode visualizar seus relatórios de tarefas usando AWS serviços como AWS Glue Amazon Athena e Amazon. QuickSight Para obter mais informações, consulte o [blog AWS de armazenamento](#).

Monitorando suas transferências com o CloudWatch Logs

No mínimo, recomendamos que você configure sua tarefa para registrar informações básicas e erros de transferência. Para obter mais informações, consulte [Monitoramento de transferências de dados com o Amazon CloudWatch Logs](#).

AWS DataSync API

Além do AWS Management Console e AWS CLI, você pode usar a AWS DataSync API para configurar e gerenciar DataSync com [AWS SDKs](#).

Tópicos

- [Ações](#)
- [Tipos de dados](#)
- [Erros comuns](#)
- [Parâmetros gerais](#)

Ações

As ações a seguir são compatíveis:

- [CancelTaskExecution](#)
- [CreateAgent](#)
- [CreateLocationAzureBlob](#)
- [CreateLocationEfs](#)
- [CreateLocationFsxLustre](#)
- [CreateLocationFsxOntap](#)
- [CreateLocationFsxOpenZfs](#)
- [CreateLocationFsxWindows](#)
- [CreateLocationHdfs](#)
- [CreateLocationNfs](#)
- [CreateLocationObjectStorage](#)
- [CreateLocationS3](#)
- [CreateLocationSmb](#)
- [CreateTask](#)
- [DeleteAgent](#)
- [DeleteLocation](#)
- [DeleteTask](#)

- [DescribeAgent](#)
- [DescribeLocationAzureBlob](#)
- [DescribeLocationEfs](#)
- [DescribeLocationFsxLustre](#)
- [DescribeLocationFsxOntap](#)
- [DescribeLocationFsxOpenZfs](#)
- [DescribeLocationFsxWindows](#)
- [DescribeLocationHdfs](#)
- [DescribeLocationNfs](#)
- [DescribeLocationObjectStorage](#)
- [DescribeLocationS3](#)
- [DescribeLocationSmb](#)
- [DescribeTask](#)
- [DescribeTaskExecution](#)
- [ListAgents](#)
- [ListLocations](#)
- [ListTagsForResource](#)
- [ListTaskExecutions](#)
- [ListTasks](#)
- [StartTaskExecution](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateAgent](#)
- [UpdateLocationAzureBlob](#)
- [UpdateLocationEfs](#)
- [UpdateLocationFsxLustre](#)
- [UpdateLocationFsxOntap](#)
- [UpdateLocationFsxOpenZfs](#)
- [UpdateLocationFsxWindows](#)
- [UpdateLocationHdfs](#)

- [UpdateLocationNfs](#)
- [UpdateLocationObjectStorage](#)
- [UpdateLocationS3](#)
- [UpdateLocationSmb](#)
- [UpdateTask](#)
- [UpdateTaskExecution](#)

CancelTaskExecution

Interrompe AWS DataSync a execução de uma tarefa que está em andamento. A transferência de alguns arquivos é interrompida abruptamente. O conteúdo do arquivo transferido para o destino pode estar incompleto ou inconsistente com os arquivos de origem.

No entanto, se você iniciar uma nova execução de tarefa usando a mesma tarefa e permitir que ela termine, o conteúdo do arquivo no destino será completo e consistente. Isto se aplica a outras falhas inesperadas que interrompem a execução de uma tarefa. Em todos esses casos, conclui DataSync com êxito a transferência ao iniciar a próxima execução da tarefa.

Sintaxe da Solicitação

```
{  
  "TaskExecutionArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[TaskExecutionArn](#)

O nome do recurso da Amazon (ARN) da execução da tarefa a ser interrompida.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Exigido: Sim

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateAgent

Ativa um AWS DataSync agente que você implanta em seu ambiente de armazenamento. O processo de ativação associa o agente ao seu Conta da AWS.

Se você ainda não implantou um agente, consulte [Preciso de um DataSync agente?](#)

Sintaxe da Solicitação

```
{
  "ActivationKey": "string",
  "AgentName": "string",
  "SecurityGroupArns": [ "string" ],
  "SubnetArns": [ "string" ],
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "VpcEndpointId": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[ActivationKey](#)

Especifica a chave de ativação do seu DataSync agente. Se você não tiver uma chave de ativação, consulte [Activating your agent](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 29.

Padrão: [A-Z0-9]{5}(-[A-Z0-9]{5}){4}

Exigido: Sim

AgentName

Especifica um nome para o seu agente. Recomendamos especificar um nome que possa lembrar.

Tipo: String

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Obrigatório: Não

SecurityGroupArns

Especifica o nome do recurso da Amazon (ARN) do grupo de segurança que permite tráfego entre o agente e endpoint de serviço da VPC. Você pode especificar apenas ARN.

Tipo: matriz de strings

Membros da matriz: número fixo de 1 item.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Obrigatório: Não

SubnetArns

Especifica o ARN da sub-rede em que o endpoint da VPC está localizado. Você pode especificar apenas ARN.

Tipo: matriz de strings

Membros da matriz: número fixo de 1 item.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:subnet/.*$`

Obrigatório: Não

Tags

Especifica rótulos que ajudam você a categorizar, filtrar e pesquisar seus AWS recursos. Recomendamos criar pelo menos uma etiqueta para o seu agente.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

VpcEndpointId

Especifica o ID do [endpoint de serviço da VPC](#) que você está usando. Por exemplo, um ID de endpoint da VPC parece `vpce-01234d5aff67890e1`.

Important

O endpoint de serviço VPC que você usa deve incluir o nome do DataSync serviço (por exemplo,). `com.amazonaws.us-east-2.datasync`

Tipo: sequência

Padrão: `^vpce-[0-9a-f]{17}$`

Obrigatório: Não

Sintaxe da Resposta

```
{  
  "AgentArn": "string"  
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AgentArn

O ARN do agente que você acabou de ativar. Use a [ListAgents](#) operação para retornar uma lista de agentes em sua Conta da AWS Região da AWS e.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo de solicitação

O exemplo a seguir ativa um DataSync agente.

```
{
  "ActivationKey": "AAAAA-1AAAA-BB1CC-33333-EEEEEE",
  "AgentName": "MyAgent",
  "Tags": [{
    "Key": "Job",
    "Value": "TransferJob-1"
  }]
}
```

```
}
```

Resposta da amostra

A resposta retorna o ARN do agente ativado.

```
{
  "AgentArn": "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44baca3"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationAzureBlob

Cria um local de transferência para um contêiner do Microsoft Azure Blob Storage. AWS DataSync pode usar esse local como origem ou destino de transferência. Você pode fazer transferências com ou sem um [DataSync agente](#) que se conecta ao seu contêiner.

[Antes de começar, certifique-se de saber como DataSync acessa o Armazenamento de Blobs do Azure e trabalha com camadas de acesso e tipos de blob.](#)

Sintaxe da Solicitação

```
{
  "AccessTier": "string",
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "BlobType": "string",
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "ContainerUrl": "string",
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "SasConfiguration": {
    "Token": "string"
  },
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

AccessTier

Especifica o nível de acesso para o qual deseja que seus objetos ou arquivos sejam transferidos. Isso só se aplica ao usar o local como destino de transferência. Para obter mais informações, consulte [Níveis de acesso](#).

Tipo: String

Valores Válidos: HOT | COOL | ARCHIVE

Obrigatório: Não

AgentArns

(Opcional) Especifica o Amazon Resource Name (ARN) do agente que pode se conectar DataSync ao seu contêiner do Azure Blob Storage. Se você estiver configurando uma transferência entre nuvens sem agente, não precisará especificar um valor para esse parâmetro.

Você pode especificar mais de um atendente. Para obter mais informações, consulte [Utilizar vários agentes para sua transferência](#).

Note

Certifique-se de configurar esse parâmetro corretamente ao criar seu local de armazenamento pela primeira vez. Você não pode adicionar ou remover agentes de um local de armazenamento depois de criá-lo.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obrigatório: Não

AuthenticationType

Especifica o método de autenticação DataSync usado para acessar seu Armazenamento de Blobs do Azure. DataSync pode acessar o armazenamento de blobs usando uma assinatura de acesso compartilhado (SAS).

Tipo: String

Valores Válidos: SAS | NONE

Obrigatório: Sim

BlobType

Especifica o tipo de blob que você deseja que seus objetos ou arquivos sejam ao transferi-los para o Armazenamento de Blobs do Azure. Atualmente, DataSync só dá suporte à movimentação de dados para o Armazenamento de Blobs do Azure como blobs de blocos. Para obter mais informações sobre os tipos de blob, consulte a [Documentação do armazenamento de blobs do Azure](#).

Tipo: String

Valores Válidos: BLOCK

Obrigatório: Não

CmkSecretConfig

Especifica as informações de configuração DataSync de um segredo gerenciado, que inclui o token de autenticação DataSync usado para acessar um local de AzureBlob armazenamento específico, com um gerenciado pelo cliente. AWS KMS key

Ao incluir esse parâmetro como parte de uma `CreateLocationAzureBlob` solicitação, você fornece somente o ARN da chave KMS. DataSync usa essa chave KMS junto com o token de autenticação que você especifica `SasConfiguration` para criar um segredo DataSync gerenciado para armazenar as credenciais de acesso à localização.

Verifique se DataSync ele tem permissão para acessar a chave KMS especificada.

Note

Você pode usar `CmkSecretConfig` (`comSasConfiguration`) ou `CustomSecretConfig` (`semSasConfiguration`) para fornecer credenciais para

uma `CreateLocationAzureBlob` solicitação. Não forneça os dois parâmetros para a mesma solicitação.

Tipo: objeto [CmkSecretConfig](#)

Obrigatório: Não

[ContainerUrl](#)

Especifica a URL do contêiner de Armazenamento de Blobs do Azure envolvido na transferência.

Tipo: String

Restrições de tamanho: tamanho máximo de 325.

Padrão: `^https:\\\\[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]){0,252}\\[a-z0-9](-?[a-z0-9]){2,62}$`

Exigido: Sim

[CustomSecretConfig](#)

Especifica as informações de configuração para um segredo do Secrets Manager gerenciado pelo cliente em que o token de autenticação de um local AzureBlob de armazenamento é armazenado em texto simples. Essa configuração inclui o ARN secreto e o ARN de uma função do IAM que fornece acesso ao segredo.

Note

Você pode usar `CmkSecretConfig` (`comSasConfiguration`) ou `CustomSecretConfig` (`semSasConfiguration`) para fornecer credenciais para uma `CreateLocationAzureBlob` solicitação. Não forneça os dois parâmetros para a mesma solicitação.

Tipo: objeto [CustomSecretConfig](#)

Obrigatório: Não

[SasConfiguration](#)

Especifica a configuração SAS que permite acessar seu DataSync Armazenamento de Blobs do Azure.

Note

Se você fornecer um token de autenticação usando `SasConfiguration`, mas não fornecer detalhes de configuração secreta usando `CmkSecretConfig` ou `CustomSecretConfig`, então DataSync armazena o token usando o segredo do gerenciador de segredos da sua AWS conta.

Tipo: objeto [AzureBlobSasConfiguration](#)

Obrigatório: Não

Subdirectory

Especifica segmentos de caminho se você quiser limitar a transferência para um diretório virtual no contêiner (por exemplo, `/my/images`).

Tipo: String

Restrições de comprimento: comprimento máximo de 1024.

Padrão: `^[\\p{L}\\p{M}\\p{Z}\\p{S}\\p{N}\\p{P}\\p{C}]*$`

Obrigatório: Não

Tags

Especifica rótulos que ajudam você a categorizar, filtrar e pesquisar seus recursos da AWS . Recomendamos criar pelo menos uma etiqueta de nome para seu local de transferência.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

Sintaxe da Resposta

```
{
  "LocationArn": "string"
}
```


Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[LocationArn](#)

O ARN do local de transferência do Armazenamento de Blobs do Azure que você criou.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)

- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationEfs

Criar um local de transferência para um sistema de arquivos Amazon EFS. O AWS DataSync pode usar esse local como origem ou de destino para transferir dados.

Antes de começar, certifique-se de entender como DataSync [acessa os sistemas de arquivos do Amazon EFS](#).

Sintaxe da Solicitação

```
{
  "AccessPointArn": "string",
  "Ec2Config": {
    "SecurityGroupArns": [ "string" ],
    "SubnetArn": "string"
  },
  "EfsFileSystemArn": "string",
  "FileSystemAccessRoleArn": "string",
  "InTransitEncryption": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AccessPointArn](#)

Especifica o Amazon Resource Name (ARN) do ponto DataSync de acesso usado para montar seu sistema de arquivos Amazon EFS.

Para obter mais informações, consulte [Acesso a sistemas de arquivos restritos](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-\0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}$`

Obrigatório: Não

[Ec2Config](#)

Especifica a sub-rede e os grupos de segurança DataSync usados para se conectar a um dos destinos de [montagem](#) do seu sistema de arquivos Amazon EFS.

Tipo: objeto [Ec2Config](#)

Obrigatório: Sim

[EfsFileSystemArn](#)

Especifica o ARN do sistema de arquivos Amazon EFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

Exigido: Sim

[FileSystemAccessRoleArn](#)

Especifica uma função AWS Identity and Access Management (IAM) que permite DataSync acessar seu sistema de arquivos Amazon EFS.

Para obter informações sobre como criar essa função, consulte [Criação de uma função DataSync do IAM para acesso ao sistema de arquivos](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Obrigatório: Não

[InTransitEncryption](#)

Especifica se você deseja usar DataSync a criptografia Transport Layer Security (TLS) 1.2 ao transferir dados para ou do seu sistema de arquivos Amazon EFS.

Se você especificar um ponto de acesso usando `AccessPointArn` ou um perfil do IAM usando `FileSystemAccessRoleArn`, deverá definir esse parâmetro como `TLS1_2`.

Tipo: String

Valores Válidos: NONE | TLS1_2

Obrigatório: Não

[Subdirectory](#)

Especifica um caminho de montagem para seu sistema de arquivos do Amazon EFS. É aqui que DataSync lê ou grava dados em seu sistema de arquivos (dependendo se esse é um local de origem ou destino).

Por padrão, DataSync usa o diretório raiz (ou [ponto de acesso](#), se você fornecer um `usingAccessPointArn`). Você também pode incluir subdiretórios usando barras (por exemplo, `/path/to/folder`).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obrigatório: Não

[Tags](#)

Especifica o par de chave-valor que representa uma etiqueta que você deseja adicionar ao recurso. O valor pode ser uma string vazia. Esse valor ajuda você a gerenciar, filtrar e pesquisar seus recursos. Recomendamos que você crie uma tag de nome para a sua localização.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

Sintaxe da Resposta

```
{  
  "LocationArn": "string"  
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

LocationArn

O nome de recurso da Amazon (ARN) do local do sistema de arquivos do Amazon EFS que você criar.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo de solicitação

O exemplo a seguir cria um local para um sistema de arquivos do Amazon EFS.

```
{
  "Ec2Config": {
    "SubnetArn": "arn:aws:ec2:us-east-2:11122233344:subnet/
subnet-1234567890abcdef1",
    "SecurityGroupArns": [
      "arn:aws:ec2:us-east-2:11122233344:security-group/sg-1234567890abcdef2"
    ]
  },
  "EfsFileSystemArn": "arn:aws:elasticfilesystem:us-east-2:111222333444:file-system/
fs-021345abcdef6789",
  "Subdirectory": "/mount/path",
  "Tags": [{
    "Key": "Name",
    "Value": "ElasticFileSystem-1"
  }]
}
```

Solicitação de amostra: criar um local para um sistema de arquivos restrito do Amazon EFS

O exemplo a seguir cria um local para um sistema de arquivos do Amazon EFS configurado para acesso restrito. Nesse tipo de cenário, talvez você precise especificar valores para `AccessPointArn`, `FileSystemAccessRoleArn` e `InTransitEncryption` na sua solicitação.

```
{
  "AccessPointArn": "arn:aws:elasticfilesystem:us-east-2:111222333444:access-point/
fsap-1234567890abcdef0",
  "Ec2Config": {
    "SubnetArn": "arn:aws:ec2:us-east-2:111222333444:subnet/
subnet-1234567890abcdef1",
    "SecurityGroupArns": [
      "arn:aws:ec2:us-east-2:111222333444:security-group/sg-1234567890abcdef2"
    ]
  },
  "FileSystemAccessRoleArn": "arn:aws:iam::111222333444:role/
AwsDataSyncFullAccessNew",
  "InTransitEncryption": "TLS1_2",
}
```

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-
abcdef01234567890",
  "LocationUri": "efs://us-east-2.fs-021345abcdef6789/",
  "Subdirectory": "/mount/path",
  "Tags": [{
    "Key": "Name",
    "Value": "ElasticFileSystem-1"
  }]
}
```

Resposta da amostra

Uma resposta retorna o ARN de localização do sistema de arquivos do Amazon EFS.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-12abcdef012345678"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationFsxLustre

Cria um local de transferência para um sistema de arquivos Amazon FSx for Lustre. AWS DataSync pode usar esse local como origem ou destino para transferir dados.

Antes de começar, certifique-se de entender como DataSync [acessar os sistemas FSx de arquivos Lustre](#).

Sintaxe da Solicitação

```
{
  "FsxFilesystemArn": "string",
  "SecurityGroupArns": [ "string" ],
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[FsxFilesystemArn](#)

Especifica o Amazon Resource Name (ARN) do sistema de FSx arquivos for Lustre.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

Exigido: Sim

SecurityGroupArns

Especifica os nomes de recursos da Amazon (ARNs) de até cinco grupos de segurança que fornecem acesso ao seu sistema de arquivos FSx for Lustre.

Os grupos de segurança devem conseguir acessar as portas do sistema de arquivos. O sistema de arquivos também deve permitir o acesso a partir dos grupos de segurança. Para obter informações sobre o acesso ao sistema de arquivos, consulte o [Guia do usuário do Amazon FSx for Lustre](#).

Tipo: matriz de strings

Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Exigido: Sim

Subdirectory

Especifica um caminho de montagem para seu sistema de arquivos FSx for Lustre. O caminho pode incluir subdiretórios.

Quando o local é usado como fonte, DataSync lê os dados do caminho de montagem. Quando o local é usado como destino, DataSync grava dados no caminho de montagem. Se você não incluir esse parâmetro, DataSync usa o diretório raiz do sistema de arquivos (/).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\+\.\(\)\$\p{Zs}]+$`

Obrigatório: Não

Tags

Especifica rótulos que ajudam você a categorizar, filtrar e pesquisar seus recursos da AWS . Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

Sintaxe da Resposta

```
{  
  "LocationArn": "string"  
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[LocationArn](#)

O Amazon Resource Name (ARN) da localização do sistema de arquivos FSx for Lustre que você criou.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationFsxOntap

Cria um local de transferência para um sistema de arquivos Amazon FSx for NetApp ONTAP. AWS DataSync pode usar esse local como origem ou destino para transferir dados.

Antes de começar, certifique-se de entender como DataSync [acessar os sistemas FSx de arquivos ONTAP](#).

Sintaxe da Solicitação

```
{
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "SecurityGroupArns": [ "string" ],
  "StorageVirtualMachineArn": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

Protocol

Especifica o protocolo de transferência de dados AWS DataSync usado para acessar seu sistema de FSx arquivos da Amazon.

Tipo: objeto [FsxProtocol](#)

Obrigatório: Sim

SecurityGroupArns

Especifica os grupos de EC2 segurança da Amazon que fornecem acesso à sub-rede preferencial do seu sistema de arquivos.

Os grupos de segurança devem permitir tráfego de saída nas seguintes portas (dependendo do protocolo em uso):

- Sistema de arquivos de rede (NFS): portas TCP 111, 635 e 2049
- Server Message Block (SMB): porta TCP 445

Os grupos de segurança do seu sistema de arquivos também devem permitir tráfego de entrada na mesma porta.

Tipo: matriz de strings

Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Exigido: Sim

StorageVirtualMachineArn

Especifica o ARN da máquina virtual de armazenamento (SVM) no sistema de arquivos para o qual e do qual você copia dados.

Tipo: String

Restrições de tamanho: tamanho máximo de 162.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:storage-virtual-machine/fs-[0-9a-f]+/svm-[0-9a-f]{17,}$`

Exigido: Sim

Subdirectory

Especifica um caminho para o compartilhamento de arquivos no SVM para o qual você deseja transferir dados de ou para.

Você pode especificar um caminho de união (também conhecido como ponto de montagem), caminho qtree (para compartilhamentos de arquivos NFS) ou nome de compartilhamento (para compartilhamentos de arquivos SMB). Por exemplo, seu caminho de montagem pode ser /vol1, /vol1/tree1 ou /share1.

Note

Não especifique um caminho de junção no volume raiz do SVM. Para obter mais informações, consulte [Gerenciamento FSx de máquinas virtuais de armazenamento ONTAP no Guia](#) do usuário do Amazon FSx for NetApp ONTAP.

Tipo: String

Restrições de tamanho: tamanho máximo de 255.

Padrão: `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

Obrigatório: Não

Tags

Especifica rótulos que ajudam você a categorizar, filtrar e pesquisar seus recursos da AWS . Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

Sintaxe da Resposta

```
{  
  "LocationArn": "string"
```

```
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

LocationArn

Especifica o ARN da localização FSx do sistema de arquivos for ONTAP que você cria.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)

- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationFsxOpenZfs

Cria um local de transferência para um sistema de arquivos Amazon FSx for OpenZFS. AWS DataSync pode usar esse local como origem ou destino para transferir dados.

Antes de começar, certifique-se de entender como DataSync [acessar os sistemas FSx de arquivos OpenZFS](#).

Note

Os parâmetros de solicitação relacionados a SMB não são compatíveis com a operação CreateLocationFsxOpenZfs.

Sintaxe da Solicitação

```
{
  "FsxFilesystemArn": "string",
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "SecurityGroupArns": [ "string" ],
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

```
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[FsxFilesystemArn](#)

O Amazon Resource Name (ARN) do sistema de arquivos FSx for OpenZFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

Exigido: Sim

[Protocol](#)

O tipo de protocolo AWS DataSync usado para acessar seu sistema de arquivos.

Tipo: objeto [FsxProtocol](#)

Obrigatório: Sim

[SecurityGroupArns](#)

Os grupos ARNs de segurança usados para configurar o sistema de arquivos FSx para OpenZFS.

Tipo: matriz de strings

Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Exigido: Sim

[Subdirectory](#)

Um subdiretório no caminho do local que deve começar com /fsx. DataSync usa esse subdiretório para ler ou gravar dados (dependendo se o sistema de arquivos é um local de origem ou destino).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[^\u0000\u0085\u2028\u2029\r\n]{1,4096}$`

Obrigatório: Não

[Tags](#)

O par de chave-valor que representa uma tag que você deseja adicionar ao recurso. O valor pode ser uma string vazia. Esse valor ajuda você a gerenciar, filtrar e pesquisar seus recursos. Recomendamos que você crie uma tag de nome para a sua localização.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

Sintaxe da Resposta

```
{
  "LocationArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[LocationArn](#)

O ARN da localização do sistema de arquivos FSx para OpenZFS que você criou.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

CreateLocationFsxWindows

Cria um local de transferência para um sistema de arquivos Amazon FSx for Windows File Server. AWS DataSync pode usar esse local como origem ou destino para transferir dados.

Antes de começar, certifique-se de entender como DataSync [acessar os sistemas FSx de arquivos do Windows File Server](#).

Sintaxe da Solicitação

```
{
  "Domain": "string",
  "FsxFilesystemArn": "string",
  "Password": "string",
  "SecurityGroupArns": [ "string" ],
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "User": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

Domain

Especifica o nome do domínio do Windows ao qual o sistema FSx de arquivos do Windows File Server pertence.

Se você tiver vários domínios do Active Directory em seu ambiente, a configuração desse parâmetro garante que ele DataSync se conecte ao sistema de arquivos correto.

Tipo: String

Restrições de tamanho: tamanho máximo de 253.

Padrão: `^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}$`

Obrigatório: Não

FsxFilesystemArn

Especifica o Amazon Resource Name (ARN) para FSx o sistema de arquivos do Windows File Server.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

Exigido: Sim

Password

Especifica a senha do usuário com as permissões para montar e acessar os arquivos, pastas e metadados de arquivos no seu FSx sistema de arquivos do Windows File Server.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^\.{0,104}$`

Exigido: Sim

SecurityGroupArns

Especifica os grupos ARNs de EC2 segurança da Amazon que fornecem acesso à sub-rede preferencial do seu sistema de arquivos.

Os grupos de segurança que você especificar devem ser capazes de se comunicar com os grupos de segurança do seu sistema de arquivos. Para obter informações sobre a configuração de grupos de segurança para acesso ao sistema de arquivos, consulte o [Guia do usuário do Amazon FSx para Windows File Server](#).

Note

Se você escolher um grupo de segurança que não permite conexões de dentro de si mesmo, siga um destes procedimentos:

- Configure o grupo de segurança para permitir que ele se comunique dentro de si próprio.
- Escolha outro grupo de segurança diferente que possa se comunicar com o grupo de segurança do destino de montagem.

Tipo: Matriz de strings

Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Exigido: Sim

Subdirectory

Especifica um caminho de montagem para seu sistema de arquivos usando barras. É aqui que DataSync lê ou grava dados (dependendo se esse é um local de origem ou destino).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\+\.\^(\)\$\\p{Zs}]+$`

Obrigatório: Não

Tags

Especifica rótulos que ajudam você a categorizar, filtrar e pesquisar seus recursos da AWS . Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

User

Especifica o usuário com as permissões para montar e acessar os arquivos, pastas e metadados de arquivos no seu FSx sistema de arquivos do Windows File Server.

Para obter informações sobre como escolher um usuário com o nível certo de acesso para sua transferência, consulte [as permissões necessárias](#) FSx para locais do Windows File Server.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^[^\\x22\\x5B\\x5D\\/\\:;|=, +*?\\x3C\\x3E]{1,104}$`

Exigido: Sim

Sintaxe da Resposta

```
{
  "LocationArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[LocationArn](#)

O ARN da localização do sistema FSx de arquivos do Windows File Server que você criou.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationHdfs

Cria um local de transferência para um Hadoop Distributed File System (HDFS). AWS DataSync pode usar esse local como origem ou destino para transferir dados.

Antes de começar, certifique-se de entender como DataSync [acessa os clusters do HDFS](#).

Sintaxe da Solicitação

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "BlockSize": number,
  "KerberosKeytab": blob,
  "KerberosKrb5Conf": blob,
  "KerberosPrincipal": "string",
  "KmsKeyProviderUri": "string",
  "NameNodes": [
    {
      "Hostname": "string",
      "Port": number
    }
  ],
  "QopConfiguration": {
    "DataTransferProtection": "string",
    "RpcProtection": "string"
  },
  "ReplicationFactor": number,
  "SimpleUser": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AgentArns](#)

Os nomes de recursos da Amazon (ARNs) dos DataSync agentes que podem se conectar ao seu cluster HDFS.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Exigido: Sim

[AuthenticationType](#)

O tipo de autenticação usado para determinar a identidade do usuário.

Tipo: String

Valores Válidos: SIMPLE | KERBEROS

Obrigatório: Sim

[BlockSize](#)

O tamanho dos blocos de dados a serem gravados no cluster do HDFS. O tamanho deve ser um múltiplo de 512 bytes. O tamanho padrão do bloco é 128 mebibytes (MiB).

Tipo: inteiro

Intervalo válido: valor mínimo de 1.048.576. Valor máximo de 1.073.741.824

Obrigatório: Não

[KerberosKeytab](#)

A tabela de chaves Kerberos (keytab) que contém mapeamentos entre a entidade principal Kerberos definida e as chaves criptografadas. Você pode carregar o keytab de um arquivo fornecendo o endereço do arquivo.

 Note

Se KERBEROS for especificado para `AuthenticationType`, esse parâmetro será obrigatório.

Tipo: objeto de dados binários codificado pelo Base64

Restrições de tamanho: tamanho máximo de 65536.

Obrigatório: Não

KerberosKrb5Conf

O arquivo `krb5.conf` que contém as informações de configuração do Kerberos. Você pode carregar o arquivo `krb5.conf` fornecendo o endereço do arquivo. Se você estiver usando o AWS CLI, ele executa a codificação base64 para você. Caso contrário, você deve fornecer o texto codificado em base64.

 Note

Se KERBEROS for especificado para `AuthenticationType`, esse parâmetro será obrigatório.

Tipo: objeto de dados binários codificado pelo Base64

Restrições de tamanho: tamanho máximo de 131.072.

Obrigatório: Não

KerberosPrincipal

A entidade principal do Kerberos com acesso aos arquivos e pastas no cluster do HDFS.

 Note

Se KERBEROS for especificado para `AuthenticationType`, esse parâmetro será obrigatório.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^.+`

Obrigatório: Não

[KmsKeyProviderUri](#)

O URI do Key Management Server (KMS) do cluster do HDFS.

Tipo: String

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 255.

Padrão: `^kms:\\\\http[s]?@(([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9])(;(([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9]))*:[0-9]{1,5}\\kms$`

Obrigatório: Não

[NameNodes](#)

O NameNode que gerencia o namespace HDFS. O NameNode executa operações como abrir, fechar e renomear arquivos e diretórios. O NameNode contém as informações para mapear blocos de dados para DataNodes o. Você pode usar apenas um NameNode.

Tipo: Matriz de objetos [HdfsNameNode](#)

Membros da matriz: número mínimo de 1 item.

Obrigatório: Sim

[QopConfiguration](#)

A configuração da Qualidade da Proteção (QOP) especifica as configurações de privacidade da Chamada de Procedimento Remoto (RPC) e das configurações de proteção de transferência de dados definidas no cluster do Hadoop Distributed File System (HDFS). Se `QopConfiguration` não for especificado, `RpcProtection` e `DataTransferProtection` assumirão `PRIVACY` como padrão. Se você definir `RpcProtection` ou `DataTransferProtection`, o outro parâmetro assumirá o mesmo valor.

Tipo: objeto [QopConfiguration](#)

Obrigatório: Não

ReplicationFactor

O número de DataNodes para os quais replicar os dados ao gravar no cluster HDFS. Por padrão, os dados são replicados para três DataNodes.

Tipo: inteiro

Intervalo válido: valor mínimo de 1. Valor máximo de 512.

Obrigatório: Não

SimpleUser

O nome de usuário utilizado para identificar o cliente no sistema operacional host.

Note

Se SIMPLE for especificado para `AuthenticationType`, esse parâmetro será obrigatório.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^[_.A-Za-z0-9][_.A-Za-z0-9]*$`

Obrigatório: Não

Subdirectory

Um subdiretório no cluster do HDFS. Esse subdiretório é utilizado para ler ou gravar dados no cluster do HDFS. Se o subdiretório não for especificado, o padrão será `/`.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\\-\\+\\.\\/(\\)\\$\\p{Zs}]+$`

Obrigatório: Não

Tags

O par de chave-valor que representa a tag que você deseja adicionar ao local. O valor pode ser uma string vazia. Recomendamos usar tags para nomear os recursos.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

Sintaxe da Resposta

```
{
  "LocationArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[LocationArn](#)

O ARN do local do cluster de origem do HDFS que você criou.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationNfs

Cria um local de transferência para um servidor de arquivos do Network File System (NFS). AWS DataSync pode usar esse local como origem ou destino para transferir dados.

Antes de começar, certifique-se de entender como DataSync [acessa os servidores de arquivos NFS](#).

Sintaxe da Solicitação

```
{
  "MountOptions": {
    "Version": "string"
  },
  "OnPremConfig": {
    "AgentArns": [ "string" ]
  },
  "ServerHostname": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[MountOptions](#)

Especifica as opções que DataSync podem ser usadas para montar seu servidor de arquivos NFS.

Tipo: objeto [NfsMountOptions](#)

Obrigatório: Não

OnPremConfig

Especifica o Amazon Resource Name (ARN) do DataSync agente que pode se conectar ao seu servidor de arquivos NFS.

Você pode especificar mais de um atendente. Para obter mais informações, consulte [Uso de vários DataSync agentes](#).

Tipo: objeto [OnPremConfig](#)

Obrigatório: Sim

ServerHostname

Especifica o nome DNS ou o endereço IP versão 4 do servidor de arquivos NFS ao qual seu DataSync agente se conecta.

Tipo: String

Restrições de tamanho: tamanho máximo de 255.

Padrão: `^([a-zA-Z0-9\-\.]*[a-zA-Z0-9])\.([A-Za-z0-9\-\:]*[A-Za-z0-9])$`

Exigido: Sim

Subdirectory

Especifica o caminho de exportação no servidor de arquivos NFS que você deseja DataSync montar.

Esse caminho (ou um subdiretório do caminho) é onde os dados são DataSync transferidos de ou para. Para obter informações sobre como configurar uma exportação para DataSync, consulte [Acessando servidores de arquivos NFS](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\+\.\^(\)\p{Zs}]+$`

Exigido: Sim

Tags

Especifica rótulos que ajudam você a categorizar, filtrar e pesquisar seus AWS recursos. Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

Sintaxe da Resposta

```
{  
  "LocationArn": "string"  
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[LocationArn](#)

O ARN do local de transferência que você criou para seu servidor de arquivos NFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo

O exemplo a seguir cria um local DataSync de transferência para um servidor de arquivos NFS.

Exemplo de solicitação

```
{
  "MountOptions": {
    "Version": : "NFS4_0"
  },
  "OnPremConfig": {
    "AgentArn": [ "arn:aws:datasync:us-east-2:111222333444:agent/
agent-0b0addbeef44b3nfs" ]
  },

  "ServerHostname": "MyServer@amazon.com",
  "Subdirectory": "/MyFolder",
  "Tags": [
    {
      "Key": "Name",
      "Value": "FileSystem-1"
    }
  ]
}
```

Exemplo

A resposta retorna o ARN do local do NFS.

Resposta da amostra

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
```

```
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationObjectStorage

Cria um local de transferência para um sistema de armazenamento de objetos. AWS DataSync pode usar esse local como origem ou destino para transferir dados. Você pode fazer transferências com ou sem um [DataSyncagente](#).

Antes de começar, certifique-se de compreender os [pré-requisitos](#) para trabalhar com sistemas de DataSync armazenamento de objetos.

Sintaxe da Solicitação

```
{
  "AccessKey": "string",
  "AgentArns": [ "string" ],
  "BucketName": "string",
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "SecretKey": "string",
  "ServerCertificate": blob,
  "ServerHostname": "string",
  "ServerPort": number,
  "ServerProtocol": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

AccessKey

Especifica a chave de acesso (por exemplo, um nome de usuário) se as credenciais forem necessárias para autenticação no servidor de armazenamento de objetos.

Tipo: String

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 200.

Padrão: `^.*$`

Obrigatório: Não

AgentArns

(Opcional) Especifica os nomes de recursos da Amazon (ARNs) dos DataSync agentes que podem se conectar ao seu sistema de armazenamento de objetos. Se você estiver configurando uma transferência entre nuvens sem agente, não precisará especificar um valor para esse parâmetro.

Note

Certifique-se de configurar esse parâmetro corretamente ao criar seu local de armazenamento pela primeira vez. Você não pode adicionar ou remover agentes de um local de armazenamento depois de criá-lo.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obrigatório: Não

BucketName

Especifica o nome do bucket de armazenamento de objetos envolvido na transferência.

Tipo: String

Restrições de tamanho: comprimento mínimo de 3. Tamanho máximo de 63.

Padrão: `^[a-zA-Z0-9_\-\.\\(\)\$\p{Zs}]+$`

Exigido: Sim

[CmkSecretConfig](#)

Especifica as informações de configuração de um segredo DataSync gerenciado, que inclui o `SecretKey` que é DataSync usado para acessar um local específico de armazenamento de objetos, com um gerenciado pelo cliente. AWS KMS key

Ao incluir esse parâmetro como parte de uma `CreateLocationObjectStorage` solicitação, você fornece somente o ARN da chave KMS. DataSync usa essa chave KMS junto com o valor que você especifica para o `SecretKey` parâmetro para criar um segredo DataSync gerenciado para armazenar as credenciais de acesso à localização.

Verifique se DataSync ele tem permissão para acessar a chave KMS especificada.

Note

Você pode usar `CmkSecretConfig` (com `SecretKey`) ou `CustomSecretConfig` (sem `SecretKey`) para fornecer credenciais para uma `CreateLocationObjectStorage` solicitação. Não forneça os dois parâmetros para a mesma solicitação.

Tipo: objeto [CmkSecretConfig](#)

Obrigatório: Não

[CustomSecretConfig](#)

Especifica as informações de configuração para um segredo do Secrets Manager gerenciado pelo cliente, em que a chave secreta de um local específico de armazenamento de objetos é armazenada em texto sem formatação. Essa configuração inclui o ARN secreto e o ARN de uma função do IAM que fornece acesso ao segredo.

Note

Você pode usar `CmkSecretConfig` (com `SecretKey`) ou `CustomSecretConfig` (sem `SecretKey`) para fornecer credenciais para uma

CreateLocationObjectStorage solicitação. Não forneça os dois parâmetros para a mesma solicitação.

Tipo: objeto [CustomSecretConfig](#)

Obrigatório: Não

[SecretKey](#)

Especifica a chave secreta (por exemplo, uma senha) se as credenciais forem necessárias para autenticação no servidor de armazenamento de objetos.

Note

Se você fornecer um segredo usando `SecretKey`, mas não fornecer detalhes de configuração secreta usando `CmkSecretConfig` ou `CustomSecretConfig`, então DataSync armazena o token usando o segredo do Secrets Manager da sua AWS conta.

Tipo: String

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 200.

Padrão: `^.*$`

Obrigatório: Não

[ServerCertificate](#)

Especifica uma cadeia de certificados DataSync para autenticação em seu sistema de armazenamento de objetos se o sistema usar uma autoridade de certificação (CA) privada ou autoassinada. Você deve especificar um único arquivo `.pem` com uma cadeia de certificados completa (por exemplo, `file:///home/user/.ssh/object_storage_certificates.pem`).

A cadeia de certificados pode incluir:

- O certificado do sistema de armazenamento de objetos
- Todos os certificados intermediários (se for o caso)
- O certificado-raiz da CA assinante

Você pode concatenar os certificados em um arquivo .pem (que pode ter até 32.768 bytes antes da codificação base64). O exemplo de comando cat a seguir cria um arquivo `object_storage_certificates.pem` que inclui três certificados:

```
cat object_server_certificate.pem intermediate_certificate.pem  
ca_root_certificate.pem > object_storage_certificates.pem
```

Para usar esse parâmetro, configure `ServerProtocol` para HTTPS.

Tipo: objeto de dados binários codificado pelo Base64

Restrições de tamanho: tamanho máximo de 32768.

Obrigatório: Não

ServerHostname

Especifica o nome de domínio ou endereço IP versão 4 (IPv4) do servidor de armazenamento de objetos ao qual seu DataSync agente se conecta.

Tipo: String

Restrições de tamanho: tamanho máximo de 255.

Padrão: `^(([a-zA-Z0-9\-\ ]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-\ :]*[A-Za-z0-9])$`

Exigido: Sim

ServerPort

Especifica a porta em que o servidor de armazenamento de objetos aceita o tráfego de rede de entrada (por exemplo, a porta 443).

Tipo: inteiro

Intervalo válido: valor mínimo de 1. Valor máximo de 65536.

Obrigatório: Não

ServerProtocol

Especifica o protocolo que o servidor de armazenamento de objetos utiliza para se comunicar. Se não for especificado, o valor padrão será HTTPS.

Tipo: String

Valores Válidos: HTTPS | HTTP

Obrigatório: Não

[Subdirectory](#)

Especifica o prefixo de objeto do servidor de armazenamento de objetos. Se esse for um local de origem, DataSync copiará somente objetos com esse prefixo. Se esse for um local de destino, DataSync grava todos os objetos com esse prefixo.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_-\.\/\(\)\p{Zs}]*$`

Obrigatório: Não

[Tags](#)

Especifica o par de chave-valor que representa uma etiqueta que você deseja adicionar ao recurso. Tags ajudam a gerenciar, filtrar e procurar recursos. Recomendamos criar uma etiqueta de nome para a sua localização.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

Sintaxe da Resposta

```
{  
  "LocationArn": "string"  
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

LocationArn

Especifica o ARN da localização do sistema de armazenamento de objetos que você cria.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)

- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationS3

Cria um local de transferência para um bucket do Amazon S3. O AWS DataSync pode usar esse local como origem ou destino para transferência de dados.

Important

Antes de começar, não deixe de ler os seguintes tópicos:

- [Considerações sobre a classe de armazenamento com locais do Amazon S3](#)
- [Avaliando os custos de solicitação do S3 ao usar DataSync](#)

Para obter mais informações, consulte [Configurar transferências com o Amazon S3](#).

Sintaxe da Solicitação

```
{
  "AgentArns": [ "string" ],
  "S3BucketArn": "string",
  "S3Config": {
    "BucketAccessRoleArn": "string"
  },
  "S3StorageClass": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

AgentArns

(Somente Amazon S3 em Outposts) Especifica o Amazon Resource Name (ARN) do agente em seu Outpost. DataSync

Para obter mais informações, consulte [Implantar seu DataSync agente em AWS Outposts](#).

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obrigatório: Não

S3BucketArn

Especifica o ARN do bucket do S3 que você deseja usar como um local. (Ao criar sua DataSync tarefa posteriormente, você especifica se esse local é uma origem ou um destino de transferência.)

Se seu bucket do S3 estiver localizado em um AWS Outposts recurso, você deverá especificar um ponto de acesso do Amazon S3. Para obter mais informações, consulte [Gerenciando o acesso a dados com o recurso Pontos de Acesso Amazon S3](#) no Guia do usuário do Amazon S3.

Tipo: String

Restrições de comprimento: comprimento máximo de 268.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:[a-z\-\0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3-outposts:[a-z\-\0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-\-]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-\-]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9\-\-]{1,255}$`

Exigido: Sim

S3Config

Especifica o Amazon Resource Name (ARN) AWS Identity and Access Management da função DataSync (IAM) usada para acessar seu bucket do S3.

Para obter mais informações, consulte [Fornecendo DataSync acesso aos buckets do S3](#).

Tipo: objeto [S3Config](#)

Obrigatório: Sim

[S3StorageClass](#)

Especifica a classe de armazenamento que você deseja que seus objetos usem quando o Amazon S3 for um destino de transferência.

Para buckets em Regiões da AWS, o padrão da classe de armazenamento é. STANDARD Para buckets ativados AWS Outposts, o padrão da classe de armazenamento é. OUTPOSTS

Para obter mais informações, consulte [Considerações sobre classes de armazenamento com transferências do Amazon S3](#).

Tipo: String

Valores Válidos: STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL

Obrigatório: Não

[Subdirectory](#)

Especifica um prefixo no bucket do S3 que DataSync lê ou grava (dependendo se o bucket é um local de origem ou destino).

Note

DataSync não é possível transferir objetos com um prefixo que comece com uma barra (/) ou inclua ///./, ou /../ padrões. Por exemplo:

- /photos
- photos//2006/January
- photos/./2006/February
- photos/../2006/March

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obrigatório: Não

Tags

Especifica rótulos que ajudam você a categorizar, filtrar e pesquisar seus AWS recursos. Recomendamos criar pelo menos uma etiqueta de nome para seu local de transferência.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

Sintaxe da Resposta

```
{
  "LocationArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[LocationArn](#)

O ARN do local do S3 que você criou.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-zA-Z0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Etapa 1. Permitir que assuma o perfil do IAM necessário para gravar no bucket

O exemplo a seguir mostra a política mais simples que concede as permissões necessárias AWS DataSync para acessar um bucket Amazon S3 de destino, seguida por uma função do IAM à qual a `create-location-s3-iam-role` política foi anexada.

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

```
"Role": {
  "Path": "/",
  "RoleName": "amzn-s3-demo-bucket-access-role",
  "RoleId": "role-id",
  "Arn": "arn:aws:iam::account-id:role/amzn-s3-demo-bucket-access-role",
  "CreateDate": "2018-07-27T02:49:23.117Z",
  "AssumeRolePolicyDocument": {
    "Version": "2012-10-17",
    "Statement": [
```

```

    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datasync.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
}
}

```

Etapa 2. Permita que o perfil do IAM criado escreva no bucket

Associe uma política que tenha permissões suficientes para acessar o bucket ao perfil. Um exemplo dessa política é a política gerenciada `AWSDataSyncFullAccess`.

Para obter mais informações, consulte [AWSDataSyncFullAccess](#) no console do IAM.

Você não precisa criar essa política. Ele é gerenciado por AWS, então tudo o que você precisa fazer é especificar seu ARN no `attach-role-policy` comando.

```
IAM_POLICY_ARN='arn:aws:iam::aws:policy/AWSDataSyncFullAccess'
```

Etapa 3. Cria um endpoint para um bucket do Amazon S3

O exemplo a seguir cria um endpoint para um bucket do Amazon S3.

Quando o endpoint do S3 é criado, uma resposta semelhante ao segundo exemplo a seguir retorna o nome do recurso da Amazon (ARN) para a nova localização do Amazon S3.

Exemplo de solicitação

```

{
  "S3BucketArn": "arn:aws:s3:::amzn-s3-demo-bucket",
  "S3Config": {
    "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/amzn-s3-demo-bucket-access-role",
  },
  "S3StorageClass": "STANDARD",
  "Subdirectory": "/MyFolder",
  "Tags": [

```

```
{
  "Key": "Name",
  "Value": "s3Bucket-1"
}
```

Resposta da amostra

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateLocationSmb

Cria um local de transferência para um servidor de arquivos do Server Message Block (SMB). AWS DataSync pode usar esse local como origem ou destino para transferir dados.

Antes de começar, certifique-se de entender como DataSync acessa os servidores de arquivos SMB. Para obter mais informações, consulte [Fornecendo DataSync acesso a servidores de arquivos SMB](#).

Sintaxe da Solicitação

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "DnsIpAddresses": [ "string" ],
  "Domain": "string",
  "KerberosKeytab": blob,
  "KerberosKrb5Conf": blob,
  "KerberosPrincipal": "string",
  "MountOptions": {
    "Version": "string"
  },
  "Password": "string",
  "ServerHostname": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "User": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

AgentArns

Especifica o DataSync agente (ou agentes) que podem se conectar ao seu servidor de arquivos SMB. Você especifica um agente usando seu nome do recurso da Amazon (ARN).

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Exigido: Sim

AuthenticationType

Especifica o protocolo de autenticação DataSync usado para se conectar ao seu servidor de arquivos SMB. DataSync suporta NTLM (padrão) e KERBEROS autenticação.

Para obter mais informações, consulte [Fornecendo DataSync acesso a servidores de arquivos SMB](#).

Tipo: String

Valores Válidos: NTLM | KERBEROS

Obrigatório: Não

DnsIpAddresses

Especifica os IPv4 endereços dos servidores DNS aos quais seu servidor de arquivos SMB pertence. Esse parâmetro se aplica somente se `AuthenticationType` estiver definido como `KERBEROS`.

Se você tiver vários domínios em seu ambiente, a configuração desse parâmetro garante que ele se DataSync conecte ao servidor de arquivos SMB correto.

Tipo: matriz de strings

Membros da matriz: número máximo de 2 itens.

Restrições de comprimento: comprimento mínimo de 7. Comprimento máximo de 39.

Padrão: \A((25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\.(25[0-5]|2[0-4]\d|[0-1]?\d?\d))){3}|([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-fA-F]{1,4}){1,6}))\z

Obrigatório: Não

Domain

Especifica o nome de domínio do Windows ao qual o servidor de arquivos SMB pertence. Esse parâmetro se aplica somente se `AuthenticationType` estiver definido como `NTLM`.

Se você tiver vários domínios em seu ambiente, a configuração desse parâmetro garante que ele se DataSync conecte ao servidor de arquivos correto.

Tipo: String

Restrições de tamanho: tamanho máximo de 253.

Padrão: ^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}\$

Obrigatório: Não

KerberosKeytab

Especifica seu arquivo de tabela de chaves Kerberos (keytab), que inclui mapeamentos entre suas chaves principais e de criptografia do Kerberos.

Para evitar erros de execução de tarefas, certifique-se de que o principal Kerberos que você usa para criar o arquivo keytab corresponda exatamente ao que você especificou.

`KerberosPrincipal`

Tipo: objeto de dados binários codificado pelo Base64

Restrições de tamanho: tamanho máximo de 65536.

Obrigatório: Não

KerberosKrb5Conf

Especifica um arquivo de configuração Kerberos (`krb5.conf`) que define sua configuração de região Kerberos.

O arquivo deve ser codificado em base64. Se você estiver usando o AWS CLI, a codificação é feita para você.

Tipo: Objeto de dados binários codificado em Base64

Restrições de tamanho: tamanho máximo de 131.072.

Obrigatório: Não

KerberosPrincipal

Especifica um kerberos principal, que é uma identidade em seu realm Kerberos que tem permissão para acessar os arquivos, pastas e metadados de arquivos em seu servidor de arquivos SMB.

Talvez pareça um diretor de Kerberos. `HOST/kerberosuser@MYDOMAIN.ORG`

Os nomes principais diferenciam maiúsculas de minúsculas. A execução da DataSync tarefa falhará se o principal que você especificar para esse parâmetro não corresponder exatamente ao principal usado para criar o arquivo keytab.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^.+`

Obrigatório: Não

MountOptions

Especifica a versão do protocolo SMB DataSync usada para acessar seu servidor de arquivos SMB.

Tipo: objeto [SmbMountOptions](#)

Obrigatório: Não

Password

Especifica a senha do usuário que pode montar o servidor de arquivos SMB e tenha permissão para acessar os arquivos e pastas envolvidos na sua transferência. Esse parâmetro se aplica somente se `AuthenticationType` estiver definido como `NTLM`.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^[0,104]$`

Obrigatório: Não

ServerHostname

Especifica o nome de domínio ou endereço IP do servidor de arquivos SMB ao qual seu DataSync agente se conecta.

Lembre-se do seguinte ao configurar esse parâmetro:

- Você não pode especificar um endereço IP versão 6 (IPv6).
- Se você estiver usando a autenticação Kerberos, deverá especificar um nome de domínio.

Tipo: String

Restrições de tamanho: tamanho máximo de 255.

Padrão: `^(( [a-zA-Z0-9\ - ]* [a-zA-Z0-9] )\ . )* ( [A-Za-z0-9\ - : ]* [A-Za-z0-9] )$`

Exigido: Sim

Subdirectory

Especifica o nome do compartilhamento exportado pelo seu servidor de arquivos SMB onde DataSync lerá ou gravará dados. Você pode incluir um subdiretório no caminho de compartilhamento (por exemplo, `/path/to/subdirectory`). Certifique-se de que outros clientes do SMB em sua rede também possam montar este caminho.

Para copiar todos os dados no subdiretório, DataSync deve ser capaz de montar o compartilhamento SMB e acessar todos os seus dados. Para obter mais informações, consulte [Fornecendo DataSync acesso a servidores de arquivos SMB](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\$\p{Zs}]+$`

Exigido: Sim

Tags

Especifica rótulos que ajudam você a categorizar, filtrar e pesquisar seus recursos da AWS . Recomendamos criar pelo menos uma etiqueta de nome para a sua localização.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

User

Especifica o usuário que pode montar e acessar os arquivos, pastas e metadados de arquivos no servidor de arquivos SMB. Esse parâmetro se aplica somente se `AuthenticationType` estiver definido como `NLM`.

Para obter informações sobre como escolher um usuário com o nível certo de acesso para sua transferência, consulte [Fornecendo DataSync acesso a servidores de arquivos SMB](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E ] { 1 , 104 } $`

Obrigatório: Não

Sintaxe da Resposta

```
{
  "LocationArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

LocationArn

O ARN do local no SMB criado por você.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo de solicitação

O exemplo a seguir cria um local para um servidor de arquivos SMB.

```
{
  "AgentArns": [
    "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44b3nfs",
    "arn:aws:datasync:us-east-2:111222333444:agent/agent-2345noo35nnee1123ovo3"
  ],
  "Domain": "AMAZON",
```

```
"MountOptions":{
  "Version":"SMB3"
},
"Password":"string",
"ServerHostname":"MyServer.amazon.com",
"Subdirectory":"share",
"Tags":[
  {
    "Key":"department",
    "Value":"finance"
  }
],
"User":"user-1"
}
```

Resposta da amostra

Uma resposta retorna o ARN do local do seu servidor de arquivos do SMB.

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:111222333444:location/
loc-0f01451b140b2af49"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

CreateTask

Configura uma tarefa de transferência, que define onde e como o AWS DataSync transfere os dados.

Uma tarefa inclui um local de origem, um local de destino e opções de transferência (como limites de largura de banda, agendamento etc.).

Important

Se você planeja transferir dados de ou para um local do Amazon S3, analise [como isso DataSync pode afetar as cobranças de suas solicitações do S3](#) e a [página de DataSync preços](#) antes de começar.

Sintaxe da Solicitação

```
{
  "CloudWatchLogGroupArn": "string",
  "DestinationLocationArn": "string",
  "Excludes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "Includes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "ManifestConfig": {
    "Action": "string",
    "Format": "string",
    "Source": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "ManifestObjectPath": "string",
        "ManifestObjectVersionId": "string",
        "S3BucketArn": "string"
      }
    }
  }
}
```



```

},
"Name": "string",
"Options": {
  "Atime": "string",
  "BytesPerSecond": number,
  "Gid": "string",
  "LogLevel": "string",
  "Mtime": "string",
  "ObjectTags": "string",
  "OverwriteMode": "string",
  "PosixPermissions": "string",
  "PreserveDeletedFiles": "string",
  "PreserveDevices": "string",
  "SecurityDescriptorCopyFlags": "string",
  "TaskQueueing": "string",
  "TransferMode": "string",
  "Uid": "string",
  "VerifyMode": "string"
},
"Schedule": {
  "ScheduleExpression": "string",
  "Status": "string"
},
"SourceLocationArn": "string",
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"TaskMode": "string",
"TaskReportConfig": {
  "Destination": {
    "S3": {
      "BucketAccessRoleArn": "string",
      "S3BucketArn": "string",
      "Subdirectory": "string"
    }
  },
  "ObjectVersionIds": "string",
  "OutputType": "string",
  "Overrides": {
    "Deleted": {
      "ReportLevel": "string"
    }
  }
}

```

```

    },
    "Skipped": {
      "ReportLevel": "string"
    },
    "Transferred": {
      "ReportLevel": "string"
    },
    "Verified": {
      "ReportLevel": "string"
    }
  },
  "ReportLevel": "string"
}

```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[CloudWatchLogGroupArn](#)

Especifica o Amazon Resource Name (ARN) de um grupo de logs da CloudWatch Amazon para monitorar sua tarefa.

Para tarefas do modo Avançado, você não precisa especificar nada. DataSync envia automaticamente os registros para um grupo de CloudWatch registros chamado `/aws/datasync`.

Para obter mais informações, consulte [Monitoramento de transferências de dados com o CloudWatch Logs](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 562.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-\0-9]+:[0-9]{12}:log-group:([^\:]*)(:\:)?$`

Obrigatório: Não

DestinationLocationArn

Especifica o ARN do local de destino da transferência.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Excludes

Especifica filtros de exclusão que definem os arquivos, objetos e pastas em seu local de origem que você não deseja DataSync transferir. Para obter mais informações e exemplos, consulte [Especificação do que é DataSync transferido usando filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

Obrigatório: Não

Includes

Especifica a inclusão de filtros que definem os arquivos, objetos e pastas no local de origem que você deseja DataSync transferir. Para obter mais informações e exemplos, consulte [Especificação do que é DataSync transferido usando filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

Obrigatório: Não

ManifestConfig

Configura um manifesto, que é uma lista de arquivos ou objetos que você deseja DataSync transferir. Para obter mais informações e exemplos de configuração, consulte [Especificação do que é DataSync transferido usando um manifesto](#).

Ao usar esse parâmetro, sua identidade de chamador (a função DataSync com a qual você está usando) deve ter a `iam:PassRole` permissão. A [AWSDataSyncFullAccess](#) política inclui essa permissão.

Tipo: objeto [ManifestConfig](#)

Obrigatório: Não

[Name](#)

Especifica o nome da tarefa.

Tipo: String

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\s+=. _:@/- ]+$`

Obrigatório: Não

[Options](#)

Especifica as configurações da tarefa, como preservar os metadados do arquivo, verificar a integridade dos dados, entre outras opções.

Tipo: objeto [Options](#)

Obrigatório: Não

[Schedule](#)

Especifica um agendamento de quando você deseja que a tarefa seja executada. Para obter mais informações, consulte [Programar sua tarefa](#).

Tipo: objeto [TaskSchedule](#)

Obrigatório: Não

[SourceLocationArn](#)

Especifica o ARN do local de origem da transferência.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Tags

Especifica as tags que você deseja aplicar à tarefa.

As tags são pares de valores-chave que ajudam você a gerenciar, filtrar e pesquisar seus DataSync recursos.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

TaskMode

Especifica um dos seguintes modos de tarefa para sua transferência de dados:

- **ENHANCED**- Transfira um número praticamente ilimitado de objetos com desempenho superior ao do modo Básico. As tarefas do modo aprimorado otimizam o processo de transferência de dados listando, preparando, transferindo e verificando os dados em paralelo. Atualmente, o modo aprimorado está disponível para transferências entre locais do Amazon S3, transferências entre Azure Blob e Amazon S3 sem um agente e transferências entre outras nuvens e o Amazon S3 sem um agente.



Note

Para criar uma tarefa no modo Avançado, a função do IAM que você usa para chamar a `CreateTask` operação precisa ter a `iam:CreateServiceLinkedRole` permissão.

- **BASIC**(padrão) - Transfira arquivos ou objetos entre o AWS armazenamento e todos os outros DataSync locais compatíveis. As tarefas do modo básico estão sujeitas a [cotas](#) no número de arquivos, objetos e diretórios em um conjunto de dados. O modo básico prepara, transfere e verifica os dados sequencialmente, tornando-o mais lento do que o modo Avançado para a maioria das cargas de trabalho.

Para obter mais informações, consulte [Entendendo as diferenças do modo de tarefa](#).

Tipo: String

Valores Válidos: BASIC | ENHANCED

Obrigatório: Não

[TaskReportConfig](#)

Especifica como você deseja configurar um relatório de tarefas, que fornece informações detalhadas sobre sua DataSync transferência. Para obter mais informações, consulte [Monitorando suas DataSync transferências com relatórios de tarefas](#).

Ao usar esse parâmetro, sua identidade de chamador (a função DataSync com a qual você está usando) deve ter a `iam:PassRole` permissão. A [AWSDataSyncFullAccess](#) política inclui essa permissão.

Tipo: objeto [TaskReportConfig](#)

Obrigatório: Não

Sintaxe da Resposta

```
{
  "TaskArn": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[TaskArn](#)

O nome do recurso da Amazon (ARN) da tarefa.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Solicitação de amostra para uma tarefa no modo Avançado

O exemplo a seguir cria uma DataSync tarefa que usa o modo Avançado.

Ao contrário da criação de tarefas no modo Básico, você não precisa especificar um grupo de CloudWatch registros da Amazon. Com as tarefas do modo Avançado, envia DataSync automaticamente os registros de tarefas para um grupo de registros chamado `/aws/datasync`. Se esse grupo de registros não existir no seu Região da AWS, DataSync criará o grupo de registros em seu nome ao criar a tarefa.

```
{
  "SourceLocationArn": "arn:aws:datasync:us-
east-1:111222333444:location/1111aaaa2222bbbb3",
  "DestinationLocationArn": "arn:aws:datasync:us-
east-1:111222333444:location/0000zzzz1111yyyy2",
  "Name": "My Enhanced mode task",
  "TaskMode": "ENHANCED",
  "Options": {
    "TransferMode": "CHANGED",
    "VerifyMode": "ONLY_FILES_TRANSFERRED",
    "ObjectTags": "PRESERVE",
    "LogLevel": "TRANSFER"
  }
}
```

Solicitação de amostra para uma tarefa do modo Básico

O exemplo a seguir cria uma DataSync tarefa que usa o modo Básico.

```
{
  "SourceLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-1111aaaa2222bbbb3",
  "DestinationLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-0000zzzz1111yyyy2",
  "Name": "My Basic mode task",
  "TaskMode": "BASIC",
  "Options": {
    "Atime": "BEST_EFFORT",
    "Gid": "NONE",
    "Mtime": "PRESERVE",
    "PosixPermissions": "PRESERVE",
    "PreserveDevices": "NONE",
    "PreserveDeletedFiles": "PRESERVE",
    "Uid": "NONE",
    "VerifyMode": "ONLY_FILES_TRANSFERRED"
  },
  "Schedule": {
    "ScheduleExpression": "0 12 ? * SUN,WED *"
  },
  "CloudWatchLogGroupArn": "arn:aws:logs:us-east-2:111222333444:log-group:/log-group-name:*",
  "Tags": [
    {
      "Key": "Name",
      "Value": "Migration-wave-1"
    }
  ]
}
```

Resposta da amostra

A resposta a seguir inclui o ARN de uma tarefa criada.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteAgent

Remove um recurso de AWS DataSync agente do seu Conta da AWS.

Lembre-se de que essa operação (que não pode ser desfeita) não remove a máquina virtual (VM) do agente ou a EC2 instância da Amazon do seu ambiente de armazenamento. Nas próximas etapas, você pode excluir a VM ou a instância do seu ambiente de armazenamento ou reutilizá-la para [ativar um novo agente](#).

Sintaxe da Solicitação

```
{  
  "AgentArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AgentArn](#)

O nome do recurso da Amazon (ARN) do agente a ser excluído. Use a `ListAgents` operação para retornar uma lista de agentes para sua conta Região da AWS e.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Exigido: Sim

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteLocation

Exclui um recurso de local de transferência de AWS DataSync.

Sintaxe da Solicitação

```
{  
  "LocationArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

O nome do recurso da Amazon (ARN) do local a ser removido.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DeleteTask

Exclui um recurso de tarefa de transferência de AWS DataSync.

Sintaxe da Solicitação

```
{  
  "TaskArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

TaskArn

Especifica o nome do recurso da Amazon (ARN) da tarefa que deseja excluir.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Exigido: Sim

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeAgent

Retorna informações sobre um AWS DataSync agente, como nome, tipo de endpoint de serviço e status.

Sintaxe da Solicitação

```
{  
  "AgentArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AgentArn](#)

Especifica o Amazon Resource Name (ARN) do agente sobre DataSync o qual você deseja obter informações.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{  
  "AgentArn": "string",  
  "CreationTime": number,  
  "EndpointType": "string",  
  "LastConnectionTime": number,  
  "Name": "string",  
  "Platform": {
```



```

    "Version": "string"
  },
  "PrivateLinkConfig": {
    "PrivateLinkEndpoint": "string",
    "SecurityGroupArns": [ "string" ],
    "SubnetArns": [ "string" ],
    "VpcEndpointId": "string"
  },
  "Status": "string"
}

```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[AgentArn](#)

O ARN do agente.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

[CreationTime](#)

A hora em que o agente foi [ativado](#).

Tipo: Timestamp

[EndpointType](#)

O tipo de [endpoint de serviço](#) ao qual seu agente está conectado.

Tipo: String

Valores Válidos: PUBLIC | PRIVATE_LINK | FIPS

[LastConnectionTime](#)

A última vez em que o agente estava se comunicando com o DataSync serviço.

Tipo: Timestamp

Name

O nome do agente.

Tipo: String

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\s+=. _:@/- ]+$`

Platform

Os detalhes relacionados à plataforma sobre o agente, como o número da versão.

Tipo: objeto [Platform](#)

PrivateLinkConfig

A configuração de rede que o agente usa ao se conectar a um [endpoint de serviço VPC](#).

Tipo: objeto [PrivateLinkConfig](#)

Status

O status do agente.

- Se o status for ONLINE, o agente está configurado corretamente e pronto para uso.
- Se o status for OFFLINE, o agente esteve fora de contato DataSync por cinco minutos ou mais. Isso pode acontecer por alguns motivos. Para obter mais informações, consulte [O que eu faço se meu agente estiver off-line?](#)

Tipo: String

Valores Válidos: ONLINE | OFFLINE

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

`InvalidRequestException`

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo de solicitação

O exemplo a seguir retorna informações sobre um agente especificado em uma solicitação.

```
{
  "AgentArn": "arn:aws:datasync:us-east-2:111122223333:agent/agent-1234567890abcdef0"
}
```

Resposta da amostra

O exemplo de resposta a seguir descreve um agente que usa um endpoint de serviço público.

```
{
  "AgentArn": "arn:aws:datasync:us-east-2:111122223333:agent/agent-1234567890abcdef0",
  "Name": "Data center migration agent",
  "Status": "ONLINE",
  "LastConnectionTime": "2022-10-17T17:21:35.540000+00:00",
  "CreationTime": "2022-10-05T20:52:29.499000+00:00",
  "EndpointType": "PUBLIC",
  "Platform": {
    "Version": "2"
  }
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)

- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationAzureBlob

Fornecer detalhes sobre como um local AWS DataSync de transferência para o Microsoft Azure Blob Storage é configurado.

Sintaxe da Solicitação

```
{  
  "LocationArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

Especifica o nome do recurso da Amazon (ARN) do local da transferência do armazenamento de blobs do Azure.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{  
  "AccessTier": "string",  
  "AgentArns": [ "string" ],  
  "AuthenticationType": "string",  
  "BlobType": "string",  
  "CmkSecretConfig": {
```

```

    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "CreationTime": number,
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "LocationArn": "string",
  "LocationUri": "string",
  "ManagedSecretConfig": {
    "SecretArn": "string"
  }
}

```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[AccessTier](#)

O nível de acesso para o qual você deseja que seus objetos ou arquivos sejam transferidos. Isso só se aplica ao usar o local como destino de transferência. Para obter mais informações, consulte [Níveis de acesso](#).

Tipo: String

Valores Válidos: HOT | COOL | ARCHIVE

[AgentArns](#)

Os ARNs DataSync agentes que podem se conectar ao seu contêiner do Azure Blob Storage.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

O método de autenticação DataSync usado para acessar seu Armazenamento de Blobs do Azure. DataSync pode acessar o armazenamento de blobs usando uma assinatura de acesso compartilhado (SAS).

Tipo: String

Valores Válidos: SAS | NONE

BlobType

O tipo de blob no qual você deseja que seus objetos ou arquivos estejam ao transferi-los para o armazenamento de blobs do Azure. Atualmente, DataSync só dá suporte à movimentação de dados para o Armazenamento de Blobs do Azure como blobs de blocos. Para obter mais informações sobre os tipos de blob, consulte a [Documentação do armazenamento de blobs do Azure](#).

Tipo: String

Valores Válidos: BLOCK

CmkSecretConfig

Descreve as informações de configuração DataSync de um segredo gerenciado, como um token de autenticação DataSync usado para acessar um local de armazenamento específico, com um gerenciado pelo cliente AWS KMS key.

Tipo: objeto [CmkSecretConfig](#)

CreationTime

A hora em que seu local de transferência do armazenamento de blobs do Azure foi criado.

Tipo: Timestamp

CustomSecretConfig

Descreve as informações de configuração de um segredo gerenciado pelo cliente, como um token de autenticação DataSync usado para acessar um local de armazenamento específico, com um gerenciado pelo cliente. AWS KMS key

Tipo: objeto [CustomSecretConfig](#)

[LocationArn](#)

O ARN do seu local de transferência do armazenamento de blobs do Azure.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

A URL do contêiner de armazenamento de blobs do Azure envolvido na sua transferência.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:\\-]+$`

[ManagedSecretConfig](#)

Descreve as informações de configuração DataSync de um segredo gerenciado, como um token de autenticação DataSync usado para acessar um local de armazenamento específico. DataSync usa a chave KMS AWS gerenciada padrão para criptografar esse segredo. AWS Secrets Manager

Tipo: objeto [ManagedSecretConfig](#)

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationEfs

Fornece detalhes sobre como um local AWS DataSync de transferência para um sistema de arquivos Amazon EFS é configurado.

Sintaxe da Solicitação

```
{  
  "LocationArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[LocationArn](#)

O nome do recurso da Amazon (ARN) do local do sistema de arquivos do Amazon EFS do qual você deseja obter informações.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{  
  "AccessPointArn": "string",  
  "CreationTime": number,  
  "Ec2Config": {  
    "SecurityGroupArns": [ "string" ],  
    "SubnetArn": "string"  
  }  
}
```

```
},  
"FileSystemAccessRoleArn": "string",  
"InTransitEncryption": "string",  
"LocationArn": "string",  
"LocationUri": "string"  
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AccessPointArn

O ARN do ponto de acesso DataSync usado para acessar o sistema de arquivos Amazon EFS.

Para obter mais informações, consulte [Acesso a sistemas de arquivos restritos](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: ^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-\0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}\$

CreationTime

O horário em que a localização foi criada.

Tipo: Timestamp

Ec2Config

A sub-rede e os grupos de segurança AWS DataSync usados para se conectar a um dos [destinos de montagem](#) do seu sistema de arquivos Amazon EFS.

Tipo: objeto [Ec2Config](#)

FileSystemAccessRoleArn

A função AWS Identity and Access Management (IAM) que permite DataSync acessar seu sistema de arquivos Amazon EFS.

Para obter mais informações, consulte [Criação de uma função DataSync do IAM para acesso ao sistema de arquivos](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

[InTransitEncryption](#)

Indica se DataSync usa criptografia Transport Layer Security (TLS) ao transferir dados para ou do sistema de arquivos Amazon EFS.

Tipo: String

Valores Válidos: NONE | TLS1_2

[LocationArn](#)

O ARN da localização do sistema de arquivos do Amazon EFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

O URL da localização do sistema de arquivos do Amazon EFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo de solicitação

O exemplo a seguir mostra como obter informações sobre um local do sistema de arquivos do Amazon EFS específico.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-12abcdef012345678"
}
```

Resposta da amostra

O exemplo a seguir retorna detalhes de localização de um sistema de arquivos do Amazon EFS.

```
{
  "CreationTime": 1653319021.353,
  "Ec2Config": {
    "SubnetArn": "arn:aws:ec2:us-east-2:111222333444:subnet/subnet-1234567890abcdef1",
    "SecurityGroupArns": [
      "arn:aws:ec2:us-east-2:111222333444:security-group/sg-1234567890abcdef2"
    ]
  },
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-abcdef01234567890",
  "LocationUri": "efs://us-east-2.fs-021345abcdef6789/"
}
```

Exemplo de resposta: descrevendo uma localização de um sistema de arquivos restrito do Amazon EFS

O exemplo a seguir retorna detalhes de localização sobre um sistema de arquivos do Amazon EFS com acesso restrito, incluindo os elementos `AccessPointArn`, `FileSystemAccessRoleArn` e `InTransitEncryption`.

```
{
  "CreationTime": 1653319021.353,
  "AccessPointArn": "arn:aws:elasticfilesystem:us-east-2:111222333444:access-point/
fsap-1234567890abcdef0",
  "Ec2Config": {
    "SubnetArn": "arn:aws:ec2:us-east-2:111222333444:subnet/
subnet-1234567890abcdef1",
    "SecurityGroupArns": [
      "arn:aws:ec2:us-east-2:111222333444:security-group/sg-1234567890abcdef2"
    ]
  },
  "FileSystemAccessRoleArn": "arn:aws:iam::111222333444:role/
AwsDataSyncFullAccessNew",
  "InTransitEncryption": "TLS1_2",
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-
abcdef01234567890",
  "LocationUri": "efs://us-east-2.fs-021345abcdef6789/",
  "Subdirectory": "/mount/path",
  "Tags": [{
    "Key": "Name",
    "Value": "ElasticFileSystem-1"
  }]
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationFsxLustre

Fornece detalhes sobre como um local AWS DataSync de transferência para um sistema de arquivos Amazon FSx for Lustre é configurado.

Sintaxe da Solicitação

```
{
  "LocationArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

O nome de recurso da Amazon (ARN) do local do FSx for Lustre a ser descrito.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{
  "CreationTime": number,
  "LocationArn": "string",
  "LocationUri": "string",
  "SecurityGroupArns": [ "string" ]
}
```


Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A hora em que o local FSx for Lustre foi criado.

Tipo: Timestamp

LocationArn

O Amazon Resource Name (ARN) do local do FSx for Lustre que foi descrito.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

O URI da localização do FSx for Lustre que foi descrita.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

SecurityGroupArns

Os Amazon Resource Names (ARNs) dos grupos de segurança configurados FSx para o sistema de arquivos for Lustre.

Tipo: matriz de strings

Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationFsxOntap

Fornece detalhes sobre como um local AWS DataSync de transferência para um sistema de arquivos Amazon FSx for NetApp ONTAP é configurado.

Note

Se sua localização usa SMB, a operação `DescribeLocationFsxOntap` não retorna realmente um `Password`.

Sintaxe da Solicitação

```
{  
  "LocationArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

Especifica o Amazon Resource Name (ARN) do local do sistema de arquivos ONTAP sobre FSx o qual você deseja obter informações.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{
```

```

"CreationTime": number,
"FsxFilesystemArn": "string",
"LocationArn": "string",
"LocationUri": "string",
"Protocol": {
  "NFS": {
    "MountOptions": {
      "Version": "string"
    }
  },
  "SMB": {
    "Domain": "string",
    "MountOptions": {
      "Version": "string"
    },
    "Password": "string",
    "User": "string"
  }
},
"SecurityGroupArns": [ "string" ],
"StorageVirtualMachineArn": "string"
}

```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

O horário em que a localização foi criada.

Tipo: Timestamp

FsxFilesystemArn

O ARN do sistema de arquivos FSx for ONTAP.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

[LocationArn](#)

O ARN da localização do sistema de arquivos FSx for ONTAP.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

O identificador uniforme de recursos (URI) da localização do sistema de arquivos FSx for ONTAP.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[Protocol](#)

Especifica o protocolo de transferência de dados AWS DataSync usado para acessar seu sistema de FSx arquivos da Amazon.

Tipo: objeto [FsxProtocol](#)

[SecurityGroupArns](#)

Os grupos de segurança DataSync usados para acessar seu FSx sistema de arquivos do ONTAP.

Tipo: matriz de strings

Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

[StorageVirtualMachineArn](#)

O ARN da máquina virtual de armazenamento (SVM) em seu sistema de arquivos FSx for ONTAP de onde você está copiando dados de ou para.

Tipo: String

Restrições de tamanho: tamanho máximo de 162.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]+:[0-9]{12}:storage-virtual-machine/fs-[0-9a-f]+/svm-[0-9a-f]{17,}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

DescribeLocationFsxOpenZfs

Fornece detalhes sobre como um local AWS DataSync de transferência para um sistema de arquivos Amazon FSx for OpenZFS é configurado.

Note

Os elementos de resposta relacionados a SMB não são compatíveis com a operação `DescribeLocationFsxOpenZfs`.

Sintaxe da Solicitação

```
{  
  "LocationArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

O nome de recurso da Amazon (ARN) do local do OpenZFS FSx a ser descrito.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{
```



```

"CreationTime": number,
"LocationArn": "string",
"LocationUri": "string",
"Protocol": {
  "NFS": {
    "MountOptions": {
      "Version": "string"
    }
  },
  "SMB": {
    "Domain": "string",
    "MountOptions": {
      "Version": "string"
    },
    "Password": "string",
    "User": "string"
  }
},
"SecurityGroupArns": [ "string" ]
}

```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

CreationTime

A hora em que o local FSx for OpenZFS foi criado.

Tipo: Timestamp

LocationArn

O ARN da localização do FSx OpenZFS que foi descrita.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

O identificador uniforme de recursos (URI) da localização do FSx OpenZFS que foi descrita.

Example: `fsxz://us-west-2.fs-1234567890abcdef02/fsx/folderA/folder`

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Protocol

O tipo de protocolo AWS DataSync usado para acessar seu sistema de arquivos.

Tipo: objeto [FsxProtocol](#)

SecurityGroupArns

Os grupos ARNs de segurança que estão configurados FSx para o sistema de arquivos do OpenZFS.

Tipo: matriz de strings

Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationFsxWindows

Fornece detalhes sobre como um local AWS DataSync de transferência para um sistema de arquivos Amazon FSx para Windows File Server é configurado.

Sintaxe da Solicitação

```
{
  "LocationArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[LocationArn](#)

Especifica o nome de recurso da Amazon (ARN) da localização FSx do servidor de arquivos para Windows.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{
  "CreationTime": number,
  "Domain": "string",
  "LocationArn": "string",
  "LocationUri": "string",
  "SecurityGroupArns": [ "string" ],
  "User": "string"
}
```

```
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[CreationTime](#)

A hora em que o FSx local do servidor de arquivos do Windows foi criado.

Tipo: Timestamp

[Domain](#)

O nome do domínio do Microsoft Active Directory ao qual pertence o FSx sistema de arquivos do Windows File Server.

Tipo: String

Restrições de tamanho: tamanho máximo de 253.

Padrão: `^[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}$`

[LocationArn](#)

O ARN da localização do servidor FSx de arquivos do Windows.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

O identificador uniforme de recursos (URI) do FSx local do Windows File Server.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\\-]+$`

SecurityGroupArns

Os grupos ARNs de EC2 segurança da Amazon que fornecem acesso à sub-rede preferencial do seu sistema de arquivos.

Para obter informações sobre a configuração de grupos de segurança para acesso ao sistema de arquivos, consulte o [Guia do usuário do Amazon FSx para Windows File Server](#).

Tipo: matriz de strings

Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

User

O usuário com as permissões para montar e acessar o sistema FSx de arquivos do Windows File Server.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^[^\x22\x5B\x5D\/\\:;|=, +*?\x3C\x3E]{1,104}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationHdfs

Fornecer detalhes sobre como um local de AWS DataSync transferência para um Hadoop Distributed File System (HDFS) é configurado.

Sintaxe da Solicitação

```
{  
  "LocationArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

Especifica o nome do recurso da Amazon (ARN) do local do HDFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{  
  "AgentArns": [ "string" ],  
  "AuthenticationType": "string",  
  "BlockSize": number,  
  "CreationTime": number,  
  "KerberosPrincipal": "string",  
  "KmsKeyProviderUri": "string",  
  "LocationArn": "string",
```



```

"LocationUri": "string",
"NameNodes": [
  {
    "Hostname": "string",
    "Port": number
  }
],
"QopConfiguration": {
  "DataTransferProtection": "string",
  "RpcProtection": "string"
},
"ReplicationFactor": number,
"SimpleUser": "string"
}

```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AgentArns

O ARNs dos DataSync agentes que podem se conectar ao seu cluster HDFS.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

AuthenticationType

O tipo de autenticação usado para determinar a identidade do usuário.

Tipo: String

Valores Válidos: SIMPLE | KERBEROS

BlockSize

O tamanho dos blocos de dados a serem gravados no cluster do HDFS.

Tipo: inteiro

Intervalo válido: valor mínimo de 1.048.576. Valor máximo de 1.073.741.824

[CreationTime](#)

O horário em que a localização do HDFS foi criada.

Tipo: Timestamp

[KerberosPrincipal](#)

A entidade principal do Kerberos com acesso aos arquivos e pastas no cluster do HDFS. Esse parâmetro é usado se o `AuthenticationType` for definido como KERBEROS.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^.+`

[KmsKeyProviderUri](#)

O URI do Key Management Server (KMS) do cluster do HDFS.

Tipo: String

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 255.

Padrão: `^kms:\\\\http[s]?@(([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9])(;(([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9]))*:[0-9]{1,5}\\\\kms$`

[LocationArn](#)

O ARN do local do HDFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-zA-Z0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

O URI do local do HDFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[NameNodes](#)

O NameNode que gerencia o namespace HDFS.

Tipo: Matriz de objetos [HdfsNameNode](#)

Membros da matriz: número mínimo de 1 item.

[QopConfiguration](#)

A configuração de Qualidade de Proteção (QOP), que especifica as configurações de Chamada de Procedimento Remoto (RPC) e de proteção de transferência de dados definidas no cluster do HDFS.

Tipo: objeto [QopConfiguration](#)

[ReplicationFactor](#)

O número de DataNodes para os quais replicar os dados ao gravar no cluster HDFS.

Tipo: inteiro

Intervalo válido: valor mínimo de 1. Valor máximo de 512.

[SimpleUser](#)

O nome de usuário para identificar o cliente no sistema operacional do host. Esse parâmetro é usado se o `AuthenticationType` for definido como SIMPLE.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^[_.A-Za-z0-9][_.A-Za-z0-9]*$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationNfs

Fornecer detalhes sobre como um local AWS DataSync de transferência para um servidor de arquivos do Sistema de Arquivos de Rede (NFS) é configurado.

Sintaxe da Solicitação

```
{  
  "LocationArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

Especifica o nome do recurso da Amazon (ARN) do local do NFS sobre o qual deseja informações.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{  
  "CreationTime": number,  
  "LocationArn": "string",  
  "LocationUri": "string",  
  "MountOptions": {  
    "Version": "string"  
  }  
}
```

```
},  
  "OnPremConfig": {  
    "AgentArns": [ "string" ]  
  }  
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[CreationTime](#)

O horário em que o local do NFS foi criado.

Tipo: Timestamp

[LocationArn](#)

O ARN do local do NFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

O URI do local do NFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\\-]+$`

[MountOptions](#)

As opções de montagem DataSync usadas para montar seu servidor de arquivos NFS.

Tipo: objeto [NfsMountOptions](#)

[OnPremConfig](#)

Os AWS DataSync agentes que podem se conectar ao seu servidor de arquivos do Sistema de Arquivos de Rede (NFS).

Tipo: objeto [OnPremConfig](#)

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo

O exemplo a seguir retorna informações sobre o local do NFS especificado na solicitação de amostras.

Exemplo de solicitação

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
}
```

Exemplo

Este exemplo ilustra um uso do. DescribeLocationNfs

Resposta da amostra

```
{
  "CreationTime": 1532660733.39,
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-07db7abfc326c50aa",
  "LocationUri": "hostname.amazon.com",
  "OnPremConfig": {
    "AgentArns": [ "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44b3nfs" ]
  }
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationObjectStorage

Fornecer detalhes sobre como um local AWS DataSync de transferência para um sistema de armazenamento de objetos é configurado.

Sintaxe da Solicitação

```
{  
  "LocationArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[LocationArn](#)

Especifica o nome do recurso da Amazon (ARN) do local do sistema de armazenamento de objetos.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{  
  "AccessKey": "string",  
  "AgentArns": [ "string" ],  
  "CmkSecretConfig": {  
    "KmsKeyArn": "string",  
    "SecretArn": "string"  
  }  
}
```

```
{,
  "CreationTime": number,
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "LocationArn": "string",
  "LocationUri": "string",
  "ManagedSecretConfig": {
    "SecretArn": "string"
  },
  "ServerCertificate": blob,
  "ServerPort": number,
  "ServerProtocol": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[AccessKey](#)

A chave de acesso (por exemplo, um nome de usuário) necessária para se autenticar com o sistema de armazenamento de objetos.

Tipo: String

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 200.

Padrão: ^.*\$

[AgentArns](#)

Os ARNs DataSync agentes que podem se conectar ao seu sistema de armazenamento de objetos.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

[CmkSecretConfig](#)

Descreve as informações de configuração DataSync de um segredo gerenciado, como um token de autenticação ou conjunto de credenciais DataSync usado para acessar um local de transferência específico e um gerenciado pelo cliente. AWS KMS key

Tipo: objeto [CmkSecretConfig](#)

[CreationTime](#)

O horário em que a localização foi criada.

Tipo: Timestamp

[CustomSecretConfig](#)

Descreve as informações de configuração de um segredo gerenciado pelo cliente, como um token de autenticação ou conjunto de credenciais DataSync usado para acessar um local de transferência específico e um gerenciado pelo cliente. AWS KMS key

Tipo: objeto [CustomSecretConfig](#)

[LocationArn](#)

O ARN do local do sistema de armazenamento de objetos.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

O URI do local do sistema de armazenamento de objetos.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[ManagedSecretConfig](#)

Descreve as informações de configuração DataSync de um segredo gerenciado, como um token de autenticação ou um conjunto de credenciais DataSync usado para acessar um local de transferência específico. DataSync usa a chave KMS AWS gerenciada padrão para criptografar esse segredo. AWS Secrets Manager

Tipo: objeto [ManagedSecretConfig](#)

[ServerCertificate](#)

A cadeia de certificados DataSync para autenticação em seu sistema de armazenamento de objetos se o sistema usar uma autoridade de certificação (CA) privada ou autoassinada.

Tipo: Objeto de dados binários codificado em Base64

Restrições de tamanho: tamanho máximo de 32768.

[ServerPort](#)

A porta em que o servidor de armazenamento de objetos aceita o tráfego de rede de entrada (por exemplo, a porta 443).

Tipo: inteiro

Intervalo válido: valor mínimo de 1. Valor máximo de 65536.

[ServerProtocol](#)

O protocolo que o seu sistema de armazenamento de objetos usa para se comunicar.

Tipo: String

Valores Válidos: HTTPS | HTTP

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationS3

Fornece detalhes sobre como um local AWS DataSync de transferência para um bucket do S3 é configurado.

Sintaxe da Solicitação

```
{  
  "LocationArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

O nome do recurso da Amazon (ARN) do local do Amazon S3.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{  
  "AgentArns": [ "string" ],  
  "CreationTime": number,  
  "LocationArn": "string",  
  "LocationUri": "string",  
  "S3Config": {  
    "BucketAccessRoleArn": "string"  
  },  
}
```

```
"S3StorageClass": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

AgentArns

O ARNs dos DataSync agentes implantados em seu Outpost ao trabalhar com o Amazon S3 em Outposts.

Para obter mais informações, consulte [Implantar seu DataSync agente em AWS Outposts](#).

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

CreationTime

O horário em que o local do bucket da Amazon S3 foi criado.

Tipo: Timestamp

LocationArn

O ARN do local do Amazon S3.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

O URL do local do Amazon S3 que foi descrito.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[S3Config](#)

Especifica o Amazon Resource Name (ARN) AWS Identity and Access Management da função DataSync (IAM) usada para acessar seu bucket do S3.

Para obter mais informações, consulte [Fornecendo DataSync acesso aos buckets do S3](#).

Tipo: objeto [S3Config](#)

[S3StorageClass](#)

Quando o Amazon S3 é um local de destino, essa é a classe de armazenamento que você escolheu para seus objetos.

Algumas classes de armazenamento têm comportamentos que podem afetar os custos de armazenamento do Amazon S3. Para obter mais informações, consulte [Considerações sobre classes de armazenamento com transferências do Amazon S3](#).

Tipo: String

Valores Válidos: STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo

O exemplo a seguir retorna informações sobre o local do Amazon S3 especificado no exemplo de solicitação.

Exemplo de solicitação

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

Exemplo

Este exemplo ilustra um uso do DescribeLocation S3.

Resposta da amostra

```
{
  "CreationTime": 1532660733.39,
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3",
  "LocationUri": "s3://amzn-s3-demo-bucket",
  "S3Config": {
    "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/amzn-s3-demo-bucket-
access-role",
  }
  "S3StorageClass": "STANDARD"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)

- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeLocationSmb

Fornece detalhes sobre como um local AWS DataSync de transferência para um servidor de arquivos SMB (Server Message Block) é configurado.

Sintaxe da Solicitação

```
{
  "LocationArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[LocationArn](#)

Especifica o nome do recurso da Amazon (ARN) do local SMB sobre o qual você deseja informações.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "CreationTime": number,
  "DnsIpAddresses": [ "string" ],
  "Domain": "string",
  "KerberosPrincipal": "string",
```

```
"LocationArn": "string",
"LocationUri": "string",
"MountOptions": {
  "Version": "string"
},
"User": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[AgentArns](#)

O ARNs dos DataSync agentes que podem se conectar ao seu servidor de arquivos SMB.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

[AuthenticationType](#)

O protocolo de autenticação DataSync usado para se conectar ao seu servidor de arquivos SMB.

Tipo: String

Valores Válidos: NTLM | KERBEROS

[CreationTime](#)

O horário em que o local do SMB foi criado.

Tipo: Timestamp

[DnsIpAddresses](#)

Os IPv4 endereços dos servidores DNS aos quais seu servidor de arquivos SMB pertence. Esse elemento se aplica somente se `AuthenticationType` estiver definido como `KERBEROS`.

Tipo: matriz de strings

Membros da matriz: número máximo de 2 itens.

Restrições de comprimento: comprimento mínimo de 7. Comprimento máximo de 39.

Padrão: \A((25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\.(25[0-5]|2[0-4]\d|[0-1]?\d?\d))){3}|([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-fA-F]{1,4}){1,6}))\z

[Domain](#)

O nome do domínio do Windows ao qual o servidor de arquivos SMB pertence. Esse elemento se aplica somente se AuthenticationType estiver definido como NTLM.

Tipo: String

Restrições de tamanho: tamanho máximo de 253.

Padrão: ^[A-Za-z0-9](\(|-+)?[A-Za-z0-9]){0,252}\$

[KerberosPrincipal](#)

O diretor do Kerberos que tem permissão para acessar os arquivos, pastas e metadados de arquivos em seu servidor de arquivos SMB.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: ^.+\$

[LocationArn](#)

O ARN do local SMB.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

LocationUri

O URI do local SMB.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

MountOptions

A versão do protocolo SMB DataSync usada para acessar seu servidor de arquivos SMB.

Tipo: objeto [SmbMountOptions](#)

User

O usuário que pode montar e acessar os arquivos, pastas e metadados de arquivos no servidor de arquivos SMB. Esse elemento se aplica somente se `AuthenticationType` estiver definido como `NTLM`.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^[^\\x22\\x5B\\x5D\\/\\:;|, +*?\\x3C\\x3E]{1,104}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo

Este exemplo ilustra um uso do `DescribeLocationSmb`

Exemplo de solicitação

```
{
  "arn:aws:datasync:us-east-1:111222333444:location/loc-0f01451b140b2af49"
}
```

Exemplo

Este exemplo ilustra um uso do `DescribeLocationSmb`

Resposta da amostra

```
{
  "AgentArns":[
    "arn:aws:datasync:us-east-2:111222333444:agent/agent-0bc3b3dc9bbc15145",
    "arn:aws:datasync:us-east-2:111222333444:agent/agent-04b3fe3d261a18c8f"
  ],
  "CreationTime":"1532660733.39",
  "Domain":"AMAZON",
  "LocationArn":"arn:aws:datasync:us-east-1:111222333444:location/loc-0f01451b140b2af49",
  "LocationUri":"smb://hostname.amazon.com/share",
  "MountOptions":{"
    "Version":"SMB3"
  },
  "User":"user-1"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)

- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeTask

Fornecer informações sobre uma tarefa, que definem para onde e como o AWS DataSync transfere os dados.

Sintaxe da Solicitação

```
{
  "TaskArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

TaskArn

Especifica o nome do recurso da Amazon (ARN) a tarefa de transferência sobre a qual você deseja informações.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{
  "CloudWatchLogGroupArn": "string",
  "CreationTime": number,
  "CurrentTaskExecutionArn": "string",
  "DestinationLocationArn": "string",
  "DestinationNetworkInterfaceArns": [ "string" ],
  "ErrorCode": "string",
  "ErrorDetail": "string",
```

```

"Excludes": [
  {
    "FilterType": "string",
    "Value": "string"
  }
],
"Includes": [
  {
    "FilterType": "string",
    "Value": "string"
  }
],
"ManifestConfig": {
  "Action": "string",
  "Format": "string",
  "Source": {
    "S3": {
      "BucketAccessRoleArn": "string",
      "ManifestObjectPath": "string",
      "ManifestObjectVersionId": "string",
      "S3BucketArn": "string"
    }
  }
},
"Name": "string",
"Options": {
  "Atime": "string",
  "BytesPerSecond": number,
  "Gid": "string",
  "LogLevel": "string",
  "Mtime": "string",
  "ObjectTags": "string",
  "OverwriteMode": "string",
  "PosixPermissions": "string",
  "PreserveDeletedFiles": "string",
  "PreserveDevices": "string",
  "SecurityDescriptorCopyFlags": "string",
  "TaskQueueing": "string",
  "TransferMode": "string",
  "Uid": "string",
  "VerifyMode": "string"
},
"Schedule": {
  "ScheduleExpression": "string",

```

```

    "Status": "string"
  },
  "ScheduleDetails": {
    "DisabledBy": "string",
    "DisabledReason": "string",
    "StatusUpdateTime": number
  },
  "SourceLocationArn": "string",
  "SourceNetworkInterfaceArns": [ "string " ],
  "Status": "string",
  "TaskArn": "string",
  "TaskMode": "string",
  "TaskReportConfig": {
    "Destination": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "S3BucketArn": "string",
        "Subdirectory": "string"
      }
    },
    "ObjectVersionIds": "string",
    "OutputType": "string",
    "Overrides": {
      "Deleted": {
        "ReportLevel": "string"
      },
      "Skipped": {
        "ReportLevel": "string"
      },
      "Transferred": {
        "ReportLevel": "string"
      },
      "Verified": {
        "ReportLevel": "string"
      }
    }
  },
  "ReportLevel": "string"
}
}

```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[CloudWatchLogGroupArn](#)

O Amazon Resource Name (ARN) de um grupo de CloudWatch logs da Amazon para monitorar sua tarefa.

Para obter mais informações, consulte [Monitoramento de transferências de dados com o CloudWatch Logs](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 562.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-\0-9]+:[0-9]{12}:log-group:([^\:]*)(:\:)*$`

[CreationTime](#)

A data e hora em que a tarefa foi criada.

Tipo: Timestamp

[CurrentTaskExecutionArn](#)

O ARN da última execução da tarefa.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

[DestinationLocationArn](#)

O ARN do local de destino da transferência.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

DestinationNetworkInterfaceArns

A ARNs das [interfaces de rede](#) DataSync criadas para seu local de destino.

Tipo: matriz de strings

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:aws[\-a-z]{0,}:ec2:[a-z\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

ErrorCode

Se houver um problema com a tarefa, você pode usar o código de erro para ajudar você a solucionar o problema. Para obter mais informações, consulte [Solução de problemas com DataSync transferências](#).

Tipo: String

ErrorDetail

Se houver um problema com a tarefa, você pode usar os detalhes do erro para ajudar você a solucionar o problema. Para obter mais informações, consulte [Solução de problemas com DataSync transferências](#).

Tipo: String

Excludes

Os filtros de exclusão que definem os arquivos, objetos e pastas em seu local de origem que você não DataSync deseja transferir. Para obter mais informações e exemplos, consulte [Especificação do que é DataSync transferido usando filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

Includes

Incluem filtros que definem os arquivos, objetos e pastas em seu local de origem que você DataSync deseja transferir. Para obter mais informações e exemplos, consulte [Especificação do que é DataSync transferido usando filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

ManifestConfig

A configuração do manifesto que lista os arquivos ou objetos que você DataSync deseja transferir. Para obter mais informações, consulte [Especificando quais DataSync transferências usando um manifesto](#).

Tipo: objeto [ManifestConfig](#)

Name

O nome da tarefa.

Tipo: String

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\s+=. _:@/- ]+$`

Options

As configurações da tarefa. Por exemplo, quais metadados de arquivos são preservados, como a integridade dos dados é verificada no final da transferência, limites de largura de banda, entre outras opções.

Tipo: objeto [Options](#)

Schedule

O agendamento de quando você deseja que a tarefa seja executada. Para obter mais informações, consulte [Programar sua tarefa](#).

Tipo: objeto [TaskSchedule](#)

ScheduleDetails

Os detalhes sobre o [agendamento da tarefa](#).

Tipo: objeto [TaskScheduleDetails](#)

SourceLocationArn

O ARN do local de origem da transferência.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:location/loc-[0-9a-z]{17}$`

SourceNetworkInterfaceArns

A ARNs das [interfaces de rede](#) DataSync criadas para seu local de origem.

Tipo: matriz de strings

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:aws[\\-a-z]{0,}:ec2:[a-z\\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

Status

O status da tarefa. Para obter informações sobre o significado de cada status, consulte [Status das tarefas](#).

Tipo: String

Valores Válidos: AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE

TaskArn

O ARN da tarefa.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

TaskMode

O modo de tarefa que você está usando. Para obter mais informações, consulte [Escolha de um modo de tarefa para sua transferência de dados](#).

Tipo: String

Valores Válidos: BASIC | ENHANCED

[TaskReportConfig](#)

A configuração do seu relatório de tarefas, que fornece informações detalhadas sobre sua DataSync transferência. Para obter mais informações, consulte [Monitorando suas DataSync transferências com relatórios de tarefas](#).

Tipo: objeto [TaskReportConfig](#)

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo de solicitação

O exemplo a seguir especifica o ARN de DataSync uma tarefa sobre a qual obter informações.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

Resposta da amostra

O exemplo a seguir mostra uma DescribeTask resposta.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026",
  "Name": "MyTask",
}
```



```
"TaskMode": "BASIC",
"Status": "RUNNING",
"SourceLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-1111aaaa2222bbbb3",
"DestinationLocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-0000zzzz1111yyyy2",
"CurrentTaskExecutionArn": "arn:aws:datasync:us-east-2:111222333444:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f",
"CreationTime": 1532660733.39,
"Options": {
  "Atime": "BEST_EFFORT",
  "BytesPerSecond": 1000,
  "Gid": "NONE",
  "Mtime": "PRESERVE",
  "PosixPermissions": "PRESERVE",
  "PreserveDevices": "NONE",
  "PreserveDeletedFiles": "PRESERVE",
  "Uid": "NONE",
  "VerifyMode": "POINT_IN_TIME_CONSISTENT"
},
"CloudWatchLogGroupArn": "arn:aws:logs:us-east-2:111222333444:log-group:/log-group-
name:*"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

DescribeTaskExecution

Fornece informações sobre a execução de sua AWS DataSync tarefa. Você pode usar essa operação para ajudar a monitorar o progresso de uma transferência de dados em andamento ou verificar os resultados da transferência.

Note

Alguns elementos de DescribeTaskExecution resposta são relevantes somente para um modo de tarefa específico. Para obter informações, consulte [Compreendendo as diferenças do modo de tarefa](#) e [Compreendendo os contadores de desempenho da transferência de dados](#).

Sintaxe da Solicitação

```
{  
  "TaskExecutionArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[TaskExecutionArn](#)

Especifica o nome do recurso da Amazon (ARN) da execução da tarefa sobre a qual você deseja informações.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z \-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Exigido: Sim

Sintaxe da Resposta

```
{
  "BytesCompressed": number,
  "BytesTransferred": number,
  "BytesWritten": number,
  "EndTime": number,
  "EstimatedBytesToTransfer": number,
  "EstimatedFilesToDelete": number,
  "EstimatedFilesToTransfer": number,
  "Excludes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "FilesDeleted": number,
  "FilesFailed": {
    "Delete": number,
    "Prepare": number,
    "Transfer": number,
    "Verify": number
  },
  "FilesListed": {
    "AtDestinationForDelete": number,
    "AtSource": number
  },
  "FilesPrepared": number,
  "FilesSkipped": number,
  "FilesTransferred": number,
  "FilesVerified": number,
  "Includes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "LaunchTime": number,
  "ManifestConfig": {
    "Action": "string",
    "Format": "string",
    "Source": {
      "S3": {
```

```

        "BucketAccessRoleArn": "string",
        "ManifestObjectPath": "string",
        "ManifestObjectVersionId": "string",
        "S3BucketArn": "string"
    }
},
"Options": {
    "Atime": "string",
    "BytesPerSecond": number,
    "Gid": "string",
    "LogLevel": "string",
    "Mtime": "string",
    "ObjectTags": "string",
    "OverwriteMode": "string",
    "PosixPermissions": "string",
    "PreserveDeletedFiles": "string",
    "PreserveDevices": "string",
    "SecurityDescriptorCopyFlags": "string",
    "TaskQueueing": "string",
    "TransferMode": "string",
    "Uid": "string",
    "VerifyMode": "string"
},
"ReportResult": {
    "ErrorCode": "string",
    "ErrorDetail": "string",
    "Status": "string"
},
"Result": {
    "ErrorCode": "string",
    "ErrorDetail": "string",
    "PrepareDuration": number,
    "PrepareStatus": "string",
    "TotalDuration": number,
    "TransferDuration": number,
    "TransferStatus": "string",
    "VerifyDuration": number,
    "VerifyStatus": "string"
},
"StartTime": number,
"Status": "string",
"TaskExecutionArn": "string",
"TaskMode": "string",

```

```

"TaskReportConfig": {
  "Destination": {
    "S3": {
      "BucketAccessRoleArn": "string",
      "S3BucketArn": "string",
      "Subdirectory": "string"
    }
  },
  "ObjectVersionIds": "string",
  "OutputType": "string",
  "Overrides": {
    "Deleted": {
      "ReportLevel": "string"
    },
    "Skipped": {
      "ReportLevel": "string"
    },
    "Transferred": {
      "ReportLevel": "string"
    },
    "Verified": {
      "ReportLevel": "string"
    }
  },
  "ReportLevel": "string"
}

```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

BytesCompressed

O número de bytes físicos que são DataSync transferidos pela rede após a compactação (se a compactação for possível). Esse número geralmente é menor do que, [BytesTransferred](#) menos que os dados não sejam compactáveis.

Tipo: longo

[BytesTransferred](#)

O número de bytes DataSync enviados para a rede antes da compactação (se a compactação for possível). Para saber o número de bytes transferidos pela rede, consulte [BytesCompressed](#).

Tipo: longo

[BytesWritten](#)

O número de bytes lógicos que DataSync realmente gravam no local de destino.

Tipo: longo

[EndTime](#)

A hora em que a tarefa de transferência termina.

Tipo: Timestamp

[EstimatedBytesToTransfer](#)

O número de bytes lógicos que DataSync esperam gravar no local de destino.

Tipo: longo

[EstimatedFilesToDelete](#)

O número de arquivos, objetos e diretórios que você DataSync espera excluir em seu local de destino. Se você não [configurar sua tarefa](#) para excluir os dados no destino que não estão na origem, o valor sempre será 0.

Tipo: longo

[EstimatedFilesToTransfer](#)

O número de arquivos, objetos e diretórios que DataSync esperam ser transferidos pela rede. Esse valor é calculado enquanto DataSync [prepara](#) a transferência.

A forma como isso é calculado depende principalmente da configuração do [modo de transferência](#) da sua tarefa:

- Se TransferMode estiver definido como CHANGED: o cálculo será baseado na comparação do conteúdo dos locais de origem e na diferença e na determinação da diferença que precisa ser transferida. A diferença pode incluir:

- Tudo o que for adicionado ou modificado no local de origem.
- Qualquer coisa que esteja nos dois locais e modificada no destino após uma transferência inicial (a menos que [OverwriteMode](#) esteja configurada como NEVER).
- (Somente no modo de tarefa básica) O número de itens que DataSync espera excluir (se [PreserveDeletedFiles](#) estiver definido como REMOVE).
- Se `TransferMode` estiver definido como ALL - O cálculo é baseado somente nos itens DataSync encontrados no local de origem.

Tipo: longo

[Excludes](#)

Uma lista de regras de filtro que excluem dados específicos durante a transferência. Para obter mais informações e exemplos, consulte [Filtragem de dados transferidos por DataSync](#).

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

[FilesDeleted](#)

O número de arquivos, objetos e diretórios que DataSync realmente são excluídos em seu local de destino. Se você não [configurar sua tarefa](#) para excluir os dados no destino que não estão na origem, o valor sempre será 0.

Tipo: longo

[FilesFailed](#)

O número de objetos que DataSync falham na preparação, transferência, verificação e exclusão durante a execução da tarefa.

Note

Aplica-se somente às [tarefas do modo Avançado](#).

Tipo: objeto [TaskExecutionFilesFailedDetail](#)

[FilesListed](#)

O número de objetos DataSync encontrados em seus locais.

 Note

Aplica-se somente às [tarefas do modo Avançado](#).

Tipo: objeto [TaskExecutionFilesListedDetail](#)

[FilesPrepared](#)

O número de objetos que DataSync tentarão ser transferidos depois de comparar seus locais de origem e destino.

 Note

Aplica-se somente às [tarefas do modo Avançado](#).

Esse contador não é aplicável se você configurar sua tarefa para [transferir todos os dados](#). Nesse cenário, DataSync copia tudo da origem ao destino sem comparar as diferenças entre os locais.

Tipo: longo

[FilesSkipped](#)

O número de arquivos, objetos e diretórios que são DataSync ignorados durante a transferência.

Tipo: longo

[FilesTransferred](#)

O número de arquivos, objetos e diretórios que DataSync realmente são transferidos pela rede. Esse valor é atualizado periodicamente durante a execução da tarefa quando algo é lido da fonte e enviado pela rede.

Se DataSync não conseguir transferir algo, esse valor pode ser menor que `EstimatedFilesToTransfer`. Em alguns casos, esse valor também pode ser maior que `EstimatedFilesToTransfer`. Esse elemento é específico de implementação para alguns tipos de local, portanto, não o use como uma indicação exata do que está sendo transferido ou para monitorar a execução da tarefa.

Tipo: longo

FilesVerified

O número de arquivos, objetos e diretórios que são DataSync verificados durante a transferência.

Note

Quando você configura sua tarefa para [verificar somente os dados transferidos](#), DataSync não verifica diretórios em algumas situações ou arquivos que falham na transferência.

Tipo: longo

Includes

Uma lista de regras de filtro que incluem dados específicos durante a transferência. Para obter mais informações e exemplos, consulte [Filtragem de dados transferidos por DataSync](#).

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

LaunchTime

A hora em que a execução da tarefa realmente começa. Para tarefas não enfileiradas, LaunchTime e geralmente StartTime são as mesmas. Para tarefas em fila, geralmente LaunchTime é mais tarde do que StartTime porque as tarefas anteriormente enfileiradas devem terminar de ser executadas antes que as tarefas mais recentes possam começar.

Tipo: Timestamp

ManifestConfig

A configuração do manifesto que lista os arquivos ou os objetos que você deseja transferir. Para obter mais informações, consulte [Especificando quais DataSync transferências usando um manifesto](#).

Tipo: objeto [ManifestConfig](#)

Options

Indica como sua tarefa de transferência está configurada. Essas opções incluem como DataSync manipula arquivos, objetos e seus metadados associados durante a transferência. Você também pode especificar como verificar a integridade dos dados, definir limites de largura de banda para sua tarefa, entre outras opções.

Cada opção tem um valor padrão. A menos que seja necessário, você não precisa configurar nenhuma opção antes de ligar [StartTaskExecution](#).

Você também pode substituir suas opções de tarefa para cada execução de tarefa. Por exemplo, pode ser bom ajustar o `LogLevel` para uma execução individual.

Tipo: objeto [Options](#)

[ReportResult](#)

Indica se DataSync gerou um [relatório de tarefa](#) completo para sua transferência.

Tipo: objeto [ReportResult](#)

[Result](#)

O resultado da execução da tarefa.

Tipo: objeto [TaskExecutionResultDetail](#)

[StartTime](#)

A hora em que a solicitação é DataSync enviada para iniciar a execução da tarefa. Para tarefas não enfileiradas, `LaunchTime` e geralmente `StartTime` são as mesmas. Para tarefas em fila, geralmente `LaunchTime` é mais tarde do que `StartTime` porque as tarefas anteriormente enfileiradas devem terminar de ser executadas antes que as tarefas mais recentes possam começar.

Tipo: Timestamp

[Status](#)

O status da execução da tarefa.

Para obter informações detalhadas sobre os status de execução de tarefas, consulte [Status de execução de tarefas](#).

Tipo: String

Valores Válidos: QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR

[TaskExecutionArn](#)

O ARN da execução da tarefa sobre a qual deseja obter informações. O `TaskExecutionArn` é hierárquico e inclui `TaskArn` para a tarefa que foi executada.

Por exemplo, um valor `TaskExecution` com o ARN `arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2/execution/exec-08ef1e88ec491019b` executou a tarefa com o ARN `arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2`.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

TaskMode

O modo de tarefa que você está usando. Para obter mais informações, consulte [Escolha de um modo de tarefa para sua transferência de dados](#).

Tipo: String

Valores Válidos: BASIC | ENHANCED

TaskReportConfig

A configuração do seu relatório de tarefas, que fornece informações detalhadas sobre sua DataSync transferência. Para obter mais informações, consulte [Criar um relatório de tarefas](#).

Tipo: objeto [TaskReportConfig](#)

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo de solicitação

Este exemplo ilustra uma solicitação `DescribeTaskExecution`.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccdddf/execution/exec-1234abcd1234abcd1"
}
```

Exemplo de resposta 1 para uma execução de tarefa no modo aprimorado

O exemplo a seguir descreve a execução de uma DataSync tarefa que usa o modo Avançado. A execução também está transferindo dados específicos usando filtros de exclusão e inclusão.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccdddf/execution/exec-1234abcd1234abcd1",
  "Status": "SUCCESS",
  "Options": {
    "VerifyMode": "ONLY_FILES_TRANSFERRED",
    "OverwriteMode": "ALWAYS",
    "Atime": "BEST_EFFORT",
    "Mtime": "PRESERVE",
    "Uid": "NONE",
    "Gid": "NONE",
    "PreserveDeletedFiles": "PRESERVE",
    "PreserveDevices": "NONE",
    "PosixPermissions": "NONE",
    "BytesPerSecond": -1,
    "TaskQueueing": "ENABLED",
    "LogLevel": "BASIC",
    "TransferMode": "CHANGED",
    "SecurityDescriptorCopyFlags": "NONE",
    "ObjectTags": "PRESERVE"
  },
  "Excludes": [{
    "FilterType": "SIMPLE_PATTERN",
    "Value": "/archive-files"
  }],
  "Includes": [{
```

```

    "FilterType": "SIMPLE_PATTERN",
    "Value": "/files"
  ]],
  "StartTime": "2024-10-16T11:19:56.844000-04:00",
  "EstimatedFilesToTransfer": 7,
  "EstimatedBytesToTransfer": 30,
  "FilesTransferred": 7,
  "BytesWritten": 30,
  "BytesTransferred": 30,
  "BytesCompressed": 30,
  "Result": {
    "PrepareDuration": 0,
    "PrepareStatus": "SUCCESS",
    "TotalDuration": 3310,
    "TransferDuration": 0,
    "TransferStatus": "SUCCESS",
    "VerifyDuration": 0,
    "VerifyStatus": "SUCCESS"
  },
  "FilesDeleted": 0,
  "FilesSkipped": 0,
  "FilesVerified": 7,
  "EstimatedFilesToDelete": 0,
  "TaskMode": "ENHANCED",
  "FilesPrepared": 7,
  "FilesListed": {
    "AtSource": 7,
    "AtDestinationForDelete": 0
  },
  "FilesFailed": {
    "Prepare": 0,
    "Transfer": 0,
    "Verify": 0,
    "Delete": 0
  }
}

```

Resposta de amostra 2 para uma execução de tarefa no modo aprimorado

O exemplo a seguir descreve outra execução de DataSync tarefa que usa o modo Avançado. Nessa situação, a execução está transferindo dados específicos usando um manifesto em vez de filtros.

```
{
```

```

    "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddd/execution/exec-1234abcd1234abcd1",
    "Status": "SUCCESS",
    "Options": {
        "VerifyMode": "ONLY_FILES_TRANSFERRED",
        "OverwriteMode": "ALWAYS",
        "Atime": "BEST_EFFORT",
        "Mtime": "PRESERVE",
        "Uid": "NONE",
        "Gid": "NONE",
        "PreserveDeletedFiles": "PRESERVE",
        "PreserveDevices": "NONE",
        "PosixPermissions": "NONE",
        "BytesPerSecond": -1,
        "TaskQueueing": "ENABLED",
        "LogLevel": "TRANSFER",
        "TransferMode": "CHANGED",
        "SecurityDescriptorCopyFlags": "NONE",
        "ObjectTags": "PRESERVE"
    },
    "Excludes": [],
    "Includes": [],
    "ManifestConfig": {
        "Action": "TRANSFER",
        "Format": "CSV",
        "S3AccessRoleArn": "arn:aws:iam::111222333444:role/service-role/
DataSyncS3ManifestAccess",
        "S3Bucket": "arn:aws:s3:::manifests-datasync",
        "VersionId": "Ixs7NQzEOj8BkL9r4ywX2FtDh_cPf3mG",
        "Source": {
            "S3": {
                "ManifestObjectPath": "manifest-folder/manifest-versioned-files",
                "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-manifest-
role/DataSyncS3ManifestAccess",
                "S3BucketArn": "arn:aws:s3:::manifests-datasync",
                "ManifestObjectVersionId": "Ixs7NQzEOj8BkL9r4ywX2FtDh_cPf3mG"
            }
        }
    },
    "StartTime": "2024-10-16T09:29:56.757000-04:00",
    "EstimatedFilesToTransfer": 1,
    "EstimatedBytesToTransfer": 6,
    "FilesTransferred": 1,
    "BytesWritten": 6,

```

```

"BytesTransferred": 6,
"BytesCompressed": 6,
"Result": {
  "PrepareDuration": 0,
  "PrepareStatus": "SUCCESS",
  "TotalDuration": 3089,
  "TransferDuration": 0,
  "TransferStatus": "SUCCESS",
  "VerifyDuration": 0,
  "VerifyStatus": "SUCCESS"
},
"TaskReportConfig": {
  "Destination": {
    "S3": {
      "Subdirectory": "reports/",
      "S3BucketArn": "arn:aws:s3:::my-task-report",
      "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-task-report-
role/DataSyncTaskReportS3BucketAccess"
    }
  },
  "OutputType": "STANDARD",
  "ReportLevel": "SUCSESSES_AND_ERRORS",
  "ObjectVersionIds": "INCLUDE"
},
"FilesDeleted": 0,
"FilesSkipped": 0,
"FilesVerified": 1,
"ReportResult": {
  "Status": "SUCCESS"
},
"EstimatedFilesToDelete": 0,
"TaskMode": "ENHANCED",
"FilesPrepared": 1,
"FilesListed": {
  "AtSource": 1,
  "AtDestinationForDelete": 0
},
"FilesFailed": {
  "Prepare": 0,
  "Transfer": 0,
  "Verify": 0,
  "Delete": 0
}

```



```
}
```

Exemplo de resposta para a execução de uma tarefa no modo Básico

O exemplo a seguir descreve a execução de uma DataSync tarefa que usa o modo Básico.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccdddf/execution/exec-1234abcd1234abcd1",
  "BytesCompressed": 3500,
  "BytesTransferred": 5000,
  "BytesWritten": 5000,
  "EstimatedBytesToTransfer": 5000,
  "EstimatedFilesToDelete": 10,
  "EstimatedFilesToTransfer": 100,
  "FilesDeleted": 10,
  "FilesSkipped": 0,
  "FilesTransferred": 100,
  "FilesVerified": 100,
  "Result": {
    "PrepareDuration": 100,
    "PrepareStatus": "SUCCESS",
    "TransferDuration": 60,
    "TransferStatus": "SUCCESS",
    "VerifyDuration": 30,
    "VerifyStatus": "SUCCESS"
  },
  "StartTime": "2024-10-16T11:19:56.844000-04:00",
  "Status": "SUCCESS",
  "OverrideOptions": {
    "Atime": "BEST_EFFORT",
    "BytesPerSecond": "1000",
    "Gid": "NONE",
    "Mtime": "PRESERVE",
    "PosixPermissions": "PRESERVE",
    "PreserveDeletedFiles": "PRESERVE",
    "Uid": "NONE",
    "VerifyMode": "POINT_IN_TIME_CONSISTENT"
  },
  "TaskReportConfig": {
    "Destination": {
      "S3": {
        "BucketAccessRoleArn": "arn:aws:iam::111222333444:role/my-datasync-
role",
```

```
        "S3BucketArn": "arn:aws:s3:::my-task-reports-bucket/*",
        "Subdirectory": "reports"
    },
    "ObjectVersionIds": "INCLUDE",
    "OutputType": "STANDARD",
    "Overrides": {
        "Deleted": {
            "ReportLevel": "ERRORS_ONLY"
        },
        "Skipped": {
            "ReportLevel": "SUCSESSES_AND_ERRORS"
        },
        "Transferred": {
            "ReportLevel": "ERRORS_ONLY"
        },
        "Verified": {
            "ReportLevel": "ERRORS_ONLY"
        }
    },
    "ReportLevel": "ERRORS_ONLY"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListAgents

Retorna uma lista de AWS DataSync agentes que pertencem a um Conta da AWS no Região da AWS especificado na solicitação.

Com a paginação, você pode reduzir o número de atendentes retornados em uma resposta. Se você receber uma lista truncada de atendentes em uma resposta, a resposta conterá um marcador que você pode especificar em sua próxima solicitação para buscar a próxima página de atendentes.

ListAgents eventualmente é consistente. Isso significa que o resultado da execução da operação pode não refletir que você acabou de criar ou excluir um atendente. Por exemplo, se você criar um agente com [CreateAgent](#) depois executá-lo imediatamente ListAgents, esse agente pode não aparecer na lista imediatamente. Em situações como essa, você sempre pode confirmar se um agente foi criado (ou excluído) usando [DescribeAgent](#).

Sintaxe da Solicitação

```
{  
  "MaxResults": number,  
  "NextToken": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[MaxResults](#)

Especifica o número máximo de DataSync agentes a serem listados em uma resposta. Por padrão, uma resposta mostra no máximo 100 atendentes.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 100.

Obrigatório: Não

[NextToken](#)

Especifica uma string opaca que indica a posição para começar a próxima lista de resultados na resposta.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: [a-zA-Z0-9=_-]+

Obrigatório: Não

Sintaxe da Resposta

```
{
  "Agents": [
    {
      "AgentArn": "string",
      "Name": "string",
      "Platform": {
        "Version": "string"
      },
      "Status": "string"
    }
  ],
  "NextToken": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[Agents](#)

Uma lista de DataSync agentes Conta da AWS em sua área Região da AWS especificada na solicitação. A lista é ordenada pelos nomes de recursos da Amazon dos agentes (ARNs).

Tipo: matriz de objetos [AgentListEntry](#)

NextToken

Uma string opaca que indica a posição para começar a próxima lista de resultados na resposta.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: [a-zA-Z0-9=_-]+

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)

- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListLocations

Retorna uma lista de pontos de origem e de destino.

Se você tiver mais locais do que os retornados em uma resposta (ou seja, a resposta retornará apenas uma lista truncada de seus agentes), a resposta conterá um token que você pode especificar em sua próxima solicitação para buscar a próxima página de locais.

Sintaxe da Solicitação

```
{
  "Filters": [
    {
      "Name": "string",
      "Operator": "string",
      "Values": [ "string" ]
    }
  ],
  "MaxResults": number,
  "NextToken": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

Filters

Você pode usar filtros de API para refinar a lista de recursos retornados por `ListLocations`. Por exemplo, para recuperar todas as tarefas em um local de origem específico, você pode usar `ListLocations` com o nome do filtro `LocationType` `S3` e `Operator` `Equals`.

Tipo: matriz de objetos [LocationFilter](#)

Obrigatório: Não

MaxResults

O número máximo de localizações a serem retornadas.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 100.

Obrigatório: Não

[NextToken](#)

Uma sequência opaca que indica a posição na qual começar a próxima lista de locais.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: [a-zA-Z0-9=_-]+

Obrigatório: Não

Sintaxe da Resposta

```
{
  "Locations": [
    {
      "LocationArn": "string",
      "LocationUri": "string"
    }
  ],
  "NextToken": "string"
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[Locations](#)

Uma matriz que contém uma lista de locais.

Tipo: matriz de objetos [LocationListEntry](#)

[NextToken](#)

Uma sequência opaca que indica a posição na qual começar a retornar a próxima lista de locais.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: [a-zA-Z0-9=_-]+

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalServerError

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListTagsForResource

Retorna todas as tags associadas a um AWS recurso.

Sintaxe da Solicitação

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "ResourceArn": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[MaxResults](#)

Especifica quantos resultados você deseja na resposta.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 100.

Obrigatório: Não

[NextToken](#)

Especifica uma string opaca que indica a posição para começar a próxima lista de resultados na resposta.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: [a-zA-Z0-9=_-]+

Obrigatório: Não

[ResourceArn](#)

Especifica o nome do recurso da Amazon (ARN) do recurso sobre o qual você deseja obter informações de tag.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:((agent|task|location|system)/((agent|task|loc)-[a-f0-9]{17}|storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}))(/execution/exec-[a-f0-9]{17})?$`

Exigido: Sim

Sintaxe da Resposta

```
{
  "NextToken": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[NextToken](#)

Uma string opaca que indica a posição para começar a próxima lista de resultados na resposta.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: [a-zA-Z0-9=_-]+

Tags

Uma matriz de tags aplicadas ao recurso especificado.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 55 itens.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)

- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListTaskExecutions

Retorna uma lista de execuções para uma tarefa AWS DataSync de transferência.

Sintaxe da Solicitação

```
{
  "MaxResults": number,
  "NextToken": "string",
  "TaskArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[MaxResults](#)

Especifica quantos resultados você deseja na resposta.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 100.

Obrigatório: Não

[NextToken](#)

Especifica uma string opaca que indica a posição na qual começar a próxima lista de resultados na resposta.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: [a-zA-Z0-9=_-]+

Obrigatório: Não

[TaskArn](#)

Especifica o nome do recurso da Amazon (ARN) da tarefa sobre cuja execução você deseja informações.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Obrigatório: Não

Sintaxe da Resposta

```
{
  "NextToken": "string",
  "TaskExecutions": [
    {
      "Status": "string",
      "TaskExecutionArn": "string",
      "TaskMode": "string"
    }
  ]
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[NextToken](#)

Uma string opaca que indica a posição para começar a próxima lista de resultados na resposta.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: `[a-zA-Z0-9=_-]+`

[TaskExecutions](#)

Uma lista de execuções da tarefa.

Tipo: matriz de objetos [TaskExecutionListEntry](#)

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

ListTasks

Retorna uma lista das AWS DataSync tarefas que você criou.

Sintaxe da Solicitação

```
{
  "Filters": [
    {
      "Name": "string",
      "Operator": "string",
      "Values": [ "string" ]
    }
  ],
  "MaxResults": number,
  "NextToken": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[Filters](#)

Você pode usar filtros de API para refinar a lista de recursos retornados por ListTasks. Por exemplo, para recuperar todas as tarefas em um local de origem específico, você pode usar ListTasks com o nome do filtro LocationId e Operator Equals com o ARN do local.

Tipo: matriz de objetos [TaskFilter](#)

Obrigatório: Não

[MaxResults](#)

O número máximo de tarefas a serem retornadas.

Tipo: inteiro

Intervalo válido: valor mínimo de 0. Valor máximo de 100.

Obrigatório: Não

[NextToken](#)

Um string opaco que indica a posição de onde começar a próxima lista de locais.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: [a-zA-Z0-9=_-]+

Obrigatório: Não

Sintaxe da Resposta

```
{
  "NextToken": "string",
  "Tasks": [
    {
      "Name": "string",
      "Status": "string",
      "TaskArn": "string",
      "TaskMode": "string"
    }
  ]
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[NextToken](#)

Um string opaco que indica a posição de onde começar a próxima lista de locais.

Tipo: String

Restrições de tamanho: tamanho máximo de 65535.

Padrão: [a-zA-Z0-9=_-]+

Tasks

Uma lista de todas as tarefas que são retornadas.

Tipo: matriz de objetos [TaskListEntry](#)

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

StartTaskExecution

Inicia uma tarefa AWS DataSync de transferência. Para cada tarefa, você só pode executar uma tarefa por vez.

Há várias etapas para a execução de uma tarefa. Para obter mais informações, consulte [Status da execução de tarefas](#).

Important

Se você planeja transferir dados de ou para um local do Amazon S3, analise [como isso DataSync pode afetar as cobranças de suas solicitações do S3](#) e a [página de DataSync preços](#) antes de começar.

Sintaxe da Solicitação

```
{
  "Excludes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "Includes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "ManifestConfig": {
    "Action": "string",
    "Format": "string",
    "Source": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "ManifestObjectPath": "string",
        "ManifestObjectVersionId": "string",
        "S3BucketArn": "string"
      }
    }
  }
},
```



```

"OverrideOptions": {
  "Atime": "string",
  "BytesPerSecond": number,
  "Gid": "string",
  "LogLevel": "string",
  "Mtime": "string",
  "ObjectTags": "string",
  "OverwriteMode": "string",
  "PosixPermissions": "string",
  "PreserveDeletedFiles": "string",
  "PreserveDevices": "string",
  "SecurityDescriptorCopyFlags": "string",
  "TaskQueueing": "string",
  "TransferMode": "string",
  "Uid": "string",
  "VerifyMode": "string"
},
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"TaskArn": "string",
"TaskReportConfig": {
  "Destination": {
    "S3": {
      "BucketAccessRoleArn": "string",
      "S3BucketArn": "string",
      "Subdirectory": "string"
    }
  },
  "ObjectVersionIds": "string",
  "OutputType": "string",
  "Overrides": {
    "Deleted": {
      "ReportLevel": "string"
    },
    "Skipped": {
      "ReportLevel": "string"
    },
    "Transferred": {
      "ReportLevel": "string"
    }
  },

```

```
    "Verified": {  
      "ReportLevel": "string"  
    },  
    "ReportLevel": "string"  
  }  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[Excludes](#)

Especifica uma lista de regras de filtro que determina quais arquivos excluir de uma tarefa. A lista contém uma única string de filtro que consiste nos padrões a serem excluídos. Os padrões são delimitados por “|” (isto é, um tubo), por exemplo, “/folder1|/folder2”.

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

Obrigatório: Não

[Includes](#)

Especifica uma lista de regras de filtro que determina quais arquivos incluir ao executar uma tarefa. O padrão deverá conter uma única string de filtro que consiste nos padrões a serem incluídos. Os padrões são delimitados por “|” (isto é, um tubo), por exemplo, “/folder1|/folder2”.

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

Obrigatório: Não

[ManifestConfig](#)

Configura um manifesto, que é uma lista de arquivos ou objetos que você deseja DataSync transferir. Para obter mais informações e exemplos de configuração, consulte [Especificação do que é DataSync transferido usando um manifesto](#).

Ao usar esse parâmetro, sua identidade de chamador (a função DataSync com a qual você está usando) deve ter a `iam:PassRole` permissão. A [AWSDataSyncFullAccess](#) política inclui essa permissão.

Para remover uma configuração de manifesto, especifique esse parâmetro com um valor vazio.

Tipo: objeto [ManifestConfig](#)

Obrigatório: Não

[OverrideOptions](#)

Indica como sua tarefa de transferência está configurada. Essas opções incluem como DataSync manipula arquivos, objetos e seus metadados associados durante a transferência. Você também pode especificar como verificar a integridade dos dados, definir limites de largura de banda para sua tarefa, entre outras opções.

Cada opção tem um valor padrão. A menos que seja necessário, você não precisa configurar nenhuma opção antes de ligar [StartTaskExecution](#).

Você também pode substituir suas opções de tarefa para cada execução de tarefa. Por exemplo, pode ser bom ajustar o `LogLevel` para uma execução individual.

Tipo: objeto [Options](#)

Obrigatório: Não

[Tags](#)

Especifica as tags que você deseja aplicar ao nome do recurso da Amazon (ARN) que representa a execução da tarefa.

As tags são pares de valores-chave que ajudam você a gerenciar, filtrar e pesquisar seus DataSync recursos.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Não

[TaskArn](#)

Especifica o nome do recurso da Amazon (ARN) da tarefa que você deseja iniciar.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Exigido: Sim

[TaskReportConfig](#)

Especifica como você deseja configurar um relatório de tarefas, que fornece informações detalhadas sobre sua DataSync transferência. Para obter mais informações, consulte [Monitorando suas DataSync transferências com relatórios de tarefas](#).

Ao usar esse parâmetro, sua identidade de chamador (a função DataSync com a qual você está usando) deve ter a `iam:PassRole` permissão. A [AWSDataSyncFullAccess](#) política inclui essa permissão.

Para remover uma configuração de relatório de tarefa, especifique esse parâmetro como vazio.

Tipo: objeto [TaskReportConfig](#)

Obrigatório: Não

Sintaxe da Resposta

```
{  
  "TaskExecutionArn": "string"  
}
```

Elementos de Resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

[TaskExecutionArn](#)

O ARN da execução da tarefa em execução.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de status HTTP: 400

Exemplos

Exemplo de solicitação

O exemplo a seguir inicia a execução de uma tarefa usando as opções padrão para a tarefa especificada.

```
{
  "OverrideOptions": {
    "Atime": "BEST_EFFORT",
    "BytesPerSecond": 1000,
    "Gid": "NONE",
    "Mtime": "PRESERVE",
    "PosixPermissions": "PRESERVE",
    "PreserveDevices": "NONE",
    "PreserveDeletedFiles": "PRESERVE",
    "Uid": "NONE",
    "VerifyMode": "POINT_IN_TIME_CONSISTENT"
  },
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
```

```
}
```

Resposta da amostra

Este exemplo ilustra um uso do `StartTaskExecution`

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-2:111222333444:task/
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"
}
```

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

TagResource

Aplica uma tag a um AWS recurso. Tags são pares chave-valor que podem ajudar você a gerenciar, filtrar e pesquisar recursos.

Isso inclui AWS DataSync recursos, como locais, tarefas e execuções de tarefas.

Sintaxe da Solicitação

```
{
  "ResourceArn": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

ResourceArn

Especifica o nome do recurso da Amazon (ARN) do recurso ao qual aplicar a tag.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:(agent|task|location|system)/((agent|task|loc)-[a-f0-9]{17}|storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})/(execution/exec-[a-f0-9]{17})?$`

Exigido: Sim

Tags

Especifique as tags que você quer aplicar ao recurso.

Tipo: matriz de objetos [TagListEntry](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens.

Obrigatório: Sim

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UntagResource

Remove as tags de um AWS recurso.

Sintaxe da Solicitação

```
{
  "Keys": [ "string" ],
  "ResourceArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[Keys](#)

Especifica as chaves nas tags que você deseja remover.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 50 itens.

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^[a-zA-Z0-9\s+=. _:/-]+$`

Exigido: Sim

[ResourceArn](#)

O nome do recurso da Amazon (ARN) do recurso do qual remover as tags.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z-0-9]+:[0-9]{12}:(agent|task|location|system)/((agent|task|loc)-[a-`

```
f0-9]{17}|storage-system-[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})(/execution/exec-[a-f0-9]{17})?>
```

Exigido: Sim

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)

- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateAgent

Atualiza o nome de um AWS DataSync agente.

Sintaxe da Solicitação

```
{  
  "AgentArn": "string",  
  "Name": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AgentArn](#)

O nome do recurso da Amazon (ARN) do atendente para ser atualizado.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Exigido: Sim

[Name](#)

Escolha o nome que você deseja usar para configurar o atendente.

Tipo: String

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\\s+=. _:@/-]+$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationAzureBlob

Modifica as seguintes configurações do local de transferência do Microsoft Azure Blob Storage com o qual você está usando. AWS DataSync

Para obter mais informações, consulte [Configurando DataSync transferências com o Azure Blob Storage](#).

Sintaxe da Solicitação

```
{
  "AccessTier": "string",
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "BlobType": "string",
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "LocationArn": "string",
  "SasConfiguration": {
    "Token": "string"
  },
  "Subdirectory": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AccessTier](#)

Especifica o nível de acesso para o qual deseja que seus objetos ou arquivos sejam transferidos. Isso só se aplica ao usar o local como destino de transferência. Para obter mais informações, consulte [Níveis de acesso](#).

Tipo: String

Valores Válidos: HOT | COOL | ARCHIVE

Obrigatório: Não

AgentArns

(Opcional) Especifica o Amazon Resource Name (ARN) do agente que pode se conectar DataSync ao seu contêiner do Azure Blob Storage. Se você estiver configurando uma transferência entre nuvens sem agente, não precisará especificar um valor para esse parâmetro.

Você pode especificar mais de um atendente. Para obter mais informações, consulte [Utilizar vários agentes para sua transferência](#).

Note

Você não pode adicionar ou remover agentes de um local de armazenamento depois de criá-lo inicialmente.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obrigatório: Não

AuthenticationType

Especifica o método de autenticação DataSync usado para acessar seu Armazenamento de Blobs do Azure. DataSync pode acessar o armazenamento de blobs usando uma assinatura de acesso compartilhado (SAS).

Tipo: String

Valores Válidos: SAS | NONE

Obrigatório: Não

BlobType

Especifica o tipo de blob que você deseja que seus objetos ou arquivos sejam ao transferi-los para o Armazenamento de Blobs do Azure. Atualmente, DataSync só dá suporte à movimentação de dados para o Armazenamento de Blobs do Azure como blobs de blocos. Para obter mais informações sobre os tipos de blob, consulte a [Documentação do armazenamento de blobs do Azure](#).

Tipo: String

Valores Válidos: BLOCK

Obrigatório: Não

CmkSecretConfig

Especifica as informações de configuração DataSync de um segredo gerenciado, como um token de autenticação ou conjunto de credenciais DataSync usado para acessar um local de transferência específico e um gerenciado pelo cliente. AWS KMS key

Tipo: objeto [CmkSecretConfig](#)

Obrigatório: Não

CustomSecretConfig

Especifica as informações de configuração de um segredo gerenciado pelo cliente, como um token de autenticação ou conjunto de credenciais DataSync usado para acessar um local de transferência específico e um gerenciado pelo cliente. AWS KMS key

Tipo: objeto [CustomSecretConfig](#)

Obrigatório: Não

LocationArn

Especifica o ARN do local de transferência do Armazenamento de Blobs do Azure que você está atualizando.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

[SasConfiguration](#)

Especifica a configuração SAS que permite acessar seu DataSync Armazenamento de Blobs do Azure.

Tipo: objeto [AzureBlobSasConfiguration](#)

Obrigatório: Não

[Subdirectory](#)

Especifica segmentos de caminho se você quiser limitar a transferência para um diretório virtual no contêiner (por exemplo, /my/images).

Tipo: String

Restrições de comprimento: comprimento máximo de 1024.

Padrão: `^[\\p{L}\\p{M}\\p{Z}\\p{S}\\p{N}\\p{P}\\p{C}]]*$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationEfs

Modifica os seguintes parâmetros de configuração do local de transferência do Amazon EFS com AWS DataSync o qual você está usando.

Para obter mais informações, consulte [Configuração de DataSync transferências com o Amazon EFS](#).

Sintaxe da Solicitação

```
{
  "AccessPointArn": "string",
  "FileSystemAccessRoleArn": "string",
  "InTransitEncryption": "string",
  "LocationArn": "string",
  "Subdirectory": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AccessPointArn](#)

Especifica o Amazon Resource Name (ARN) do ponto DataSync de acesso usado para montar seu sistema de arquivos Amazon EFS.

Para obter mais informações, consulte [Acesso a sistemas de arquivos restritos do Amazon EFS](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: (^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-\0-9]+:[0-9]{12}:access-point/fsap-[0-9a-f]{8,40}\$)|(^\$)

Obrigatório: Não

FileSystemAccessRoleArn

Especifica uma função AWS Identity and Access Management (IAM) que permite DataSync acessar seu sistema de arquivos Amazon EFS.

Para obter informações sobre a criação dessa função, consulte [Criação de uma função DataSync do IAM para acesso ao sistema de arquivos do Amazon EFS](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `(^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*)|(^$)`

Obrigatório: Não

InTransitEncryption

Especifica se você deseja usar DataSync a criptografia Transport Layer Security (TLS) 1.2 ao transferir dados para ou do seu sistema de arquivos Amazon EFS.

Se você especificar um ponto de acesso usando `AccessPointArn` ou um perfil do IAM usando `FileSystemAccessRoleArn`, deverá definir esse parâmetro como `TLS1_2`.

Tipo: String

Valores Válidos: `NONE` | `TLS1_2`

Obrigatório: Não

LocationArn

Especifica o Amazon Resource Name (ARN) do local de transferência do Amazon EFS que você está atualizando.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Subdirectory

Especifica um caminho de montagem para seu sistema de arquivos do Amazon EFS. É aqui que DataSync lê ou grava dados em seu sistema de arquivos (dependendo se esse é um local de origem ou destino).

Por padrão, DataSync usa o diretório raiz (ou [ponto de acesso](#), se você fornecer um `usingAccessPointArn`). Você também pode incluir subdiretórios usando barras (por exemplo, `/path/to/folder`).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\+\.\(\)\p{Zs}]*$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationFsxLustre

Modifica os seguintes parâmetros de configuração do local de transferência do Amazon FSx for Lustre com o qual você está usando. AWS DataSync

Para obter mais informações, consulte [Configurando DataSync transferências com o FSx for Lustre](#).

Sintaxe da Solicitação

```
{  
  "LocationArn": "string",  
  "Subdirectory": "string"  
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[LocationArn](#)

Especifica o Amazon Resource Name (ARN) do local de transferência FSx do Lustre que você está atualizando.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

[Subdirectory](#)

Especifica um caminho de montagem para seu sistema de arquivos FSx for Lustre. O caminho pode incluir subdiretórios.

Quando o local é usado como fonte, DataSync lê os dados do caminho de montagem. Quando o local é usado como destino, DataSync grava dados no caminho de montagem. Se você não incluir esse parâmetro, DataSync usa o diretório raiz do sistema de arquivos (/).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\$\p{Zs}]+$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationFsxOntap

Modifica os seguintes parâmetros de configuração do local de transferência do Amazon FSx for NetApp ONTAP com o qual você está usando. AWS DataSync

Para obter mais informações, consulte [Configurando DataSync transferências com o FSx for ONTAP](#).

Sintaxe da Solicitação

```
{
  "LocationArn": "string",
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "Subdirectory": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

Especifica o Amazon Resource Name (ARN) do local de FSx transferência para ONTAP que você está atualizando.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Protocol

Especifica o protocolo de transferência de dados DataSync usado para acessar seu sistema de FSx arquivos da Amazon.

Tipo: objeto [FsxUpdateProtocol](#)

Obrigatório: Não

Subdirectory

Especifica um caminho para o compartilhamento de arquivos na máquina virtual de armazenamento (SVM) para a qual você deseja transferir dados de ou para.

Você pode especificar um caminho de união (também conhecido como ponto de montagem), caminho qtree (para compartilhamentos de arquivos NFS) ou nome de compartilhamento (para compartilhamentos de arquivos SMB). Por exemplo, seu caminho de montagem pode ser `/vol1`, `/vol1/tree1` ou `/share1`.

Note

Não especifique um caminho de junção no volume raiz do SVM. Para obter mais informações, consulte [Gerenciamento FSx de máquinas virtuais de armazenamento ONTAP no Guia](#) do usuário do Amazon FSx for NetApp ONTAP.

Tipo: String

Restrições de tamanho: tamanho máximo de 255.

Padrão: `^[^\\u0000\\u0085\\u2028\\u2029\\r\\n]{1,255}$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationFsxOpenZfs

Modifica os seguintes parâmetros de configuração do local de transferência do Amazon FSx for OpenZFS com o qual você está usando. AWS DataSync

Para obter mais informações, consulte [Configurando DataSync transferências com FSx para OpenZFS](#).

Note

Os parâmetros de solicitação relacionados a SMB não são compatíveis com a operação UpdateLocationFsxOpenZfs.

Sintaxe da Solicitação

```
{
  "LocationArn": "string",
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "Subdirectory": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

Especifica o Amazon Resource Name (ARN) do local de FSx transferência para OpenZFS que você está atualizando.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Protocol

Especifica o protocolo de transferência de dados AWS DataSync usado para acessar seu sistema de FSx arquivos da Amazon.

Tipo: objeto [FsxProtocol](#)

Obrigatório: Não

Subdirectory

Especifica um subdiretório no caminho do local que deve começar com. /fsx DataSync usa esse subdiretório para ler ou gravar dados (dependendo se o sistema de arquivos é um local de origem ou destino).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\\-\\+\\.\\/(\\)\\$\\p{Zs}]+$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationFsxWindows

Modifica os seguintes parâmetros de configuração do local de transferência do Amazon FSx para Windows File Server com AWS DataSync o qual você está usando.

Para obter mais informações, consulte [Configurando DataSync transferências com o FSx Windows File Server](#).

Sintaxe da Solicitação

```
{
  "Domain": "string",
  "LocationArn": "string",
  "Password": "string",
  "Subdirectory": "string",
  "User": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

Domain

Especifica o nome do domínio do Windows ao qual seu sistema FSx de arquivos do Windows File Server pertence.

Se você tiver vários domínios do Active Directory em seu ambiente, a configuração desse parâmetro garante que ele DataSync se conecte ao sistema de arquivos correto.

Tipo: String

Restrições de tamanho: tamanho máximo de 253.

Padrão: `^([A-Za-z0-9](\\.|-+)?[A-Za-z0-9]){0,252})?$`

Obrigatório: Não

LocationArn

Especifica o ARN do local de transferência FSx do Windows File Server que você está atualizando.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

Password

Especifica a senha do usuário com as permissões para montar e acessar os arquivos, pastas e metadados de arquivos no seu FSx sistema de arquivos do Windows File Server.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^.{0,104}$`

Obrigatório: Não

Subdirectory

Especifica um caminho de montagem para seu sistema de arquivos usando barras. DataSync usa esse subdiretório para ler ou gravar dados (dependendo se o sistema de arquivos é um local de origem ou destino).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\\-\\+\\.\\/(\\)\\$\\p{Zs}]+$`

Obrigatório: Não

User

Especifica o usuário com as permissões para montar e acessar os arquivos, pastas e metadados de arquivos no seu FSx sistema de arquivos do Windows File Server.

Para obter informações sobre como escolher um usuário com o nível certo de acesso para sua transferência, consulte [as permissões necessárias](#) FSx para locais do Windows File Server.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E ] { 1 , 104 } $`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)

- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationHdfs

Modifica os seguintes parâmetros de configuração do local de transferência do Hadoop Distributed File System (HDFS) com o qual você está usando. AWS DataSync

Para obter mais informações, consulte [Configurando DataSync transferências com um cluster HDFS](#).

Sintaxe da Solicitação

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "BlockSize": number,
  "KerberosKeytab": blob,
  "KerberosKrb5Conf": blob,
  "KerberosPrincipal": "string",
  "KmsKeyProviderUri": "string",
  "LocationArn": "string",
  "NameNodes": [
    {
      "Hostname": "string",
      "Port": number
    }
  ],
  "QopConfiguration": {
    "DataTransferProtection": "string",
    "RpcProtection": "string"
  },
  "ReplicationFactor": number,
  "SimpleUser": "string",
  "Subdirectory": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AgentArns](#)

Os nomes de recursos da Amazon (ARNs) dos DataSync agentes que podem se conectar ao seu cluster HDFS.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obrigatório: Não

[AuthenticationType](#)

O tipo de autenticação usado para determinar a identidade do usuário.

Tipo: String

Valores Válidos: SIMPLE | KERBEROS

Obrigatório: Não

[BlockSize](#)

O tamanho dos blocos de dados a serem gravados no cluster do HDFS.

Tipo: inteiro

Intervalo válido: valor mínimo de 1.048.576. Valor máximo de 1.073.741.824

Obrigatório: Não

[KerberosKeytab](#)

A tabela de chaves Kerberos (keytab) que contém mapeamentos entre a entidade principal Kerberos definida e as chaves criptografadas. Você pode carregar o keytab de um arquivo fornecendo o endereço do arquivo.

Tipo: objeto de dados binários codificado pelo Base64

Restrições de tamanho: tamanho máximo de 65536.

Obrigatório: Não

[KerberosKrb5Conf](#)

O arquivo `krb5.conf` que contém as informações de configuração do Kerberos. Você pode carregar o arquivo `krb5.conf` fornecendo o endereço do arquivo. Se você estiver usando o AWS CLI, ele executa a codificação base64 para você. Caso contrário, você deve fornecer o texto codificado em base64.

Tipo: objeto de dados binários codificado pelo Base64

Restrições de tamanho: tamanho máximo de 131.072.

Obrigatório: Não

[KerberosPrincipal](#)

A entidade principal do Kerberos com acesso aos arquivos e pastas no cluster do HDFS.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^.+$`

Obrigatório: Não

[KmsKeyProviderUri](#)

O URI do Key Management Server (KMS) do cluster do HDFS.

Tipo: String

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 255.

Padrão: `^kms:\\\\http[s]?@(([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9])(;((([a-zA-Z0-9\\-]*[a-zA-Z0-9])\\.)*([A-Za-z0-9\\-]*[A-Za-z0-9]))*:[0-9]{1,5}\\kms$`

Obrigatório: Não

[LocationArn](#)

O nome do recurso da Amazon (ARN) do local do cluster do HDFS de origem.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

[NameNodes](#)

O NameNode que gerencia o namespace HDFS. O NameNode executa operações como abrir, fechar e renomear arquivos e diretórios. O NameNode contém as informações para mapear blocos de dados para DataNodes o. Você pode usar apenas um NameNode.

Tipo: Matriz de objetos [HdfsNameNode](#)

Membros da matriz: número mínimo de 1 item.

Obrigatório: Não

[QopConfiguration](#)

A configuração da Qualidade da Proteção (QOP) especifica as configurações de privacidade da Chamada de Procedimento Remoto (RPC) e da transferência de dados definidas no cluster do Sistema de Arquivos Distribuído do Hadoop (HDFS).

Tipo: objeto [QopConfiguration](#)

Obrigatório: Não

[ReplicationFactor](#)

O número de DataNodes para os quais replicar os dados ao gravar no cluster HDFS.

Tipo: inteiro

Intervalo válido: valor mínimo de 1. Valor máximo de 512.

Obrigatório: Não

[SimpleUser](#)

O nome de usuário utilizado para identificar o cliente no sistema operacional host.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^[_.A-Za-z0-9][_.A-Za-z0-9]*$`

Obrigatório: Não

[Subdirectory](#)

Um subdiretório no cluster do HDFS. Esse subdiretório é utilizado para ler ou gravar dados no cluster do HDFS.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\$\p{Zs}]+$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationNfs

Modifica os seguintes parâmetros de configuração do local de transferência do Sistema de Arquivos de Rede (NFS) com o qual você está usando. AWS DataSync

Para obter mais informações, consulte [Configurando transferências com um servidor de arquivos NFS](#).

Sintaxe da Solicitação

```
{
  "LocationArn": "string",
  "MountOptions": {
    "Version": "string"
  },
  "OnPremConfig": {
    "AgentArns": [ "string" ]
  },
  "ServerHostname": "string",
  "Subdirectory": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[LocationArn](#)

Especifica o nome do recurso da Amazon (ARN) do local de transferência do NFS que deseja atualizar.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

MountOptions

Especifica como DataSync acessar um local usando o protocolo NFS.

Tipo: objeto [NfsMountOptions](#)

Obrigatório: Não

OnPremConfig

Os AWS DataSync agentes que podem se conectar ao seu servidor de arquivos do Sistema de Arquivos de Rede (NFS).

Tipo: objeto [OnPremConfig](#)

Obrigatório: Não

ServerHostname

Especifica o nome DNS ou o endereço IP versão 4 (IPv4) do servidor de arquivos NFS ao qual seu DataSync agente se conecta.

Tipo: String

Restrições de tamanho: tamanho máximo de 255.

Padrão: `^([a-zA-Z0-9\-\_]*[a-zA-Z0-9])\.([A-Za-z0-9\-\_]*[A-Za-z0-9])$`

Obrigatório: Não

Subdirectory

Especifica o caminho de exportação no servidor de arquivos NFS que você deseja DataSync montar.

Esse caminho (ou um subdiretório do caminho) é onde os dados são DataSync transferidos de ou para. Para obter informações sobre como configurar uma exportação para DataSync, consulte [Acessando servidores de arquivos NFS](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\+\.\^(\)\p{Zs}]+$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)

- [AWS SDK para Ruby V3](#)

UpdateLocationObjectStorage

Modifica os seguintes parâmetros de configuração do local de transferência do armazenamento de objetos com AWS DataSync o qual você está usando.

Para obter mais informações, consulte [Configurando DataSync transferências com um sistema de armazenamento de objetos](#).

Sintaxe da Solicitação

```
{
  "AccessKey": "string",
  "AgentArns": [ "string" ],
  "CmkSecretConfig": {
    "KmsKeyArn": "string",
    "SecretArn": "string"
  },
  "CustomSecretConfig": {
    "SecretAccessRoleArn": "string",
    "SecretArn": "string"
  },
  "LocationArn": "string",
  "SecretKey": "string",
  "ServerCertificate": blob,
  "ServerHostname": "string",
  "ServerPort": number,
  "ServerProtocol": "string",
  "Subdirectory": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AccessKey](#)

Especifica a chave de acesso (por exemplo, um nome de usuário) se as credenciais forem necessárias para autenticação no servidor de armazenamento de objetos.

Tipo: String

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 200.

Padrão: `^.*$`

Obrigatório: Não

[AgentArns](#)

(Opcional) Especifica os nomes de recursos da Amazon (ARNs) dos DataSync agentes que podem se conectar ao seu sistema de armazenamento de objetos. Se você estiver configurando uma transferência entre nuvens sem agente, não precisará especificar um valor para esse parâmetro.

Note

Você não pode adicionar ou remover agentes de um local de armazenamento depois de criá-lo inicialmente.

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obrigatório: Não

[CmkSecretConfig](#)

Especifica as informações de configuração DataSync de um segredo gerenciado, como um token de autenticação ou conjunto de credenciais DataSync usado para acessar um local de transferência específico e um gerenciado pelo cliente. AWS KMS key

Tipo: objeto [CmkSecretConfig](#)

Obrigatório: Não

[CustomSecretConfig](#)

Especifica as informações de configuração de um segredo gerenciado pelo cliente, como um token de autenticação ou conjunto de credenciais DataSync usado para acessar um local de transferência específico e um gerenciado pelo cliente. AWS KMS key

Tipo: objeto [CustomSecretConfig](#)

Obrigatório: Não

[LocationArn](#)

Especifica o ARN do local do sistema de armazenamento de objetos que você está atualizando.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

[SecretKey](#)

Especifica a chave secreta (por exemplo, uma senha) se as credenciais forem necessárias para autenticação no servidor de armazenamento de objetos.

Note

Se você fornecer um segredo usando `SecretKey`, mas não fornecer detalhes de configuração secreta usando `CmkSecretConfig` ou `CustomSecretConfig`, então DataSync armazena o token usando o segredo do Secrets Manager da sua AWS conta.

Tipo: String

Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 200.

Padrão: `^.*$`

Obrigatório: Não

ServerCertificate

Especifica uma cadeia de certificados DataSync para autenticação em seu sistema de armazenamento de objetos se o sistema usar uma autoridade de certificação (CA) privada ou autoassinada. Você deve especificar um único arquivo .pem com uma cadeia de certificados completa (por exemplo, `file:///home/user/.ssh/object_storage_certificates.pem`).

A cadeia de certificados pode incluir:

- O certificado do sistema de armazenamento de objetos
- Todos os certificados intermediários (se for o caso)
- O certificado-raiz da CA assinante

Você pode concatenar os certificados em um arquivo .pem (que pode ter até 32.768 bytes antes da codificação base64). O exemplo de comando `cat` a seguir cria um arquivo `object_storage_certificates.pem` que inclui três certificados:

```
cat object_server_certificate.pem intermediate_certificate.pem  
ca_root_certificate.pem > object_storage_certificates.pem
```

Para usar esse parâmetro, configure `ServerProtocol` para HTTPS.

A atualização desse parâmetro não interfere nas tarefas que estão em andamento.

Tipo: Objeto de dados binários codificado em Base64

Restrições de tamanho: tamanho máximo de 32768.

Obrigatório: Não

ServerHostname

Especifica o nome de domínio ou endereço IP versão 4 (IPv4) do servidor de armazenamento de objetos ao qual seu DataSync agente se conecta.

Tipo: String

Restrições de tamanho: tamanho máximo de 255.

Padrão: `^(([a-zA-Z0-9\-\ ]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-\ :]*[A-Za-z0-9])$`

Obrigatório: Não

ServerPort

Especifica a porta em que o servidor de armazenamento de objetos aceita o tráfego de rede de entrada (por exemplo, a porta 443).

Tipo: inteiro

Intervalo válido: valor mínimo de 1. Valor máximo de 65536.

Obrigatório: Não

ServerProtocol

Especifica o protocolo que o servidor de armazenamento de objetos utiliza para se comunicar.

Tipo: String

Valores Válidos: HTTPS | HTTP

Obrigatório: Não

Subdirectory

Especifica o prefixo de objeto do servidor de armazenamento de objetos. Se esse for um local de origem, DataSync copiará somente objetos com esse prefixo. Se esse for um local de destino, DataSync grava todos os objetos com esse prefixo.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationS3

Modifica os seguintes parâmetros de configuração do local de transferência do Amazon S3 com o qual você está usando. AWS DataSync

Important

Antes de começar, não deixe de ler os seguintes tópicos:

- [Considerações sobre a classe de armazenamento com locais do Amazon S3](#)
- [Avaliando os custos de solicitação do S3 ao usar DataSync](#)

Sintaxe da Solicitação

```
{
  "LocationArn": "string",
  "S3Config": {
    "BucketAccessRoleArn": "string"
  },
  "S3StorageClass": "string",
  "Subdirectory": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

LocationArn

Especifica o Amazon Resource Name (ARN) do local de transferência do Amazon S3 que você está atualizando.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

S3Config

Especifica o Amazon Resource Name (ARN) AWS Identity and Access Management da função DataSync (IAM) usada para acessar seu bucket do S3.

Para obter mais informações, consulte [Fornecendo DataSync acesso aos buckets do S3](#).

Tipo: objeto [S3Config](#)

Obrigatório: Não

S3StorageClass

Especifica a classe de armazenamento que você deseja que seus objetos usem quando o Amazon S3 for um destino de transferência.

Para buckets em Regiões da AWS, o padrão da classe de armazenamento é. STANDARD Para buckets ativados AWS Outposts, o padrão da classe de armazenamento é. OUTPOSTS

Para obter mais informações, consulte [Considerações sobre classes de armazenamento com transferências do Amazon S3](#).

Tipo: String

Valores Válidos: STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL

Obrigatório: Não

Subdirectory

Especifica um prefixo no bucket do S3 que DataSync lê ou grava (dependendo se o bucket é um local de origem ou destino).

Note

DataSync não é possível transferir objetos com um prefixo que comece com uma barra (/) ou inclua ///./, ou /./ padrões. Por exemplo:

- /photos
- photos//2006/January
- photos/./2006/February

- `photos/./2006/March`

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)

- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateLocationSmb

Modifica os seguintes parâmetros de configuração do local de transferência do Server Message Block (SMB) com o qual você está usando. AWS DataSync

Para obter mais informações, consulte [Configurando DataSync transferências com um servidor de arquivos SMB](#).

Sintaxe da Solicitação

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "DnsIpAddresses": [ "string" ],
  "Domain": "string",
  "KerberosKeytab": blob,
  "KerberosKrb5Conf": blob,
  "KerberosPrincipal": "string",
  "LocationArn": "string",
  "MountOptions": {
    "Version": "string"
  },
  "Password": "string",
  "ServerHostname": "string",
  "Subdirectory": "string",
  "User": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[AgentArns](#)

Especifica o DataSync agente (ou agentes) que podem se conectar ao seu servidor de arquivos SMB. Você especifica um agente usando seu nome do recurso da Amazon (ARN).

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obrigatório: Não

AuthenticationType

Especifica o protocolo de autenticação DataSync usado para se conectar ao seu servidor de arquivos SMB. DataSync suporta NTLM (padrão) e KERBEROS autenticação.

Para obter mais informações, consulte [Fornecendo DataSync acesso a servidores de arquivos SMB](#).

Tipo: String

Valores Válidos: NTLM | KERBEROS

Obrigatório: Não

DnsIpAddresses

Especifica os IPv4 endereços dos servidores DNS aos quais seu servidor de arquivos SMB pertence. Esse parâmetro se aplica somente se `AuthenticationType` estiver definido como `KERBEROS`.

Se você tiver vários domínios em seu ambiente, a configuração desse parâmetro garante que ele se DataSync conecte ao servidor de arquivos SMB correto.

Tipo: matriz de strings

Membros da matriz: número máximo de 2 itens.

Restrições de comprimento: comprimento mínimo de 7. Comprimento máximo de 39.

Padrão: `\A((25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\.(25[0-5]|2[0-4]\d|[0-1]?\d?\d)\d)){3}|([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,7}:|([0-9a-fA-F]{1,4}:){1,6}:([0-9a-fA-F]{1,4}|([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2}|([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-fA-F]{1,4}){1,3}|([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4}|([0-9a-fA-F]`

`F]{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5}|[0-9a-fA-F]{1,4}:((:[0-9a-fA-F]{1,4}){1,6}))\z`

Obrigatório: Não

[Domain](#)

Especifica o nome de domínio do Windows ao qual o servidor de arquivos SMB pertence. Esse parâmetro se aplica somente se `AuthenticationType` estiver definido como `NTLM`.

Se você tiver vários domínios em seu ambiente, a configuração desse parâmetro garante que ele se DataSync conecte ao servidor de arquivos correto.

Tipo: String

Restrições de tamanho: tamanho máximo de 253.

Padrão: `^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}$`

Obrigatório: Não

[KerberosKeytab](#)

Especifica seu arquivo de tabela de chaves Kerberos (keytab), que inclui mapeamentos entre suas chaves principais e de criptografia do Kerberos.

Para evitar erros de execução de tarefas, certifique-se de que o principal Kerberos que você usa para criar o arquivo keytab corresponda exatamente ao que você especificou.

`KerberosPrincipal`

Tipo: objeto de dados binários codificado pelo Base64

Restrições de tamanho: tamanho máximo de 65536.

Obrigatório: Não

[KerberosKrb5Conf](#)

Especifica um arquivo de configuração Kerberos (`krb5.conf`) que define sua configuração de região Kerberos.

O arquivo deve ser codificado em base64. Se você estiver usando o AWS CLI, a codificação é feita para você.

Tipo: Objeto de dados binários codificado em Base64

Restrições de tamanho: tamanho máximo de 131.072.

Obrigatório: Não

[KerberosPrincipal](#)

Especifica um kerberos principal, que é uma identidade em seu realm Kerberos que tem permissão para acessar os arquivos, pastas e metadados de arquivos em seu servidor de arquivos SMB.

Talvez seja a aparência de um diretor de Kerberos. `HOST/kerberosuser@MYDOMAIN.ORG`

Os nomes principais diferenciam maiúsculas de minúsculas. A execução da DataSync tarefa falhará se o principal que você especificar para esse parâmetro não corresponder exatamente ao principal usado para criar o arquivo keytab.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^.+`

Obrigatório: Não

[LocationArn](#)

Especifica o ARN do local do SMB que você deseja atualizar.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Exigido: Sim

[MountOptions](#)

Especifica a versão do protocolo Server Message Block (SMB) AWS DataSync usada para acessar um servidor de arquivos SMB.

Tipo: objeto [SmbMountOptions](#)

Obrigatório: Não

Password

Especifica a senha do usuário que pode montar o servidor de arquivos SMB e tenha permissão para acessar os arquivos e pastas envolvidos na sua transferência. Esse parâmetro se aplica somente se `AuthenticationType` estiver definido como `NTLM`.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^.{0,104}$`

Obrigatório: Não

ServerHostname

Especifica o nome de domínio ou endereço IP do servidor de arquivos SMB ao qual seu DataSync agente se conecta.

Lembre-se do seguinte ao configurar esse parâmetro:

- Você não pode especificar um endereço IP versão 6 (IPv6).
- Se você estiver usando a autenticação Kerberos, deverá especificar um nome de domínio.

Tipo: String

Restrições de tamanho: tamanho máximo de 255.

Padrão: `^(( [a-zA-Z0-9\ - ]* [a-zA-Z0-9] )\ . )* ( [A-Za-z0-9\ - : ]* [A-Za-z0-9] )$`

Obrigatório: Não

Subdirectory

Especifica o nome do compartilhamento exportado pelo seu servidor de arquivos SMB onde DataSync lerá ou gravará dados. Você pode incluir um subdiretório no caminho de compartilhamento (por exemplo, `/path/to/subdirectory`). Certifique-se de que outros clientes do SMB em sua rede também possam montar este caminho.

Para copiar todos os dados no subdiretório especificado, DataSync deve ser capaz de montar o compartilhamento SMB e acessar todos os seus dados. Para obter mais informações, consulte [Fornecendo DataSync acesso a servidores de arquivos SMB](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\$\p{Zs}]+$`

Obrigatório: Não

User

Especifica o nome de usuário que pode montar seu servidor de arquivos SMB e tem permissão para acessar os arquivos e pastas envolvidos na sua transferência. Esse parâmetro se aplica somente se `AuthenticationType` estiver definido como NTLM.

Para obter informações sobre como escolher um usuário com o nível certo de acesso para sua transferência, consulte [Fornecendo DataSync acesso a servidores de arquivos SMB](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^[^\x22\x5B\x5D/\\";|, +*?\x3C\x3E]{1,104}$`

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateTask

Atualiza a configuração de uma tarefa, que define onde e como o AWS DataSync transfere os dados.

Sintaxe da Solicitação

```
{
  "CloudWatchLogGroupArn": "string",
  "Excludes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "Includes": [
    {
      "FilterType": "string",
      "Value": "string"
    }
  ],
  "ManifestConfig": {
    "Action": "string",
    "Format": "string",
    "Source": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "ManifestObjectPath": "string",
        "ManifestObjectVersionId": "string",
        "S3BucketArn": "string"
      }
    }
  },
  "Name": "string",
  "Options": {
    "Atime": "string",
    "BytesPerSecond": number,
    "Gid": "string",
    "LogLevel": "string",
    "Mtime": "string",
    "ObjectTags": "string",
    "OverwriteMode": "string",
    "PosixPermissions": "string",
    "PreserveDeletedFiles": "string",
```



```

    "PreserveDevices": "string",
    "SecurityDescriptorCopyFlags": "string",
    "TaskQueueing": "string",
    "TransferMode": "string",
    "Uid": "string",
    "VerifyMode": "string"
  },
  "Schedule": {
    "ScheduleExpression": "string",
    "Status": "string"
  },
  "TaskArn": "string",
  "TaskReportConfig": {
    "Destination": {
      "S3": {
        "BucketAccessRoleArn": "string",
        "S3BucketArn": "string",
        "Subdirectory": "string"
      }
    },
    "ObjectVersionIds": "string",
    "OutputType": "string",
    "Overrides": {
      "Deleted": {
        "ReportLevel": "string"
      },
      "Skipped": {
        "ReportLevel": "string"
      },
      "Transferred": {
        "ReportLevel": "string"
      },
      "Verified": {
        "ReportLevel": "string"
      }
    },
    "ReportLevel": "string"
  }
}

```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[CloudWatchLogGroupArn](#)

Especifica o Amazon Resource Name (ARN) de um grupo de logs da CloudWatch Amazon para monitorar sua tarefa.

Para tarefas do modo Avançado, você deve usar `/aws/datasync` como nome do seu grupo de registros. Por exemplo:

```
arn:aws:logs:us-east-1:111222333444:log-group:/aws/datasync:*
```

Para obter mais informações, consulte [Monitoramento de transferências de dados com o CloudWatch Logs](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 562.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-\0-9]+:[0-9]{12}:log-group:([^\:]*)(:\:)*$`

Obrigatório: Não

[Excludes](#)

Especifica filtros de exclusão que definem os arquivos, objetos e pastas em seu local de origem que você não deseja DataSync transferir. Para obter mais informações e exemplos, consulte [Especificação do que é DataSync transferido usando filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

Obrigatório: Não

Includes

Especifica que os filtros de inclusão definem os arquivos, objetos e pastas em seu local de origem que você deseja DataSync transferir. Para obter mais informações e exemplos, consulte [Especificação do que é DataSync transferido usando filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Membros da Matriz: número mínimo de 0 itens. Número máximo de 1 item.

Obrigatório: Não

ManifestConfig

Configura um manifesto, que é uma lista de arquivos ou objetos que você deseja DataSync transferir. Para obter mais informações e exemplos de configuração, consulte [Especificação do que é DataSync transferido usando um manifesto](#).

Ao usar esse parâmetro, sua identidade de chamador (a função do IAM DataSync com a qual você está usando) deve ter a `iam:PassRole` permissão. A [AWSDataSyncFullAccess](#) política inclui essa permissão.

Para remover uma configuração de manifesto, especifique esse parâmetro como vazio.

Tipo: objeto [ManifestConfig](#)

Obrigatório: Não

Name

Especifica o nome da tarefa.

Tipo: String

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Obrigatório: Não

Options

Indica como sua tarefa de transferência está configurada. Essas opções incluem como DataSync manipula arquivos, objetos e seus metadados associados durante a transferência. Você também

pode especificar como verificar a integridade dos dados, definir limites de largura de banda para sua tarefa, entre outras opções.

Cada opção tem um valor padrão. A menos que seja necessário, você não precisa configurar nenhuma opção antes de ligar [StartTaskExecution](#).

Você também pode substituir suas opções de tarefa para cada execução de tarefa. Por exemplo, pode ser bom ajustar o `LogLevel` para uma execução individual.

Tipo: objeto [Options](#)

Obrigatório: Não

[Schedule](#)

Especifica um agendamento de quando você deseja que a tarefa seja executada. Para obter mais informações, consulte [Programar sua tarefa](#).

Tipo: objeto [TaskSchedule](#)

Obrigatório: Não

[TaskArn](#)

Especifica o ARN da tarefa que você deseja atualizar.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Exigido: Sim

[TaskReportConfig](#)

Especifica como você deseja configurar um relatório de tarefas, que fornece informações detalhadas sobre sua DataSync transferência. Para obter mais informações, consulte [Monitorando suas DataSync transferências com relatórios de tarefas](#).

Ao usar esse parâmetro, sua identidade de chamador (a função do IAM DataSync com a qual você está usando) deve ter a `iam:PassRole` permissão. A [AWSDataSyncFullAccess](#) política inclui essa permissão.

Para remover uma configuração de relatório de tarefa, especifique esse parâmetro como vazio.

Tipo: objeto [TaskReportConfig](#)

Obrigatório: Não

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)

- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

UpdateTaskExecution

Atualiza a configuração da execução de uma AWS DataSync tarefa em execução.

Note

Atualmente, o único Option que você pode modificar com UpdateTaskExecution é [BytesPerSecond](#), que faz o controle de utilização da largura de banda para a execução de uma tarefa em execução ou em fila.

Sintaxe da Solicitação

```
{
  "Options": {
    "Atime": "string",
    "BytesPerSecond": number,
    "Gid": "string",
    "LogLevel": "string",
    "Mtime": "string",
    "ObjectTags": "string",
    "OverwriteMode": "string",
    "PosixPermissions": "string",
    "PreserveDeletedFiles": "string",
    "PreserveDevices": "string",
    "SecurityDescriptorCopyFlags": "string",
    "TaskQueueing": "string",
    "TransferMode": "string",
    "Uid": "string",
    "VerifyMode": "string"
  },
  "TaskExecutionArn": "string"
}
```

Parâmetros da solicitação

Para obter informações sobre os parâmetros que são comuns em todas as ações, consulte [Parâmetros comuns](#).

A solicitação aceita os dados a seguir no formato JSON.

[Options](#)

Indica como sua tarefa de transferência está configurada. Essas opções incluem como DataSync manipula arquivos, objetos e seus metadados associados durante a transferência. Você também pode especificar como verificar a integridade dos dados, definir limites de largura de banda para sua tarefa, entre outras opções.

Cada opção tem um valor padrão. A menos que seja necessário, você não precisa configurar nenhuma opção antes de ligar [StartTaskExecution](#).

Você também pode substituir suas opções de tarefa para cada execução de tarefa. Por exemplo, pode ser bom ajustar o `LogLevel` para uma execução individual.

Tipo: objeto [Options](#)

Obrigatório: Sim

[TaskExecutionArn](#)

Especifica o nome do recurso da Amazon (ARN) da execução da tarefa que você está atualizando.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Exigido: Sim

Elementos de Resposta

Se a ação for bem-sucedida, o serviço reenviará uma resposta 200 HTTP com um corpo HTTP vazio.

Erros

Para obter informações sobre os erros comuns que todas as ações retornam, consulte [Erros comuns](#).

InternalException

Essa exceção é lançada quando ocorre um erro no serviço AWS DataSync .

Código de status HTTP: 500

InvalidRequestException

Essa exceção é lançada quando o cliente envia uma solicitação malformada.

Código de Status HTTP: 400

Consulte Também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS Command Line Interface](#)
- [AWS SDK para .NET](#)
- [AWS SDK para C++](#)
- [AWS SDK para Go v2](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para JavaScript V3](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK para PHP V3](#)
- [AWS SDK para Python](#)
- [AWS SDK para Ruby V3](#)

Tipos de dados

Os seguintes tipos de dados são compatíveis:

- [AgentListEntry](#)
- [AzureBlobSasConfiguration](#)
- [CmkSecretConfig](#)
- [CustomSecretConfig](#)

- [Ec2Config](#)
- [FilterRule](#)
- [FsxProtocol](#)
- [FsxProtocolNfs](#)
- [FsxProtocolSmb](#)
- [FsxUpdateProtocol](#)
- [FsxUpdateProtocolSmb](#)
- [HdfsNameNode](#)
- [LocationFilter](#)
- [LocationListEntry](#)
- [ManagedSecretConfig](#)
- [ManifestConfig](#)
- [NfsMountOptions](#)
- [OnPremConfig](#)
- [Options](#)
- [Platform](#)
- [PrivateLinkConfig](#)
- [QopConfiguration](#)
- [ReportDestination](#)
- [ReportDestinationS3](#)
- [ReportOverride](#)
- [ReportOverrides](#)
- [ReportResult](#)
- [S3Config](#)
- [S3ManifestConfig](#)
- [SmbMountOptions](#)
- [SourceManifestConfig](#)
- [TagListEntry](#)
- [TaskExecutionFilesFailedDetail](#)
- [TaskExecutionFilesListedDetail](#)

- [TaskExecutionListEntry](#)
- [TaskExecutionResultDetail](#)
- [TaskFilter](#)
- [TaskListEntry](#)
- [TaskReportConfig](#)
- [TaskSchedule](#)
- [TaskScheduleDetails](#)

AgentListEntry

Representa uma única entrada em uma lista (ou matriz) de AWS DataSync agentes quando você chama a [ListAgents](#) operação.

Conteúdo

AgentArn

O nome de recurso da Amazon (ARN) de um DataSync agente.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Obrigatório: Não

Name

O nome de um agente.

Tipo: String

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\\s+=. _:@/-]+$`

Obrigatório: Não

Platform

Os detalhes relacionados à plataforma sobre o agente, como o número da versão.

Tipo: objeto [Platform](#)

Obrigatório: Não

Status

O status de um agente.

- Se o status for ONLINE, o agente está configurado corretamente e pronto para uso.

- Se o status for OFFLINE, o agente esteve fora de contato DataSync por cinco minutos ou mais. Isso pode acontecer por alguns motivos. Para obter mais informações, consulte [O que eu faço se meu agente estiver off-line?](#)

Tipo: String

Valores Válidos: ONLINE | OFFLINE

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

AzureBlobSasConfiguration

A configuração de assinatura de acesso compartilhado (SAS) que permite AWS DataSync acessar seu Microsoft Azure Blob Storage.

Para obter mais informações, consulte [Tokens SAS](#) para acessar seu Azure Blob Storage.

Conteúdo

Token

Especifica um token SAS que fornece permissões para acessar seu Azure Blob Storage.

O token faz parte da string SAS URI que vem depois do URI do recurso de armazenamento e de um ponto de interrogação. Um token é semelhante ao seguinte:

```
sp=r&st=2023-12-20T14:54:52Z&se=2023-12-20T22:54:52Z&spr=https&sv=2021-06-08&s%2FXTI9E%2F%2Fmq171%2BZU178wcwqU%3D
```

Tipo: String

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 255.

Padrão: ^.+ \$

Exigido: Sim

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CmkSecretConfig

Especifica as informações de configuração DataSync de um segredo gerenciado, como um token de autenticação ou uma chave secreta DataSync usada para acessar um local de armazenamento específico, com um gerenciado pelo cliente. AWS KMS key

Note

Você pode usar uma CmkSecretConfig ou CustomSecretConfig para fornecer credenciais para uma CreateLocation solicitação. Não forneça os dois parâmetros para a mesma solicitação.

Conteúdo

KmsKeyArn

Especifica o ARN do servidor gerenciado pelo AWS KMS key cliente DataSync que usa para criptografar o segredo gerenciado armazenado DataSync para. SecretArn DataSync fornece essa chave para AWS Secrets Manager.

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):kms:[a-z\-\0-9]+:[0-9]{12}:key/.*)$`

Obrigatório: Não

SecretArn

Especifica o ARN para DataSync o segredo AWS Secrets Manager gerenciado que é usado para acessar um local de armazenamento específico. Essa propriedade é gerada por DataSync e é somente para leitura. DataSync criptografa esse segredo com a chave KMS que você especifica.

KmsKeyArn

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-\0-9]+:[0-9]{12}:secret:.*)$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CustomSecretConfig

Especifica as informações de configuração para um segredo do Secrets Manager gerenciado pelo cliente em que um token de autenticação do local de armazenamento ou uma chave secreta são armazenados em texto sem formatação. Essa configuração inclui o ARN secreto e o ARN de uma função do IAM que fornece acesso ao segredo.

Note

Você pode usar uma `CmkSecretConfig` ou `CustomSecretConfig` para fornecer credenciais para uma `CreateLocation` solicitação. Não forneça os dois parâmetros para a mesma solicitação.

Conteúdo

SecretAccessRoleArn

Especifica o ARN AWS Identity and Access Management da função DataSync usada para acessar o segredo especificado para. `SecretArn`

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/[a-zA-Z0-9+=,._@-]+)|)$`

Obrigatório: Não

SecretArn

Especifica o ARN de um segredo. AWS Secrets Manager

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-\0-9]+:[0-9]{12}:secret:.*)$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Ec2Config

A sub-rede e os grupos de segurança AWS DataSync usados para se conectar a um dos [destinos de montagem](#) do seu sistema de arquivos Amazon EFS.

Conteúdo

SecurityGroupArns

Especifica os nomes de recursos da Amazon (ARNs) dos grupos de segurança associados ao destino de montagem do sistema de arquivos Amazon EFS.

Tipo: matriz de strings

Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Exigido: Sim

SubnetArn

Especifica o ARN de uma sub-rede DataSync onde cria as interfaces de [rede para gerenciar o](#) tráfego durante sua transferência.

A sub-rede deve estar localizada:

- Na mesma nuvem privada virtual (VPC) que o sistema de arquivos do Amazon EFS.
- Na mesma zona de disponibilidade que pelo menos um destino de montagem para o sistema de arquivos do Amazon EFS.

Note

Você não precisa especificar uma sub-rede que inclua um destino de montagem do sistema de arquivos.

Tipo: string

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:subnet/.*$`

Exigido: Sim

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FilterRule

Especifica quais arquivos, pastas e objetos devem ser incluídos ou excluídos ao transferir arquivos da origem para o destino.

Conteúdo

FilterType

O tipo de regra de filtro a ser aplicada. AWS DataSync só suporta o tipo de regra `SIMPLE_PATTERN`.

Tipo: string

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^[A-Z0-9_]+$`

Valores Válidos: `SIMPLE_PATTERN`

Obrigatório: não

Value

Uma única string de filtro que consiste nos padrões a serem incluídos ou excluídos. Os padrões são delimitados por “|” (isto é, um pipe), por exemplo: `/folder1|/folder2`

Tipo: string

Restrições de comprimento: comprimento máximo de 102.400.

Padrão: `^[^\x00]+$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FsxProtocol

Especifica o protocolo de transferência de dados AWS DataSync usado para acessar seu sistema de FSx arquivos da Amazon.

Conteúdo

NFS

Especifica a configuração do protocolo Network File System (NFS) DataSync usada para acessar seu FSx sistema de arquivos OpenZFS ou a máquina virtual de armazenamento (FSx SVM) do sistema de arquivos ONTAP.

Tipo: objeto [FsxProtocolNfs](#)

Obrigatório: não

SMB

Especifica a configuração do protocolo Server Message Block (SMB) DataSync usada para acessar seu FSx SVM do sistema de arquivos ONTAP.

Tipo: objeto [FsxProtocolSmb](#)

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FsxProtocolNfs

Especifica a configuração do protocolo Network File System (NFS) DataSync usada para acessar seu FSx sistema de arquivos OpenZFS ou a máquina virtual de armazenamento (FSx SVM) do sistema de arquivos ONTAP.

Conteúdo

MountOptions

Especifica como DataSync acessar um local usando o protocolo NFS.

Tipo: objeto [NfsMountOptions](#)

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FsxProtocolSmb

Especifica a configuração do protocolo Server Message Block (SMB) AWS DataSync usada para acessar a máquina virtual de armazenamento (SVM) do sistema de arquivos Amazon FSx for NetApp ONTAP. Para obter mais informações, consulte [Fornecendo DataSync acesso aos sistemas FSx de arquivos ONTAP](#).

Conteúdo

Password

Especifica a senha de um usuário que tem permissão para acessar seu SVM.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^\.{0,104}$`

Exigido: Sim

User

Especifica um usuário que pode montar e acessar os arquivos, pastas e metadados necessários na SVM.

Para obter informações sobre a escolha de um usuário com o nível certo de acesso para a transferência, consulte [Uso do protocolo SMB](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E ] { 1 , 104 } $`

Exigido: Sim

Domain

Especifica o nome do domínio do Windows ao qual sua máquina virtual de armazenamento (SVM) pertence.

Se você tiver vários domínios em seu ambiente, definir essa configuração garante que ele se DataSync conecte ao SVM correto.

Se você tiver vários domínios do Active Directory em seu ambiente, a configuração desse parâmetro garante que ele se DataSync conecte ao SVM correto.

Tipo: String

Restrições de tamanho: tamanho máximo de 253.

Padrão: `^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}$`

Obrigatório: Não

MountOptions

Especifica a versão do protocolo Server Message Block (SMB) AWS DataSync usada para acessar um servidor de arquivos SMB.

Tipo: objeto [SmbMountOptions](#)

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FsxUpdateProtocol

Especifica o protocolo de transferência de dados AWS DataSync usado para acessar seu sistema de FSx arquivos da Amazon.

Note

Você não pode atualizar a configuração do protocolo Network File System (NFS) FSx para locais ONTAP. DataSync atualmente só oferece suporte ao NFS versão 3 com esse tipo de local.

Conteúdo

NFS

Especifica a configuração do protocolo Network File System (NFS) DataSync usada para acessar seu FSx sistema de arquivos OpenZFS ou a máquina virtual de armazenamento (FSx SVM) do sistema de arquivos ONTAP.

Tipo: objeto [FsxProtocolNfs](#)

Obrigatório: Não

SMB

Especifica a configuração do protocolo Server Message Block (SMB) DataSync usada para acessar sua FSx máquina virtual de armazenamento (SVM) do sistema de arquivos ONTAP.

Tipo: objeto [FsxUpdateProtocolSmb](#)

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para Ruby V3](#)

FsxUpdateProtocolSmb

Especifica a configuração do protocolo Server Message Block (SMB) AWS DataSync usada para acessar a máquina virtual de armazenamento (SVM) do sistema de arquivos Amazon FSx for NetApp ONTAP. Para obter mais informações, consulte [Fornecendo DataSync acesso aos sistemas FSx de arquivos ONTAP](#).

Conteúdo

Domain

Especifica o nome do domínio do Windows ao qual sua máquina virtual de armazenamento (SVM) pertence.

Se você tiver vários domínios do Active Directory em seu ambiente, a configuração desse parâmetro garante que ele se DataSync conecte ao SVM correto.

Tipo: String

Restrições de tamanho: tamanho máximo de 253.

Padrão: `^[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}?\\$`

Obrigatório: Não

MountOptions

Especifica a versão do protocolo Server Message Block (SMB) AWS DataSync usada para acessar um servidor de arquivos SMB.

Tipo: objeto [SmbMountOptions](#)

Obrigatório: Não

Password

Especifica a senha de um usuário que tem permissão para acessar seu SVM.

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^.{0,104}\\$`

Obrigatório: Não

User

Especifica um usuário que pode montar e acessar os arquivos, pastas e metadados necessários na SVM.

Para obter informações sobre a escolha de um usuário com o nível certo de acesso para a transferência, consulte [Uso do protocolo SMB](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 104.

Padrão: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E]{1,104}$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

HdfsNameNode

O NameNode do Hadoop Distributed File System (HDFS). O NameNode gerencia o namespace do sistema de arquivos. O NameNode executa operações como abrir, fechar e renomear arquivos e diretórios. O NameNode contém as informações para mapear blocos de dados para DataNodes o.

Conteúdo

Hostname

O nome do host do NameNode no cluster HDFS. Esse valor é o endereço IP ou o nome do Serviço de Nomes de Domínio (DNS) do NameNode. Um agente instalado localmente usa esse nome de host para se comunicar com o NameNode na rede.

Tipo: string

Restrições de comprimento: tamanho mínimo de 1. Comprimento máximo de 255.

Padrão: `^(( [a-zA-Z0-9\ -]*[a-zA-Z0-9] )\ . )*( [A-Za-z0-9\ -]*[A-Za-z0-9] )$`

Exigido: Sim

Port

A porta que o NameNode usa para ouvir as solicitações do cliente.

Tipo: inteiro

Faixa válida: valor mínimo de 1. Valor máximo de 65536.

Obrigatório: sim

Consulte também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

LocationFilter

Limite a lista de recursos retornados por `ListLocations`. Por exemplo, para ver todos os seus locais do Amazon S3, crie um filtro usando `"Name": "LocationType", "Operator": "Equals"` e `"Values": "S3"`.

Para obter mais informações, consulte [Recursos de filtragem](#).

Conteúdo

Name

O nome do filtro que está sendo usado. Cada chamada de API é compatível com uma lista de filtros que estão disponíveis para ela (por exemplo, `LocationType` para `ListLocations`).

Tipo: string

Valores Válidos: `LocationUri` | `LocationType` | `CreationTime`

Obrigatório: sim

Operator

O operador usado para comparar valores de filtro (por exemplo, `Equals` ou `Contains`).

Tipo: string

Valores Válidos: `Equals` | `NotEquals` | `In` | `LessThanOrEqualTo` | `LessThan` | `GreaterThanEqualTo` | `GreaterThan` | `Contains` | `NotContains` | `BeginsWith`

Obrigatório: sim

Values

Os valores que você deseja filtrar. Por exemplo, talvez você queira exibir somente locais do Amazon S3.

Tipo: matriz de strings

Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 255.

Padrão: `^[0-9a-zA-Z_\ \-:\*\.\ \\/\?\-]*$`

Exigido: Sim

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

LocationListEntry

Representa uma única entrada em uma lista de locais. `LocationListEntry` retorna uma matriz que contém uma lista de locais quando a [ListLocations](#) operação é chamada.

Conteúdo

LocationArn

O nome do recurso da Amazon (ARN) do local. Para o Network File System (NFS) ou o Amazon EFS, o local é o caminho de exportação. Para o Amazon S3, o local é o caminho do prefixo que você deseja montar e usar como a raiz do local.

Tipo: string

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

Obrigatório: não

LocationUri

Representa uma lista URIs de um local. `LocationUri` retorna uma matriz que contém uma lista de locais quando a [ListLocations](#) operação é chamada.

Formato: `TYPE://GLOBAL_ID/SUBDIR`.

TYPE designa o tipo de local (por exemplo, `nfs` ou `s3`).

GLOBAL_ID é o identificador globalmente exclusivo do recurso que respalda o local. Um exemplo para o EFS é `us-east-2.fs-abcd1234`. Um exemplo para o Amazon S3 é o nome do bucket, como `myBucket`. Um exemplo de NFS é um IPv4 endereço válido ou um nome de host compatível com o Serviço de Nomes de Domínio (DNS).

SUBDIR é um caminho válido do sistema de arquivos, delimitado por barras, seguindo a convenção `*nix`. Para NFS e Amazon EFS, é o caminho de exportação para criar o local. Para o Amazon S3, é o caminho do prefixo que você monta e usa como a raiz do local.

Tipo: string

Restrições de tamanho: tamanho máximo de 4.360.

Padrão: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ManagedSecretConfig

Especifica as informações de configuração DataSync de um segredo gerenciado, como um token de autenticação ou um conjunto de credenciais DataSync usado para acessar um local de transferência específico. DataSync usa a chave KMS AWS gerenciada padrão para criptografar esse segredo.

AWS Secrets Manager

Conteúdo

SecretArn

Especifica o ARN de um segredo. AWS Secrets Manager

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-\0-9]+:[0-9]{12}:secret:.*|)$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ManifestConfig

Configura um manifesto, que é uma lista de arquivos ou objetos que você deseja AWS DataSync transferir. Para obter mais informações e exemplos de configuração, consulte [Especificação do que é DataSync transferido usando um manifesto](#).

Conteúdo

Action

Especifica para que DataSync serve o manifesto.

Tipo: String

Valores Válidos: TRANSFER

Obrigatório: Não

Format

Especifica o formato de arquivo do manifesto. Para obter mais informações, consulte [Creating a manifest](#).

Tipo: String

Valores Válidos: CSV

Obrigatório: Não

Source

Especifica o manifesto que você deseja DataSync usar e onde ele está hospedado.

Note

Você deve especificar esse parâmetro for configurar um novo manifesto depois de 7 de fevereiro de 2024.

Caso contrário, você receberá um código de status 400 e um `ValidationException` erro informando que está faltando a função do IAM DataSync para acessar o bucket do S3 em que você está hospedando seu manifesto. Para obter mais informações, consulte [Fornecendo DataSync acesso ao seu manifesto](#).

Tipo: objeto [SourceManifestConfig](#)

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

NfsMountOptions

Especifica como DataSync acessar um local usando o protocolo NFS.

Conteúdo

Version

Especifica a versão do NFS que você deseja usar DataSync ao montar seu compartilhamento NFS. Se o servidor se recusar a usar a versão especificada, a tarefa apresentará falha.

Você pode especificar as seguintes opções:

- **AUTOMATIC**(padrão): DataSync escolhe a versão 4.1 do NFS.
- **NFS3**: versão de protocolo stateless que permite gravações assíncronas no servidor.
- **NFSv4_0**: versão de protocolo stateful, amigável para firewalls, que suporta delegações e pseudossistemas de arquivos.
- **NFSv4_1**: versão de protocolo stateful que suporta sessões, delegações de diretório e processamento de dados paralelo. NFS versão 4.1 também inclui todos os recursos disponíveis na versão 4.0.

Note

DataSync atualmente só oferece suporte ao NFS versão 3 com Amazon FSx para locais NetApp ONTAP.

Tipo: string

Valores Válidos: **AUTOMATIC** | **NFS3** | **NFS4_0** | **NFS4_1**

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

OnPremConfig

Os AWS DataSync agentes que podem se conectar ao seu servidor de arquivos do Sistema de Arquivos de Rede (NFS).

Conteúdo

AgentArns

Os nomes de recursos da Amazon (ARNs) dos DataSync agentes que podem se conectar ao seu servidor de arquivos NFS.

Você pode especificar mais de um atendente. Para obter mais informações, consulte [Uso de vários DataSync agentes](#).

Tipo: matriz de strings

Membros da matriz: número mínimo de 1 item. Número máximo de 4 itens.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]+:[0-9]{12}:agent/agent-[0-9a-z]{17}$`

Exigido: Sim

Consulte também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Options

Indica como sua tarefa de transferência está configurada. Essas opções incluem como DataSync manipula arquivos, objetos e seus metadados associados durante a transferência. Você também pode especificar como verificar a integridade dos dados, definir limites de largura de banda para sua tarefa, entre outras opções.

Cada opção tem um valor padrão. A menos que seja necessário, você não precisa configurar nenhuma opção antes de ligar [StartTaskExecution](#).

Você também pode substituir suas opções de tarefa para cada execução de tarefa. Por exemplo, pode ser bom ajustar o `LogLevel` para uma execução individual.

Conteúdo

Atime

Especifica se os metadados que indicam a última vez que um arquivo foi lido ou gravado devem ser preservados.

Note

O comportamento do `Atime` não é totalmente padrão em todas as plataformas, então só DataSync posso fazer isso com base no melhor esforço.

- `BEST_EFFORT`(padrão) - DataSync tenta preservar o `Atime` atributo original em todos os arquivos de origem (ou seja, a versão anterior às PREPARING etapas da execução da tarefa). Essa opção não é recomendada.
- `NONE`: ignora `Atime`.

Note

Se `Atime` estiver definido como `BEST_EFFORT`, o `Mtime` deverá ser definido como `PRESERVE`.

Se `Atime` estiver definido como `NONE`, o `Mtime` também deverá ser `NONE`.

Tipo: String

Valores Válidos: NONE | BEST_EFFORT

Obrigatório: Não

BytesPerSecond

Limita a largura de banda usada por uma DataSync tarefa. Por exemplo, se você quiser DataSync usar no máximo 1 MB, defina esse valor como 1048576 (=1024*1024).

Note

Não aplicável às [tarefas do modo Avançado](#).

Tipo: longo

Intervalo válido: valor mínimo de -1.

Obrigatório: Não

Gid

O ID do grupo (GID) POSIX dos proprietários do arquivo.

- INT_VALUE (padrão): preserva o valor inteiro do ID do usuário (UID) e do ID de grupo (GID), o que é recomendado.
- NONE: ignora o UID e o GID.

Para obter mais informações, consulte [Entendendo como DataSync manipula metadados de arquivos e objetos](#).

Tipo: String

Valores Válidos: NONE | INT_VALUE | NAME | BOTH

Obrigatório: Não

LogLevel

Especifica o tipo de registros que são DataSync publicados em um grupo de registros do Amazon CloudWatch Logs. Para especificar o grupo de registros, consulte [CloudWatchLogGroupArn](#).

- BASIC: publica logs apenas com informações básicas (como erros de transferência).

- **TRANSFER-** Publica registros de todos os arquivos ou objetos que sua DataSync tarefa transfere e realiza verificações de integridade de dados.
- **OFF:** nenhum log é publicado.

Tipo: String

Valores Válidos: OFF | BASIC | TRANSFER

Obrigatório: Não

Mtime

Especifica se os metadados devem ser preservados indicando a última vez em que um arquivo foi gravado antes da PREPARING etapa de execução da tarefa. Esta opção é necessária para casos em que você precisa executar a mesma tarefa mais de uma vez.

- **PRESERVE** (padrão): preserva o Mtime original, o que é recomendado.
- **NONE:** ignora Mtime.

Note

Se Mtime estiver definido como PRESERVE, o Atime deverá ser definido como BEST_EFFORT.

Se Mtime estiver definido como NONE, o Atime também deverá ser definido como NONE.

Tipo: String

Valores Válidos: NONE | PRESERVE

Obrigatório: Não

ObjectTags

Especifica se você deseja DataSync PRESERVE objetar tags (comportamento padrão) ao transferir entre sistemas de armazenamento de objetos. Se você quiser que sua DataSync tarefa ignore as tags de objeto, especifique o NONE valor.

Tipo: String

Valores Válidos: PRESERVE | NONE

Obrigatório: Não

OverwriteMode

Especifica se os dados DataSync devem ser modificados ou preservados no local de destino.

- ALWAYS (padrão) - DataSync modifica os dados no local de destino quando os dados de origem (incluindo metadados) são alterados.

Se DataSync sobrescrever objetos, você poderá incorrer em cobranças adicionais para determinadas classes de armazenamento do Amazon S3 (por exemplo, para recuperação ou exclusão antecipada). Para obter mais informações, consulte [Considerações sobre classes de armazenamento com transferências do Amazon S3](#).

- NEVER - DataSync não sobrescreve os dados no local de destino, mesmo que os dados de origem tenham sido alterados. Você pode usar essa opção como proteção contra a substituição de alterações feitas em arquivos ou objetos no destino.

Tipo: String

Valores Válidos: ALWAYS | NEVER

Obrigatório: Não

PosixPermissions

Especifica quais usuários ou grupos podem acessar um arquivo para uma finalidade específica, como leitura, gravação ou execução do arquivo.

Para obter mais informações, consulte [Entendendo como DataSync manipula metadados de arquivos e objetos](#).

- PRESERVE (padrão): preserva as permissões no estilo POSIX, o que é recomendado.
- NONE: ignora as permissões no estilo POSIX.

Note

DataSync pode preservar as permissões existentes de um local de origem.

Tipo: String

Valores Válidos: NONE | PRESERVE

Obrigatório: Não

PreserveDeletedFiles

Especifica se os arquivos no local de destino que não existem na origem devem ser preservados. Esta opção pode afetar seu custo do armazenamento no Amazon S3. Se a tarefa excluir objetos, você poderá estar sujeito a cobranças mínimas de duração de armazenamento para determinadas classes de armazenamento. Para obter informações detalhadas, consulte [Considerações ao trabalhar com as classes de armazenamento do Amazon S3](#) em. DataSync

- PRESERVE (padrão): ignora esses arquivos de destino, o que é recomendado.
- REMOVE: exclui os arquivos de destino que não estão presentes na origem.

Note

Se você definir este parâmetro como REMOVE, não poderá definir `TransferMode` como ALL. Quando você transfere todos os dados, DataSync não escaneia sua localização de destino e não sabe o que excluir.

Tipo: String

Valores Válidos: PRESERVE | REMOVE

Obrigatório: Não

PreserveDevices

Especifica se os metadados dos dispositivos de blocos e caracteres DataSync devem ser preservados no local de origem e recriar os arquivos com o nome do dispositivo e os metadados no destino. DataSync copia somente o nome e os metadados desses dispositivos.

Note

DataSync não consegue copiar o conteúdo real desses dispositivos porque eles não são terminais e não retornam um marcador end-of-file (EOF).

- NONE (padrão): ignora dispositivos especiais (recomendado).
- PRESERVE: preserva os metadados de caractere e dispositivo de blocos. Esta opção não é compatível, no momento, com o Amazon EFS.

Tipo: String

Valores Válidos: NONE | PRESERVE

Obrigatório: Não

SecurityDescriptorCopyFlags

Especifica os componentes do descritor de segurança SMB que são copiados dos objetos de origem para o destino.

Esse valor é usado somente para transferências entre SMB e Amazon FSx para locais do Windows File Server ou entre dois FSx para locais do Windows File Server. Para obter mais informações, consulte [Entendendo como DataSync manipula metadados de arquivos e objetos](#).

- OWNER_DACL (padrão) - Para cada objeto copiado, DataSync copia os seguintes metadados:
 - O proprietário do objeto.
 - Listas de controle de acesso discrecional do NTFS (DACLS), que determinam se o acesso a um objeto deve ser concedido.

DataSync não copiará listas de controle de acesso do sistema NTFS (SACLs) com essa opção.

- OWNER_DACL_SACL - Para cada objeto copiado, DataSync copie os seguintes metadados:
 - O proprietário do objeto.
 - Listas de controle de acesso discrecional do NTFS (DACLS), que determinam se o acesso a um objeto deve ser concedido.
 - SACLs, que são usados pelos administradores para registrar tentativas de acesso a um objeto protegido.

A cópia SACLs requer a concessão de permissões adicionais ao usuário do Windows que DataSync usa para acessar sua localização SMB. Para obter informações sobre como escolher um usuário com as permissões corretas, consulte [Permissões necessárias para SMB](#), [FSx Windows File Server](#) ou [FSx ONTAP](#) (dependendo do tipo de local em sua transferência).

- NONE: nenhum dos componentes do descritor de segurança SMB é copiado. Os objetos de destino pertencem ao usuário que foi fornecido para acessar o local de destino. DACLS e SACLs são definidos com base na configuração do servidor de destino.

Tipo: String

Valores Válidos: NONE | OWNER_DACL | OWNER_DACL_SACL

Obrigatório: Não

TaskQueueing

Especifica se suas tarefas de transferência devem ser colocadas em uma fila em determinados cenários ao [executar várias tarefas](#). Isto é ENABLED por padrão.

Tipo: String

Valores Válidos: ENABLED | DISABLED

Obrigatório: Não

TransferMode

Especifica se DataSync transfere somente os dados (incluindo metadados) que diferem entre os locais após uma cópia inicial ou se transfere todos os dados sempre que você executa a tarefa. Se você planeja transferências recorrentes, talvez queira transferir apenas o que mudou desde a execução anterior da tarefa.

- CHANGED(padão) - Após a transferência inicial completa, DataSync copia somente os dados e os metadados que diferem entre o local de origem e o local de destino.
- ALL- DataSync copia tudo na origem para o destino sem comparar as diferenças entre os locais.

Tipo: String

Valores Válidos: CHANGED | ALL

Obrigatório: Não

Uid

Especifica o ID de usuário (UID) do POSIX do proprietário do arquivo.

- INT_VALUE (padrão): preserva o valor inteiro do UID do usuário e do ID de grupo (GID), o que é recomendado.
- NONE: ignora o UID e o GID.

Para obter mais informações, consulte [Metadados copiados por. DataSync](#)

Tipo: String

Valores Válidos: NONE | INT_VALUE | NAME | BOTH

Obrigatório: Não

VerifyMode

Especifica se e como DataSync verifica a integridade dos seus dados no final da transferência.

- **ONLY_FILES_TRANSFERRED**(recomendado) - DataSync calcula a soma de verificação dos dados transferidos (incluindo metadados) no local de origem. Ao final da transferência, DataSync compara essa soma de verificação com a soma de verificação calculada com base nesses dados no destino.

Note

Essa é a opção padrão para [tarefas do modo Avançado](#).

Recomendamos esta opção ao transferir para as classes de armazenamento do S3 Glacier Flexible Retrieval ou para o S3 Glacier Deep Archive. Para obter mais informações, consulte [Considerações sobre a classe de armazenamento com locais do Amazon S3](#).

- **POINT_IN_TIME_CONSISTENT**- Ao final da transferência, DataSync verifica toda a origem e o destino para verificar se os dois locais estão totalmente sincronizados.

Note

Essa é a opção padrão para [tarefas do modo Básico](#) e atualmente não é compatível com as tarefas do modo Avançado.

Se você usa um [manifesto](#), DataSync apenas digitaliza e verifica o que está listado no manifesto.

Você não pode usar esta opção em transferências para as classes de armazenamento S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Para obter mais informações, consulte [Considerações sobre a classe de armazenamento com locais do Amazon S3](#).

- **NONE**- DataSync realiza verificações de integridade de dados somente durante sua transferência. Ao contrário de outras opções, não há verificação adicional no fim da transferência.

Tipo: String

Valores Válidos: **POINT_IN_TIME_CONSISTENT** | **ONLY_FILES_TRANSFERRED** | **NONE**

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Platform

Os detalhes relacionados à plataforma sobre o AWS DataSync agente, como o número da versão.

Conteúdo

Version

A versão do DataSync agente.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^[a-zA-Z0-9\s+=. _:@/- ]+$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

PrivateLinkConfig

Especifica como seu AWS DataSync agente se conecta AWS usando um endpoint de serviço de [nuvem privada virtual \(VPC\)](#). Um agente que usa um endpoint da VPC não está acessível pela Internet pública.

Conteúdo

PrivateLinkEndpoint

Especifica o endpoint da VPC fornecido por [AWS PrivateLink](#) pelo qual seu agente se conecta.

Tipo: String

Restrições de comprimento: comprimento mínimo de 7. Comprimento máximo de 15.

Padrão: `\A(25[0-5]|2[0-4]\d|[0-1]?\d?\d)(\.(25[0-5]|2[0-4]\d|[0-1]?\d?\d)){3}\z`

Obrigatório: Não

SecurityGroupArns

Especifica os nomes de recursos da Amazon (ARN) do grupo de segurança que DataSync fornece acesso ao seu VPC endpoint. Você pode especificar apenas ARN.

Tipo: matriz de strings

Membros da matriz: número fixo de 1 item.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:security-group/sg-[a-f0-9]+$`

Obrigatório: Não

SubnetArns

Especifica o ARN da sub-rede em que seu endpoint da VPC está localizado. Você pode especificar apenas ARN.

Tipo: matriz de strings

Membros da matriz: número fixo de 1 item.

Restrições de Tamanho: Tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:subnet/.*$`

Obrigatório: Não

VpcEndpointId

Especifica o ID do endpoint da VPC ao qual seu agente se conecta.

Tipo: sequência

Padrão: `^vpce-[0-9a-f]{17}$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

QopConfiguration

A configuração da Qualidade da Proteção (QOP) especifica as configurações de privacidade da Chamada de Procedimento Remoto (RPC) e da transferência de dados definidas no cluster do Sistema de Arquivos Distribuído do Hadoop (HDFS).

Conteúdo

DataTransferProtection

A configuração de proteção de transferência de dados definida no cluster HDFS. Essa configuração corresponde à configuração `dfs.data.transfer.protection` no arquivo `hdfs-site.xml` do cluster do Hadoop.

Tipo: string

Valores Válidos: DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY

Obrigatório: não

RpcProtection

A configuração de proteção de RPC definida no cluster HDFS. Essa configuração corresponde à configuração `hadoop.rpc.protection` no arquivo `core-site.xml` do cluster do Hadoop.

Tipo: string

Valores Válidos: DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportDestination

Especifica onde DataSync carrega seu relatório de [tarefas](#).

Conteúdo

S3

Especifica o bucket do Amazon S3 DataSync onde carrega seu relatório de tarefas.

Tipo: objeto [ReportDestinationS3](#)

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportDestinationS3

[Especifica o bucket do Amazon S3 DataSync onde carrega seu relatório de tarefas.](#)

Conteúdo

BucketAccessRoleArn

Especifica o Amazon Resource Name (ARN) da política do IAM que DataSync permite fazer o upload de um relatório de tarefas para seu bucket do S3. Para obter mais informações, consulte [Permitir DataSync o upload de um relatório de tarefas em um bucket do Amazon S3](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Exigido: Sim

S3BucketArn

Especifica o ARN do bucket do S3 DataSync onde carrega seu relatório.

Tipo: String

Restrições de comprimento: comprimento máximo de 268.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:[a-z\-\0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3-outposts:[a-z\-\0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-.]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_{1,255}$`

Exigido: Sim

Subdirectory

Especifica um prefixo de bucket para seu relatório.

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportOverride

Especifica o nível de detalhe de um aspecto específico do seu [relatório de DataSync tarefas](#).

Conteúdo

ReportLevel

Especifica se seu relatório de tarefas inclui somente erros ou acertos e erros.

Por exemplo, seu relatório pode incluir principalmente apenas o que não transcorreu bem na sua transferência (ERRORS_ONLY). Ao mesmo tempo, você deseja verificar se seu [filtro de tarefas](#) está funcionando corretamente. Nessa situação, você pode obter uma lista de quais arquivos foram ignorados DataSync com sucesso e se algo foi transferido que você não transferiu (SUCCESSSES_AND_ERRORS).

Tipo: String

Valores Válidos: ERRORS_ONLY | SUCCESSSES_AND_ERRORS

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportOverrides

O nível de detalhe incluído em cada aspecto do seu [relatório de DataSync tarefas](#).

Conteúdo

Deleted

Especifica o nível de relatório dos arquivos, objetos e diretórios que DataSync tentaram excluir no local de destino. Isso só se aplica se você [configurar sua tarefa](#) para excluir dados no destino que não estejam na origem.

Tipo: objeto [ReportOverride](#)

Obrigatório: Não

Skipped

Especifica o nível de relatório para os arquivos, objetos e diretórios que DataSync tentaram ignorar durante a transferência.

Tipo: objeto [ReportOverride](#)

Obrigatório: Não

Transferred

Especifica o nível de relatório dos arquivos, objetos e diretórios que DataSync tentaram ser transferidos.

Tipo: objeto [ReportOverride](#)

Obrigatório: Não

Verified

Especifica o nível de relatório dos arquivos, objetos e diretórios que DataSync tentaram verificar no final da transferência.

Tipo: objeto [ReportOverride](#)

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportResult

Indica se DataSync criou um [relatório de tarefas](#) completo para sua transferência.

Conteúdo

ErrorCode

Indica o código associado ao erro se não for DataSync possível criar um relatório completo.

Tipo: String

Obrigatório: Não

ErrorDetail

Fornece detalhes sobre problemas na criação de um relatório.

Tipo: String

Obrigatório: Não

Status

Indica se ainda DataSync está trabalhando em seu relatório, criou um relatório ou não consegue criar um relatório completo.

Tipo: string

Valores Válidos: PENDING | SUCCESS | ERROR

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

S3Config

Especifica o Amazon Resource Name (ARN) AWS Identity and Access Management da função DataSync (IAM) usada para acessar seu bucket do S3.

Para obter mais informações, consulte [Fornecendo DataSync acesso aos buckets do S3](#).

Conteúdo

BucketAccessRoleArn

Especifica o ARN da função DataSync do IAM usada para acessar seu bucket do S3.

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Exigido: Sim

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

S3ManifestConfig

Especifica o bucket do S3 em que você está hospedando o manifesto que deseja AWS DataSync usar. Para obter mais informações e exemplos de configuração, consulte [Especificação do que é DataSync transferido usando um manifesto](#).

Conteúdo

BucketAccessRoleArn

Especifica a função AWS Identity and Access Management (IAM) que permite DataSync acessar seu manifesto. Para obter mais informações, consulte [Fornecendo DataSync acesso ao seu manifesto](#).

Tipo: String

Restrições de tamanho: tamanho máximo de 2048.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Exigido: Sim

ManifestObjectPath

Especifica a chave de objeto do Amazon S3 do manifesto. Isso pode incluir um prefixo (por exemplo, `prefix/my-manifest.csv`).

Tipo: String

Restrições de tamanho: tamanho máximo de 4.096.

Padrão: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Exigido: Sim

S3BucketArn

Especifica o nome do recurso da Amazon (ARN) do bucket do S3 onde você está hospedando o manifesto.

Tipo: String

Restrições de comprimento: comprimento máximo de 268.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:[a-z\0-9]*:[0-9]{12}:accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3-outposts:[a-z\0-9]+:[0-9]{12}:outpost[/:][a-zA-Z0-9\-.]{1,63}[/:]accesspoint[/:][a-zA-Z0-9\-.]{1,63}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):s3:::[a-zA-Z0-9.\-_{1,255}$`

Exigido: Sim

ManifestObjectVersionId

Especifica o ID da versão do objeto do manifesto que você deseja DataSync usar. Se você não definir isso, DataSync usa a versão mais recente do objeto.

Tipo: String

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 100.

Padrão: `^\.+`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

SmbMountOptions

Especifica a versão do protocolo Server Message Block (SMB) AWS DataSync usada para acessar um servidor de arquivos SMB.

Conteúdo

Version

Por padrão, escolhe DataSync automaticamente uma versão do protocolo SMB com base na negociação com seu servidor de arquivos SMB. Você também pode configurar DataSync para usar uma versão SMB específica, mas recomendamos fazer isso somente se DataSync tiver problemas para negociar com o servidor de arquivos SMB automaticamente.

Essas são as opções para a configuração da versão do SMB:

- **AUTOMATIC**(padrão): DataSync e o servidor de arquivos SMB negocia a versão mais alta do SMB que eles suportam mutuamente entre 2.1 e 3.1.1.

Essa é a opção recomendada. Se, em vez disso, você escolher uma versão específica que seu servidor de arquivos não suporta, você pode receber um erro `Operation Not Supported`.

- **SMB3**: restringe a negociação do protocolo somente à versão 3.0.2 do SMB.
- **SMB2**: restringe a negociação do protocolo somente à versão 2.1 do SMB.
- **SMB2_0**: restringe a negociação do protocolo somente à versão 2.0 do SMB.
- **SMB1**: restringe a negociação do protocolo somente à versão 1.0 do SMB.

Note

A SMB1 opção não está disponível ao [criar um local Amazon FSx for NetApp ONTAP](#).

Tipo: string

Valores Válidos: `AUTOMATIC` | `SMB2` | `SMB3` | `SMB1` | `SMB2_0`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

SourceManifestConfig

Especifica o manifesto que você deseja AWS DataSync usar e onde ele está hospedado. Para obter mais informações e exemplos de configuração, consulte [Especificação do que é DataSync transferido usando um manifesto](#).

Conteúdo

S3

Especifica o bucket do S3 onde você está hospedando o manifesto.

Tipo: objeto [S3ManifestConfig](#)

Obrigatório: sim

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TagListEntry

Um par chave-valor representando uma única tag que foi aplicada a um recurso da AWS .

Conteúdo

Key

A chave para uma tag AWS de recurso.

Tipo: string

Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 256.

Padrão: `^[a-zA-Z0-9\s+=. _:/-]+$`

Exigido: Sim

Value

O valor de uma tag AWS de recurso.

Tipo: string

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskExecutionFilesFailedDetail

O número de objetos que DataSync falham na preparação, transferência, verificação e exclusão durante a execução da tarefa.

Note

Aplica-se somente às [tarefas do modo Avançado](#).

Conteúdo

Delete

O número de objetos que DataSync não são excluídos durante a execução da tarefa.

Tipo: longo

Obrigatório: não

Prepare

O número de objetos que DataSync falham na preparação durante a execução da tarefa.

Tipo: longo

Obrigatório: não

Transfer

O número de objetos que DataSync não são transferidos durante a execução da tarefa.

Tipo: longo

Obrigatório: não

Verify

O número de objetos que DataSync não são verificados durante a execução da tarefa.

Tipo: longo

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskExecutionFilesListedDetail

O número de objetos DataSync encontrados em seus locais.

Note

Aplica-se somente às [tarefas do modo Avançado](#).

Conteúdo

AtDestinationForDelete

O número de objetos DataSync encontrados no local de destino. Esse contador só é aplicável se você [configurar sua tarefa](#) para excluir dados no destino que não estejam na origem.

Tipo: longo

Obrigatório: Não

AtSource

O número de objetos DataSync encontrados no local de origem.

- Com um [manifesto](#), DataSync lista somente o que está em seu manifesto (e não tudo em seu local de origem).
- Com um [filtro](#) de inclusão, DataSync lista somente o que corresponde ao filtro no local de origem.
- Com um filtro de exclusão, DataSync lista tudo no local de origem antes de aplicar o filtro.

Tipo: longo

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)

- [AWS SDK para Ruby V3](#)

TaskExecutionListEntry

Representa uma única entrada em uma lista de execuções de AWS DataSync tarefas que é retornada com a [ListTaskExecutions](#) operação.

Conteúdo

Status

O status de execução de uma tarefa. Para obter mais informações, consulte [Status da execução de tarefas](#).

Tipo: String

Valores Válidos: QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR

Obrigatório: Não

TaskExecutionArn

O nome do recurso da Amazon (ARN) da execução da tarefa.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\\-0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}/execution/exec-[0-9a-f]{17}$`

Obrigatório: Não

TaskMode

O modo de tarefa que você está usando. Para obter mais informações, consulte [Escolha de um modo de tarefa para sua transferência de dados](#).

Tipo: String

Valores Válidos: BASIC | ENHANCED

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskExecutionResultDetail

Fornece informações detalhadas sobre o resultado da execução da AWS DataSync tarefa.

Conteúdo

ErrorCode

Um erro DataSync encontrado durante a execução da tarefa. Você pode usar essas informações para ajudar a [solucionar problemas](#).

Tipo: String

Obrigatório: Não

ErrorDetail

A descrição detalhada de um erro DataSync encontrado durante a execução da tarefa. Você pode usar essas informações para ajudar a [solucionar problemas](#).

Tipo: String

Obrigatório: Não

PrepareDuration

O tempo em milissegundos em que a execução da tarefa esteve na PREPARING etapa. Para obter mais informações, consulte [Status da execução de tarefas](#).

Para tarefas do modo Avançado, o valor é sempre 0. Para obter mais informações, consulte [Como DataSync prepara sua transferência de dados](#).

Tipo: longo

Intervalo válido: valor mínimo de 0.

Obrigatório: Não

PrepareStatus

O status da PREPARING etapa para a execução da tarefa. Para obter mais informações, consulte [Status da execução de tarefas](#).

Tipo: String

Valores Válidos: PENDING | SUCCESS | ERROR

Obrigatório: Não

TotalDuration

O tempo em milissegundos que a execução da tarefa levou.

Tipo: longo

Intervalo válido: valor mínimo de 0.

Obrigatório: Não

TransferDuration

O tempo em milissegundos em que a execução da tarefa esteve na TRANSFERRING etapa. Para obter mais informações, consulte [Status da execução de tarefas](#).

Para tarefas do modo Avançado, o valor é sempre 0. Para obter mais informações, consulte [Como DataSync transfere seus dados](#).

Tipo: longo

Intervalo válido: valor mínimo de 0.

Obrigatório: Não

TransferStatus

O status da TRANSFERRING etapa para a execução da tarefa. Para obter mais informações, consulte [Status da execução de tarefas](#).

Tipo: String

Valores Válidos: PENDING | SUCCESS | ERROR

Obrigatório: Não

VerifyDuration

O tempo em milissegundos em que a execução da tarefa esteve na VERIFYING etapa. Para obter mais informações, consulte [Status da execução de tarefas](#).

Para tarefas do modo Avançado, o valor é sempre 0. Para obter mais informações, consulte [Como DataSync verifica a integridade dos seus dados](#).

Tipo: longo

Intervalo válido: valor mínimo de 0.

Obrigatório: Não

VerifyStatus

O status da VERIFYING etapa para a execução da tarefa. Para obter mais informações, consulte [Status da execução de tarefas](#).

Tipo: String

Valores Válidos: PENDING | SUCCESS | ERROR

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskFilter

Você pode usar filtros de API para refinar a lista de recursos retornados por `ListTasks`. Por exemplo, para recuperar todas as tarefas em um local de origem, você pode usar `ListTasks` com o nome do filtro `LocationId` e `Operator` `Equals` com o ARN para o local.

Para obter mais informações, consulte [DataSync recursos de filtragem](#).

Conteúdo

Name

O nome do filtro que está sendo usado. Cada chamada de API é compatível com uma lista de filtros que estão disponíveis para ela. Por exemplo, `LocationId` para `ListTasks`.

Tipo: string

Valores Válidos: `LocationId` | `CreationTime`

Obrigatório: sim

Operator

O operador usado para comparar valores de filtro (por exemplo, `Equals` ou `Contains`).

Tipo: string

Valores Válidos: `Equals` | `NotEquals` | `In` | `LessThanOrEqualTo` | `LessThan` | `GreaterThanEqualTo` | `GreaterThan` | `Contains` | `NotContains` | `BeginsWith`

Obrigatório: sim

Values

Os valores que você deseja filtrar. Por exemplo, talvez você queira exibir somente tarefas de um local de destino específico.

Tipo: matriz de strings

Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 255.

Padrão: `^[0-9a-zA-Z_\ \-:\*\.\ \\/\?\-]*$`

Exigido: Sim

Consulte também

Para obter mais informações sobre como usar essa API em uma linguagem específica AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskListEntry

Representa uma única entrada em uma lista de tarefas. `TaskListEntry` retorna uma matriz que contém uma lista de tarefas quando a [ListTasks](#) operação é chamada. Uma tarefa inclui os sistemas de arquivos de origem e destino a serem sincronizados e as opções a serem usadas nas tarefas.

Conteúdo

Name

O nome da tarefa .

Tipo: String

Restrições de tamanho: o tamanho mínimo é 0. O tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Obrigatório: Não

Status

O status da tarefa.

Tipo: String

Valores Válidos: AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE

Obrigatório: Não

TaskArn

O nome de recurso da Amazon (ARN) da tarefa.

Tipo: String

Restrições de tamanho: tamanho máximo de 128.

Padrão: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\-\0-9]*:[0-9]{12}:task/task-[0-9a-f]{17}$`

Obrigatório: Não

TaskMode

O modo de tarefa que você está usando. Para obter mais informações, consulte [Escolha de um modo de tarefa para sua transferência de dados](#).

Tipo: String

Valores Válidos: BASIC | ENHANCED

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskReportConfig

Especifica como você deseja configurar um relatório de tarefas, que fornece informações detalhadas sobre sua AWS DataSync transferência.

Para obter mais informações, consulte [Relatórios de tarefas](#).

Conteúdo

Destination

Especifica o bucket do Amazon S3 DataSync onde carrega seu relatório de tarefas. Para obter mais informações, consulte [Relatórios de tarefas](#).

Tipo: objeto [ReportDestination](#)

Obrigatório: Não

ObjectVersionIds

Especifica se o relatório de tarefas inclui a nova versão de cada objeto transferido para um bucket do S3. Isso só se aplica se você [ativar o controle de versão em seu bucket](#). Lembre-se de que definir isso como INCLUDE pode aumentar a duração da execução da tarefa.

Tipo: String

Valores Válidos: INCLUDE | NONE

Obrigatório: Não

OutputType

Especifica o tipo de relatório de tarefas que você deseja:

- SUMMARY_ONLY: fornece os detalhes necessários sobre sua tarefa, incluindo o número de arquivos, objetos e diretórios transferidos e a duração da transferência.
- STANDARD: fornece detalhes completos sobre sua tarefa, incluindo uma lista completa de arquivos, objetos e diretórios que foram transferidos, ignorados, verificados e muito mais.

Tipo: String

Valores Válidos: SUMMARY_ONLY | STANDARD

Obrigatório: Não

Overrides

Personaliza o nível de relatório para aspectos do seu relatório de tarefas. Por exemplo, seu relatório geralmente pode incluir apenas erros, mas você pode especificar que deseja uma lista de sucessos e erros apenas para os arquivos que DataSync tentaram excluir em seu local de destino.

Tipo: objeto [ReportOverrides](#)

Obrigatório: Não

ReportLevel

Especifica se você deseja que seu relatório de tarefas inclua somente o que deu errado com sua transferência ou uma lista do que foi bem-sucedido ou não.

- **ERRORS_ONLY**: um relatório mostra o que não DataSync foi possível transferir, ignorar, verificar e excluir.
- **SUCCESSES_AND_ERRORS**: um relatório mostra o que DataSync foi possível e o que não foi possível transferir, ignorar, verificar e excluir.

Tipo: String

Valores Válidos: **ERRORS_ONLY** | **SUCCESSES_AND_ERRORS**

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskSchedule

Configura sua AWS DataSync tarefa para ser executada em um [cronograma](#) (em um intervalo mínimo de 1 hora).

Conteúdo

ScheduleExpression

Especifica o agendamento da tarefa usando uma expressão cron ou rate.

Use expressões cron para agendamentos de tarefas executadas em hora e dia específicos. Por exemplo, a expressão cron a seguir cria um agendamento de tarefa que é executada às 8 horas na primeira quarta-feira de cada mês:

```
cron(0 8 * * 3#1)
```

Use expressões rate para agendamentos de tarefas que devem ser executadas a intervalos regulares. Por exemplo, a expressão rate a seguir cria um agendamento de tarefa que é executada a cada 12 horas:

```
rate(12 hours)
```

Para obter informações sobre a sintaxe da expressão cron e de taxa, consulte o Guia [EventBridge do usuário da Amazon](#).

Tipo: string

Restrições de tamanho: o tamanho máximo é 256.

Padrão: `^[a-zA-Z0-9\ \_\*\?\,\|\^\-\\/\#\s\(\)\+]*$`

Exigido: Sim

Status

Especifica se você deseja habilitar ou desabilitar o agendamento da tarefa. O agendamento é habilitado por padrão, mas pode haver situações em que você precise desabilitá-lo. Por exemplo, pode ser necessário pausar uma transferência recorrente para corrigir um problema com a tarefa ou realizar a manutenção do sistema de armazenamento.

DataSync pode desativar sua agenda automaticamente se sua tarefa falhar repetidamente com o mesmo erro. Para obter mais informações, consulte [TaskScheduleDetails](#).

Tipo: String

Valores Válidos: ENABLED | DISABLED

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskScheduleDetails

Fornecer informações sobre o [agendamento de tarefas](#) do AWS DataSync .

Conteúdo

DisabledBy

Indica como o agendamento de tarefas foi desabilitado.

- **USER**- Sua agenda foi desativada manualmente usando a [UpdateTask](#) operação ou o DataSync console.
- **SERVICE**- Sua agenda foi desativada automaticamente DataSync porque a tarefa falhou repetidamente com o mesmo erro.

Tipo: String

Valores Válidos: **USER** | **SERVICE**

Obrigatório: Não

DisabledReason

Fornecer um motivo se o agendamento de tarefa for desabilitado.

Se o agendamento for desabilitado pelo **USER**, você verá uma mensagem `Manually disabled by user..`

Se o agendamento for desabilitado pelo **SERVICE**, você verá uma mensagem de erro para ajudar a entender por que a tarefa continua apresentando falhas. Para obter informações sobre como resolver DataSync erros, consulte [Solução de problemas com DataSync transferências](#).

Tipo: String

Restrições de comprimento: comprimento máximo de 8192.

Padrão: `^[\\w\\s.,'?!:;\\/=|<>()-]*$`

Obrigatório: Não

StatusUpdateTime

Indica a última vez que o status do agendamento de tarefas foi alterado. Por exemplo, se sua agenda for desativada DataSync automaticamente devido a um erro repetido, você poderá ver quando a agenda foi desativada.

Tipo: Timestamp

Obrigatório: Não

Consulte também

Para obter mais informações sobre como usar essa API em uma das linguagens específicas AWS SDKs, consulte o seguinte:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Erros comuns

Esta seção lista os erros comuns às ações de API de todos os AWS serviços. Para saber os erros específicos de uma ação de API para esse serviço, consulte o tópico sobre a ação de API em questão.

AccessDeniedException

Você não tem acesso suficiente para executar essa ação.

Código de status HTTP: 400

IncompleteSignature

A assinatura da solicitação não está em conformidade com os AWS padrões.

Código de status HTTP: 400

InternalFailure

O processamento da solicitação falhou por causa de um erro, uma exceção ou uma falha desconhecida.

Código de status HTTP: 500

InvalidAction

A ação ou operação solicitada é inválida. Verifique se a ação foi digitada corretamente.

Código de status HTTP: 400

InvalidClientTokenId

O certificado X.509 ou ID da chave de AWS acesso fornecido não existe em nossos registros.

Código de status HTTP: 403

NotAuthorized

Você não tem permissão para realizar esta ação.

Código de status HTTP: 400

OptInRequired

O ID da chave de AWS acesso precisa de uma assinatura para o serviço.

Código de status HTTP: 403

RequestExpired

A solicitação chegou ao serviço mais de 15 minutos após o carimbo de data na solicitação ou mais de 15 minutos após a data de expiração da solicitação (como para pré-assinada URLs), ou o carimbo de data na solicitação é mais de 15 minutos no futuro.

Código de status HTTP: 400

ServiceUnavailable

Falha na solicitação devido a um erro temporário do servidor.

Código de status HTTP: 503

ThrottlingException

A solicitação foi negada devido à limitação da solicitação.

Código de status HTTP: 400

ValidationError

A entrada não satisfaz as restrições especificadas por um AWS serviço.

Código de status HTTP: 400

Parâmetros gerais

A lista a seguir contém os parâmetros que todas as ações usam para assinar solicitações do Signature versão 4 com uma string de consulta. Todos os parâmetros específicos de uma ação são listados no tópico para a ação. Para obter mais informações sobre o Signature versão 4, consulte [Solicitações de AWS API de assinatura](#) no Guia do usuário do IAM.

Action

A ação a ser executada.

Tipo: string

Obrigatório: Sim

Version

A versão da API para a qual a solicitação foi escrita, expressa no formato YYYY-MM-DD.

Tipo: string

Obrigatório: Sim

X-Amz-Algorithm

O algoritmo de hash que foi usado para criar a assinatura da solicitação.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Valores Válidos: AWS4-HMAC-SHA256

Obrigatório: condicional

X-Amz-Credential

O valor de escopo da credencial, uma string que inclui a sua chave de acesso, a data, a região visada, o serviço que está sendo solicitado e uma sequência de encerramento ("aws4_request"). O valor é expresso no seguinte formato: chave_acesso/AAAAMMDD/região/serviço/aws4_request.

Para obter mais informações, consulte [Criar uma solicitação de AWS API assinada](#) no Guia do usuário do IAM.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Obrigatório: Condicional

X-Amz-Date

A data usada para criar a assinatura. O formato deve ser o formato básico ISO 8601 (AAAAMMDD'T'HHMMSS'Z'). Por exemplo, a data e hora a seguir é um X-Amz-Date valor válido:20120325T120000Z.

Condição: X-Amz-Date é opcional para todas as solicitações; ele pode ser usado para substituir a data usada em solicitações de assinatura. Se o cabeçalho da data for especificado no formato básico ISO 8601, não X-Amz-Date é necessário. Quando X-Amz-Date usado, ele sempre substitui o valor do cabeçalho da data. Para obter mais informações, consulte [Elementos de uma assinatura de solicitação de AWS API](#) no Guia do usuário do IAM.

Tipo: string

Obrigatório: Condicional

X-Amz-Security-Token

O token de segurança temporário obtido por meio de uma chamada para AWS Security Token Service (AWS STS). Para obter uma lista de serviços que oferecem suporte a credenciais de segurança temporárias do AWS STS, consulte [Serviços da AWS que funcionam com o IAM](#) no Guia do usuário do IAM.

Condição: se você estiver usando credenciais de segurança temporárias do AWS STS, deverá incluir o token de segurança.

Tipo: string

Obrigatório: Condicional

X-Amz-Signature

Especifica a assinatura com codificação hexadecimal que foi calculada com base na string a ser assinada e na chave de assinatura derivada.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Obrigatório: Condicional

X-Amz-SignedHeaders

Especifica todos os cabeçalhos HTTP que foram incluídos como parte da solicitação canônica. Para obter mais informações sobre a especificação de cabeçalhos assinados, consulte [Criar uma solicitação de AWS API assinada](#) no Guia do usuário do IAM.

Condição: especifique esse parâmetro quando incluir as informações de autenticação em uma string de consulta em vez de no cabeçalho da autorização HTTP.

Tipo: string

Obrigatório: Condicional

Histórico do documento

A tabela a seguir descreve adições importantes à AWS DataSync documentação. Também atualizamos a documentação com frequência para abordar os comentários enviados por você.

Para receber notificações sobre atualizações dessa documentação, inscreva-se no feed RSS.

Alteração	Descrição	Data
O Discovery não está mais disponível	A partir de 20 de maio de 2025, o Discovery não é mais um DataSync recurso disponível.	20 de maio de 2025
AWS atualização de política gerenciada - Atualização da política existente	A AWSDDataSyncFullAccess política atualizou as declarações de permissão que removem as condições de marcação das permissões DataSync usadas para criar segredos do Secrets Manager.	13 de maio de 2025
AWS atualização de política gerenciada - Atualização da política existente	A AWSDDataSyncFullAccess política tem novas permissões que DataSync permitem trabalhar com AWS Secrets Manager.	7 de maio de 2025
AWS atualização de política gerenciada - Atualização da política existente	A AWSDDataSyncFullAccess política tem novas permissões que DataSync permitem trabalhar com AWS Secrets Manager.	23 de abril de 2025
AWS atualização de política gerenciada - Atualização da política existente	A AWSDDataSyncFullAccess política tem novas permissões que DataSync permitem trabalhar com AWS	23 de abril de 2025

	Secrets Manager AWS Key Management Service e.	
AWS atualização de política gerenciada - Atualização da política existente	AWSDataSyncService RolePolicy Tem novas permissões que permitem DataSync trabalhar com AWS Secrets Manager.	15 de abril de 2025
Executando grandes migrações de dados	Saiba como planejar migrações de dados em grande escala usando DataSync para transferir arquivos ou objetos do local ou de outro armazenamento em nuvem para o. AWS	19 de fevereiro de 2025
Support para Kerberos com localizações de pequenas e médias empresas	DataSync agora pode usar a autenticação Kerberos ao se conectar aos servidores de arquivos do Server Message Block (SMB).	28 de janeiro de 2025
Novo Região da AWS	AWS DataSync está disponível para transferências de dados na região do México (Central).	14 de janeiro de 2025
Novo Região da AWS	AWS DataSync está disponível para transferências de dados na região Ásia-Pacífico (Tailândia).	7 de janeiro de 2025
Atualizar locais AWS de armazenamento	Agora você pode atualizar seus locais de FSx transferência do Amazon S3, Amazon EFS e Amazon.	18 de dezembro de 2024

Não é mais compatível com o Snowball Edge	A partir de 12 de novembro de 2024, DataSync não oferece mais suporte AWS Snowball Edge.	13 de novembro de 2024
Nova política AWS gerenciada	A função DataSync vinculada ao serviço chamada <code>AWSServiceRoleForDataSync</code> usa uma nova política gerenciada chamada <code>AWSDataSyncServiceRolePolicy</code> .	30 de outubro de 2024
Apresentando o modo Avançado	Com o modo Avançado, você pode transferir números virtualmente ilimitados de objetos entre locais do Amazon S3.	30 de outubro de 2024
AWS atualizações de políticas gerenciadas - Atualização de uma política existente	A <code>AWSDataSyncFullAccess</code> política tem uma nova permissão para serviços que funcionam com DataSync.	30 de outubro de 2024
Suporte para contas v1 de uso geral do armazenamento Azure	DataSync pode trabalhar com contas v1 de uso geral de Azure armazenamento ao transferir de ou para. Microsoft Azure Blob Storage	4 de outubro de 2024
Nova maneira de configurar agendamentos de tarefas	Você pode configurar seus agendamentos de DataSync tarefas usando expressões de taxa.	22 de agosto de 2024

Novo Região da AWS	AWS DataSync está disponível para transferências de dados na região Ásia-Pacífico (Malásia).	21 de agosto de 2024
Compatibilidade com transferências entre regiões sem agente que incluem uma região de adesão opcional	Você não precisa mais de um DataSync agente para transferências entre serviços AWS de armazenamento quando pelo menos um local de armazenamento está em um opt-in Região da AWS.	24 de julho de 2024
AWS atualizações de políticas gerenciadas - Atualização de uma política existente	A <code>AWSDataSyncFullAccess</code> política tem uma nova permissão para serviços que funcionam com DataSync.	22 de julho de 2024
Atualizado o tutorial de várias contas do S3	Foram removidas algumas permissões do usuário na conta de origem que não são mais necessárias para essa transferência.	10 de junho de 2024
Status de execução de nova tarefa	O status <code>CANCELLING</code> indica quando a execução de uma tarefa está sendo cancelada.	15 de maio de 2024
Nova opção para pausar agendamentos de tarefas	Você pode desativar o agendamento de AWS DataSync tarefas quando precisar solucionar problemas ou realizar a manutenção do sistema de armazenamento.	24 de abril de 2024

Atualizada a Cifra TLS para endpoints FIPS	AWS DataSync usa a cifra TLS_AES_128_GCM_SHA256 (secp256r1) para endpoints de serviço do Federal Information Processing Standard (FIPS).	22 de abril de 2024
AWS atualizações de políticas gerenciadas - Atualização de uma política existente	A AWSDataSyncFullAccess política tem uma nova permissão para serviços que funcionam com DataSync.	16 de fevereiro de 2024
Transferir arquivos ou objetos específicos com um manifesto	AWS DataSync pode transferir uma lista de arquivos ou objetos usando um manifesto.	7 de fevereiro de 2024
Novo Região da AWS	AWS DataSync agora está disponível para transferências de dados na região Oeste do Canadá (Calgary).	20 de dezembro de 2023
Suporte para transferências com provedores de nuvem adicionais	AWS DataSync agora pode transferir dados entre serviços AWS de armazenamento e IBM Cloud Object Storage ou Seagate Lyve Cloud.	7 de novembro de 2023
Suporte para transferências com Alibaba Cloud Object Storage Service	AWS DataSync agora pode transferir dados entre serviços AWS de armazenamento Alibaba Cloud Object Storage Service e.	25 de setembro de 2023
Suporte para relatórios de tarefas	Monitore suas AWS DataSync transferências com relatórios de tarefas.	30 de agosto de 2023

Novo Região da AWS	AWS DataSync agora está disponível para transferências de dados na região de Israel (Tel Aviv).	23 de agosto de 2023
Suporte para transferências com provedores de nuvem adicionais	AWS DataSync agora podem transferir dados entre serviços AWS de armazenamento e vários outros provedores de nuvem (como Wasabi Cloud Storage, DigitalOcean Spaces, e Oracle Cloud Infrastructure Object Storage).	8 de agosto de 2023
Disponibilidade geral de suporte Microsoft Azure Blob Storage	AWS DataSync agora pode transferir objetos de e para Microsoft Azure Blob Storage.	25 de julho de 2023
Suporte à versão 1.3 do TLS	Ao transferir entre locais de armazenamento, AWS DataSync agora criptografa todo o tráfego de rede com o Transport Layer Security (TLS) 1.3.	28 de junho de 2023
Novas métricas do DataSync Discovery	AWS DataSync Discovery agora pode dizer quantos LUNs (números de unidades lógicas) estão em um cluster de recursos de armazenamento, máquina virtual de armazenamento (SVM) ou volume.	28 de junho de 2023

Novo Região da AWS	AWS DataSync agora está disponível para transferências de dados na região Ásia-Pacífico (Melbourne).	24 de maio de 2023
Suporte para armazenamento compatível com S3 no Snowball Edge	Você pode usar AWS DataSync para transferir dados entre o armazenamento compatível com o Amazon S3 AWS Snowball Edge e os serviços de AWS armazenamento.	18 de maio de 2023
AWS atualizações de políticas gerenciadas - Atualização de uma política existente	A <code>AWSDDataSyncFullAccess</code> política tem novas permissões para serviços que funcionam com DataSync.	2 de maio de 2023
Disponibilidade geral de AWS DataSync Discovery	Use o DataSync Discovery para ajudar a acelerar sua migração para AWS.	25 de abril de 2023
Versão de pré-visualização pública do suporte ao armazenamento de Blobs do Microsoft Azure Blob	AWS DataSync agora pode transferir objetos de Microsoft Azure Blob Storage.	29 de março de 2023
Nova política do IAM	Para oferecer suporte ao recurso DataSync Discovery, DataSync usa a função vinculada ao serviço chamada <code>AWSServiceRoleForDataSyncDiscovery</code> .	21 de março de 2023

Novo Regiões da AWS	AWS DataSync agora está disponível nas seguintes regiões Regiões da AWS: Ásia-Pacífico (Hyderabad), Europa (Espanha) e Europa (Zurique).	6 de fevereiro de 2023
Utilizar tags em execuções de tarefas	Agora você pode marcar suas execuções de AWS DataSync tarefas.	16 de dezembro de 2022
Suporte ao S3 Glacier Instant Retrieval	Agora é possível transferir objetos diretamente na classe de armazenamento do S3 Glacier Instant Retrieval.	16 de dezembro de 2022
Copiar metadados do sistema de objetos	AWS DataSync agora é possível copiar metadados do sistema durante a transferência entre um sistema de armazenamento de objetos e o Amazon S3.	16 de dezembro de 2022
Novo Regiões da AWS	AWS DataSync agora está disponível nas regiões da China (Pequim) e China (Ningxia).	14 de dezembro de 2022
Novo Região da AWS	AWS DataSync agora está disponível na região do Oriente Médio (EAU).	16 de novembro de 2022
Suporte para certificados autoassinados com locais de armazenamento de objetos	AWS DataSync pode se conectar a locais de armazenamento de objetos que usam certificados autoassinados ou privados.	25 de outubro de 2022

Obtenha informações sobre compressão de dados	AWS DataSync pode fornecer o número físico de bytes transferidos pela rede após a aplicação da compressão.	25 de outubro de 2022
Versão prévia pública do AWS DataSync Discovery	Use o DataSync Discovery para ajudar a acelerar sua migração para AWS o.	21 de setembro de 2022
Nova opção para migrar dados de ou para o Google Cloud Storage	Você pode transferir dados de ou para o Google Cloud Storage implantando um agente de AWS DataSync no Google Cloud.	21 de julho de 2022
Support for Amazon FSx for NetApp ONTAP file systems	AWS DataSync agora pode transferir arquivos e pastas de e para os sistemas de FSx arquivos ONTAP.	28 de junho de 2022
Novas opções de segurança para locais do Amazon EFS	AWS DataSync pode acessar os sistemas de arquivos do Amazon EFS usando TLS, pontos de acesso e funções do IAM.	31 de maio de 2022
Migração de dados para ou do Google Cloud Storage e Azure Files	Com AWS DataSync, você pode transferir dados de ou para o Google Cloud Storage e Azure Files. Para obter mais informações, consulte Criação de um local para armazenam ento de objetos e Criação de um local para SMB .	24 de maio de 2022

Nova configuração de AWS DataSync tarefa	Com a opção Copiar tags de objeto, você pode especificar se deseja manter as tags de objeto ao transferir entre sistemas de armazenamento de objetos.	05 de maio de 2022
Novo Região da AWS	AWS DataSync agora está disponível na região Ásia-Pacífico (Jacarta).	19 de abril de 2022
Support for Amazon FSx for OpenZFS file systems	AWS DataSync agora pode transferir arquivos e pastas de e FSx para sistemas de arquivos OpenZFS.	5 de abril de 2022
Support para sistemas de arquivos Amazon FSx for Lustre	AWS DataSync agora pode transferir arquivos e pastas de e para os sistemas de FSx arquivos Lustre.	10 de dezembro de 2021
Suporte para o Sistema de Arquivos Distribuído do Hadoop (HDFS)	AWS DataSync agora suporta a transferência de arquivos e pastas de e para clusters HDFS.	3 de novembro de 2021
Novo Região da AWS	AWS DataSync agora está disponível na região Ásia-Pacífico (Osaka).	28 de julho de 2021
Transferências totalmente automatizadas entre serviços AWS de armazenamento	AWS DataSync agora é possível transferir arquivos ou objetos entre o Amazon S3, o Amazon EFS ou FSx o Windows File Server com apenas alguns cliques no console. DataSync	9 de novembro de 2020

[Ajustando a largura de banda da rede usada por uma tarefa em execução](#)

AWS DataSync agora permite que os clientes ajustem a largura de banda da rede usada por uma DataSync tarefa em execução. Isso ajuda a minimizar o impacto em outros usuários ou aplicativos quando uma tarefa se estende por vários dias.

9 de novembro de 2020

[Suporte aprimorado para funções de máquina DataSync virtual \(VM\) local](#)

O console host da VM do AWS DataSync agente agora oferece suporte a funções aprimoradas, incluindo a ativação de um agente a partir do console local.

19 de outubro de 2020

[AWS DataSync agora pode transferir dados de e para AWS Outposts](#)

DataSync agora suporta a transferência de objetos de e para o Amazon AWS Outposts S3 em diante.

30 de setembro de 2020

[Suporte para filtragem de API](#)

AWS DataSync agora suporta filtragem para chamadas de `ListLocations` API `ListTasks` e API, permitindo que você recupere facilmente a configuração das tarefas de transferência de dados usando filtros como a origem ou o destino da transferência de dados.

18 de agosto de 2020

[Suporte para copiar dados do armazenamento de objetos autogerenciados](#)

AWS DataSync agora oferece suporte à transferência de dados entre o armazenamento autogerenciado de objetos e o Amazon S3, o Amazon Elastic File System FSx ou o Windows File Server.

27 de julho de 2020

[Suporte para máquina virtual baseada em kernel \(KVM\) e hipervisores Microsoft Hyper-V](#)

AWS DataSync agora fornece a capacidade de implantar agentes locais nas plataformas de virtualização KVM e Microsoft Hyper-V, além das opções existentes e da Amazon. VMware EC2

1.º de julho de 2020

[AWS DataSync agora você pode configurar automaticamente sua configuração do Amazon CloudWatch Logs](#)

Ao usar DataSync, agora você tem a opção de gerar automaticamente o grupo de CloudWatch registros e a política de recursos necessários para publicar registros para sua transferência de dados, simplificando a criação de tarefas e a configuração do monitoramento.

1.º de julho de 2020

[AWS DataSync agora pode transferir dados de e para AWS Snowball Edge](#)

DataSync agora suporta a transferência de arquivos de e para AWS Snowball Edge, o menor membro dos dispositivos de computação AWS Snow Family de ponta e transferência de dados. O Snowball Edge é portátil, robusto e seguro — pequeno e leve o suficiente para caber em uma mochila e capaz de suportar ambientes agressivos.

17 de junho de 2020

[Novo Região da AWS](#)

AWS DataSync agora está disponível na região da África (Cidade do Cabo) e na região da Europa (Milão).

16 de junho de 2020

[Recursos de monitoramento aprimorados com registro em log no nível do arquivo](#)

Agora você pode ativar o registro detalhado de arquivos e objetos copiados entre seus servidores NFS, servidores SMB, buckets Amazon S3, sistemas de arquivos Amazon EFS e sistemas FSx de arquivos Windows File Server.

24 de abril de 2020

[Support para copiar dados entre seu compartilhamento SMB e o Amazon FSx for Windows File Server](#)

Agora você pode copiar dados entre seu compartilhamento SMB e FSx para o Windows File Server.

24 de janeiro de 2020

Suporte às tarefas de agendamento	Agora você pode executar tarefas manualmente ou programá-las para serem executadas com base em uma programação especificada.	20 de novembro de 2019
Novo Região da AWS	AWS DataSync agora está disponível na região Ásia-Pacífico (Hong Kong), na região Ásia-Pacífico (Mumbai), na região da Europa (Estocolmo), na região da América do Sul (São Paulo) e na região AWS GovCloud (Leste dos EUA).	20 de novembro de 2019
Novo Região da AWS	AWS DataSync agora está disponível na região do Canadá (Central), na região da Europa (Londres) e na região da Europa (Paris).	2 de outubro de 2019
Suporte para classes de armazenamento do Amazon S3	Agora você pode transferir objetos diretamente para classes de armazenamento do Amazon S3.	24 de setembro de 2019
Novo Região da AWS	AWS DataSync agora está disponível na região do Oriente Médio (Bahrein).	28 de agosto de 2019
Suporte para copiar dados entre o compartilhamento de Server Message Block (SMB) e o Amazon S3 ou o Amazon EFS	Agora você pode copiar dados entre o compartilhamento de arquivos SMB e o Amazon S3 ou o Amazon EFS.	22 de agosto de 2019

Suporte para uso de VPC endpoints	Agora você pode criar uma conexão privada entre seu agente AWS e executar tarefas em uma rede privada. Isso aumenta a segurança dos dados enquanto são copiados pela rede.	5 de agosto de 2019
Suporte para endpoints do Federal Information Processing Standard (FIPS - Padrão federal de processamento de informações)	Agora você pode usar endpoints do FIPS para criar agentes e executar tarefas.	5 de agosto de 2019
Novo Região da AWS	AWS DataSync agora está disponível na região AWS GovCloud (Oeste dos EUA).	11 de junho de 2019
Suporte para filtragem	Agora é possível aplicar filtros para transferir apenas um subconjunto dos arquivos no local de origem ao transferir dados da origem para o local de destino.	22 de maio de 2019
Primeiro lançamento do AWS DataSync	Lançamento geral do AWS DataSync serviço.	26 de novembro de 2018

AWS Glossário

Para obter a AWS terminologia mais recente, consulte o [AWS glossário](#) na Glossário da AWS Referência.

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.