



Guía del usuario

AWS DataSync



AWS DataSync: Guía del usuario

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS DataSync?	1
Casos de uso	2
Ventajas	3
Recursos adicionales	3
Funcionamiento	4
DataSync arquitectura de transferencia	4
Transferencia entre el almacenamiento en las instalaciones y AWS	4
Transferencia entre servicios AWS de almacenamiento	5
Transferencia entre servicios AWS de almacenamiento y sistemas de almacenamiento en otras nubes	6
Conceptos y terminología	7
Agente	8
Ubicación	8
Tarea	8
Ejecución de tarea	8
Cómo DataSync transfiere los archivos, objetos y directorios	8
¿Cómo DataSync se prepara la transferencia de datos	9
¿Cómo se DataSync transfieren tus datos	10
¿Cómo DataSync verifica la integridad de los datos	10
¿Cómo DataSync funciona con los archivos abiertos y bloqueados	11
Opciones de transferencia recurrentes	12
Introducción	13
Inscríbase en una Cuenta de AWS	13
Creación de un usuario con acceso administrativo	13
Permisos de IAM necesarios para usar DataSync	15
AWS políticas gestionadas	15
Políticas administradas por el cliente	15
¿Dónde puedo utilizarlas? DataSync	16
¿Cómo puedo usarlo? DataSync	16
¿Cuánto va a DataSync costar?	16
Componentes de código abierto utilizados por DataSync	16
¿Necesito un agente de ?	16
Situaciones en las que necesita un DataSync agente	17
Situaciones en las que no necesita un DataSync agente	17

Uso de varios DataSync agentes	17
Pasos a seguir a continuación	18
Requisitos del agente	18
Requisitos del hipervisor	18
Requisitos de agente para las DataSync transferencias	19
Requisitos de agente para las particiones Región de AWS	20
Requisitos de administración de agentes	20
Implementación de su agente	21
Despliegue de su agente en VMware	21
Implementación del agente en KVM	22
Implementación del agente en Microsoft Hyper-V	23
Despliegue de su EC2 agente de Amazon	24
Implementación de su agente en AWS Snowball Edge	29
Despliegue de su agente en AWS Outposts	30
Elección de un punto de conexión de servicio para su agente	30
Elegir un punto de conexión de servicio público	31
Elegir un punto de conexión de servicio de FIPS	31
Selección de un punto de conexión de servicio de VPC	31
Activación de su agente de	34
Requisitos previos	34
Obtención de una clave de activación	35
Activación de su agente de	37
Pasos a seguir a continuación	40
Verificación de las conexiones de red de su agente	40
Acceso a la consola local de su agente	40
Verificación de la conexión de su agente con su sistema de almacenamiento	41
Verificar la conexión de su agente al servicio DataSync	42
Pasos a seguir a continuación	43
Conexión de la red	44
1. Conexión de red entre el sistema de almacenamiento y el agente	44
2. Conexión de red entre el agente y DataSync el servicio	44
Conectar la red de almacenamiento a AWS	45
Selección de un punto de conexión de servicio	45
3. Conexión de red entre el DataSync servicio y el servicio AWS de almacenamiento	45
Establezca redes cuando no necesite un DataSync agente	46
Cómo y dónde fluye DataSync el tráfico a través de la red	46

Seguridad de red para DataSync	46
Requisitos de red	46
Requisitos de red para el almacenamiento autoadministrado en las instalaciones y otros tipos de almacenamiento periférico en la nube	46
Requisitos de red para los servicios de almacenamiento de AWS	52
Requisitos de red para puntos de conexión de servicio públicos o FIPS	53
Requisitos de red para puntos de conexión de servicio de VPC	60
Interfaces de red para transferencia de datos	63
Interfaces de red para transferencias con agentes	63
Interfaces de red para transferencias sin agentes	64
Visualización de las interfaces de red	65
Ejemplos de arquitectura y enrutamiento con Direct Connect	66
Uso de Direct Connect con un punto final de servicio de DataSync VPC	66
Uso de Direct Connect con un punto DataSync final de servicio público o FIPS	70
Pasos a seguir a continuación	70
Configurar su agente para varios NICs	71
Transferencia de datos	72
¿Dónde puedo transferir mis datos?	73
Transferencias admitidas en la misma Cuenta de AWS	73
Transferencias compatibles entre Cuentas de AWS	75
Transferencias admitidas en la misma Región de AWS	76
Transferencias compatibles entre Regiones de AWS	77
Determinar si su transferencia requiere un DataSync agente	77
Transferencia desde o hacia el almacenamiento en las instalaciones	77
Configuración de transferencias con un servidor de archivos NFS	78
Configuración de transferencias con un servidor de archivos SMB	82
Configuración de transferencias con un clúster HDFS	94
Configuración de transferencias con un sistema de almacenamiento de objetos	98
Transferir al AWS almacenamiento o desde él	103
Configuración de transferencias con Amazon S3	104
Configuración de transferencias con Amazon EFS	137
Configurar las transferencias con FSx el servidor de archivos de Windows	147
Configurar transferencias con FSx for Lustre	152
Configuración de transferencias con OpenZFS FSx	155
Configurar las transferencias con FSx ONTAP	158
Transferencia desde o hacia el almacenamiento	167

Planificación de transferencias hacia o desde sistemas de almacenamiento en la nube de terceros	167
Configuración de transferencias con Google Cloud Storage	170
Configuración de transferencias con Microsoft Azure Blob Storage	179
Configurar las transferencias con Microsoft Azure Files	197
Configuración de transferencias con otro almacenamiento de objetos en la nube	201
Transferencia a o desde un almacenamiento compatible con S3 en Snowball Edge	208
Requisitos previos	208
Proporcionar DataSync acceso al almacenamiento compatible con S3	208
Crear un DataSync agente en su entorno de almacenamiento local	210
Configuración de la ubicación de origen de la transferencia	212
Configuración de la ubicación de destino de la transferencia	213
Configuración de los ajustes de su transferencia	214
Inicio de la transferencia	214
Limitaciones	214
Crear una tarea para transferir datos	214
Creación de su tarea de	215
Estados de las tareas	217
Particionar grandes conjuntos de datos con múltiples tareas	218
Segmentación de los datos transferidos con múltiples tareas	219
Elegir un modo de tarea para la transferencia	219
Elegir qué datos transferir	224
Verificación de la integridad de los datos	264
Configuración de los límites de ancho de banda	267
Programación de la tarea	269
Etiquetado de las tareas	274
Iniciar una tarea de transferencia de datos	277
Inicio de la tarea	278
Estados de ejecución de las tareas	279
Saber cuándo la tarea está en cola	280
Cancelación de la ejecución de la tarea	281
Supervisión de las transferencias de datos	282
Descripción de los contadores de rendimiento de transferencia de datos	282
Monitorear las transferencias de datos con CloudWatch métricas	300
CloudWatch métricas para DataSync	300
Supervise las transferencias de datos con informes de tareas	304

Casos de uso	304
Resumen de los informes de tareas	305
Informes de tareas estándar	305
Ejemplos de informes de tareas	308
Limitaciones	312
Creación de informes de tareas	312
Visualización de informes de tareas	322
Supervisión de las transferencias de datos con CloudWatch Logs	323
DataSync Permitir cargar registros a un grupo de CloudWatch registros	323
Configurar el registro para su DataSync tarea	325
Visualización de los registros de DataSync tareas	328
Iniciar sesión con CloudTrail	330
Trabajar con DataSync información en CloudTrail	330
Descripción de las entradas de los archivos de DataSync registro	331
Monitorear con EventBridge	333
DataSync eventos de transferencia	333
Monitoreo de con herramientas manuales	335
Supervise su transferencia mediante la DataSync consola	335
Monitoreo de transferencias mediante la AWS CLI	335
Monitoreo de transferencias mediante la utilidad watch	338
Administración de recursos	339
Administrar a tu DataSync agente	339
Probar la conectividad y los recursos del sistema de su DataSync agente	339
Sustituir a tu agente DataSync	339
Limpiar DataSync los recursos	339
Reutilizar la infraestructura de un DataSync agente	339
Administración de su agente	339
Actualizaciones del software del agente	340
Estados de los agentes	340
Solución de problemas del agente	341
Realizar el mantenimiento de su agente	341
Acceso a la consola local de su agente	342
Configuración de los ajustes de DHCP y DNS de su agente	343
Comprobación de los recursos del sistema de su agente	346
Sincronizar la hora de su agente VMware	348
Ejecutar comandos relacionados con el mantenimiento para su agente	349

Sustitución de su agente	350
Creación de un agente nuevo	350
Actualización de su ubicación con el nuevo agente	351
Pasos a seguir a continuación	356
Filtrar DataSync recursos	356
Parámetros de filtrado	357
Filtrado por ubicación	358
Filtrado por etiquetas	359
Limpiar DataSync los recursos	360
Eliminar un agente DataSync	360
Reutilizar la infraestructura de un DataSync agente	361
Eliminar una DataSync ubicación	361
Eliminar una DataSync tarea	362
Seguridad	364
Protección de los datos	365
Cifrado en tránsito	365
Cifrado en reposo	368
Privacidad del tráfico entre redes	369
Identity and Access Management	369
Administración de accesos	370
AWS políticas gestionadas	375
Políticas administradas por el cliente	385
Cómo utilizar roles vinculados a servicios	388
Etiquetado de recursos durante la creación	392
Prevención de la sustitución confusa entre servicios	394
Validación de conformidad	396
Resiliencia	397
Seguridad de la infraestructura	398
Proteger las credenciales de ubicación de almacenamiento	398
Uso de un secreto administrado por el servicio cifrado con una clave predeterminada	399
Utilizar un secreto administrado por el servicio cifrado con una clave personalizada AWS	
KMS	399
Usando un secreto que tú administras	401
Cuotas	404
Límites del sistema de almacenamiento, de los archivos y de los objetos	404
DataSync cuotas	404

Solicitud de un aumento de cuota	410
Solución de problemas	411
Solución de problemas con los agentes	411
¿Cómo me conecto a la consola local de un EC2 agente de Amazon?	411
¿Qué significa el error Failed to retrieve agent activation key?	412
Sigo sin poder activar un agente mediante un punto de conexión de servicio de VPC	412
¿Qué hago si mi agente está desconectado?	412
No sé qué le pasa a mi agente. ¿Hay alguien que pueda ayudarme?	413
Solución de problemas de ubicación	414
Mi tarea ha fallado debido a un error de permisos de NFS denegados	414
Mi tarea ha fallado debido a un error de montaje de NFS	415
Mi tarea ha fallado debido a un error de montaje de Amazon EFS	416
La propiedad de los archivos no se mantiene con la transferencia NFS	416
Mi tarea no puede acceder a una ubicación SMB que utilice Kerberos	416
Mi tarea ha fallado debido a un error de entrada/salida	418
Error: FsS3UnableToConnectToEndpoint	419
Error: FsS3HeadBucketFailed	419
La tarea falla y se produce un Unable to list Azure Blobs on the volume root error	419
Error: FsAzureBlobVolRootListBlobsFailed	420
Error: SrcLocHitAccess	420
Error: SyncTaskErrorLocationNotAdded	420
La tarea con la ubicación de origen de S3 se produce un GetObjectTagging error HeadObject o se produce un error	420
Solución de problemas relacionados con las tareas	421
Error: SyncOption valor no válido. Opción: TransferMode, PreserveDeletedFiles, Valor: ALL, REMOVE.	421
La ejecución de la tarea falla y se produce un EniNotFounderror	421
La ejecución de la tarea falla y se produce un error de «no se puede asignar memoria»	422
La ejecución de la tarea está en estado de inicio, pero parece que no ocurre nada	422
La ejecución de la tarea parece estancada en el estado de preparación	423
La ejecución de la tarea se detiene antes de que finalice la transferencia	423
Se produce un error en la ejecución de la tarea al transferirla desde un depósito de Google Cloud Storage	424
Hay discordancias entre las marcas de tiempo de ejecución de la tarea	424
La ejecución de la tarea falla debido a NoMem un error	424

El objeto no se puede transferir a Azure Blob Storage con user metadata key error	425
Hay una /.aws-datasync carpeta en la ubicación de destino	425
No se pueden transferir enlaces simbólicos entre ubicaciones mediante SMB	425
Errores en el informe de la tarea	426
Solución de problemas de verificación de datos	426
Hay discrepancias entre el contenido de un archivo	427
Hay una discrepancia entre los metadatos SMB de un archivo	428
Los archivos que se van a transferir ya no se encuentran en la ubicación de origen	429
DataSync no puede verificar los datos de destino	429
DataSync no puede leer los metadatos del objeto	430
Hay una discrepancia en los metadatos de un objeto definidos por el sistema	431
Comprenda la duración de la verificación de datos	433
Solución de problemas de costes de almacenamiento en S3 con DataSync	433
Tutoriales	435
Transferencia del entorno en las instalaciones a S3 entre cuentas	435
Descripción general	435
Requisito previo: permisos de cuenta de origen necesarios	436
Requisito previo: permisos de cuenta de destino obligatorios	438
Paso 1: En tu cuenta de origen, crea un DataSync agente	439
Paso 2: En su cuenta de origen, cree un rol de DataSync IAM para acceder al bucket de destino	439
Paso 3: en su cuenta de destino, actualice su política de buckets de S3	441
Paso 4: En tu cuenta de destino, inhabilita tu bucket ACLs de S3	443
Paso 5: En tu cuenta de origen, crea una ubicación de DataSync origen para tu almacenamiento local	443
Paso 6: En tu cuenta de origen, crea una ubicación de DataSync destino para tu bucket de S3	444
Paso 7: En su cuenta de origen, cree e inicie DataSync la tarea	445
Recursos relacionados	445
Transferencia entre buckets de S3 entre cuentas	446
Descripción general	447
Requisito previo: permisos de cuenta de origen necesarios	448
Requisito previo: permisos de cuenta de destino obligatorios	451
Paso 1: En tu cuenta de origen, crea un rol de DataSync IAM para el acceso al bucket de destino	451
Paso 2: en su cuenta de destino, actualice su política de buckets de S3	453

Paso 3: En tu cuenta de destino, inhabilita tu bucket ACLs de S3	455
Paso 4: En tu cuenta de origen, crea tus DataSync ubicaciones	455
Paso 5: En su cuenta de origen, cree e inicie DataSync la tarea	457
Solución de problemas	459
Relacionado: Transferencias entre cuentas con buckets de S3 mediante el cifrado del servidor	457
Realizar una migración de gran tamaño	460
¿Qué es una migración de datos de gran tamaño?	460
Etapas clave de una migración de datos de gran tamaño	460
Recursos adicionales	461
Etapas 1: Planificar la migración	461
Recopilación de requisitos	462
Ejecución de una prueba de concepto	468
Estimación de los plazos de migración	470
Etapas 2: Implementación de la migración	472
Acelerar la migración con particiones	472
Ejecutando tus DataSync tareas	474
Supervisar sus transferencias	476
DataSync API	477
Acciones	477
CancelTaskExecution	480
CreateAgent	482
CreateLocationAzureBlob	487
CreateLocationEfs	494
CreateLocationFsxLustre	501
CreateLocationFsxOntap	505
CreateLocationFsxOpenZfs	510
CreateLocationFsxWindows	515
CreateLocationHdfs	520
CreateLocationNfs	527
CreateLocationObjectStorage	532
CreateLocationS3	540
CreateLocationSmb	547
CreateTask	555
DeleteAgent	565
DeleteLocation	567

DeleteTask	569
DescribeAgent	571
DescribeLocationAzureBlob	576
DescribeLocationEfs	581
DescribeLocationFsxLustre	587
DescribeLocationFsxOntap	590
DescribeLocationFsxOpenZfs	595
DescribeLocationFsxWindows	599
DescribeLocationHdfs	603
DescribeLocationNfs	608
DescribeLocationObjectStorage	612
DescribeLocationS3	617
DescribeLocationSmb	622
DescribeTask	628
DescribeTaskExecution	638
ListAgents	655
ListLocations	659
ListTagsForResource	663
ListTaskExecutions	667
ListTasks	671
StartTaskExecution	675
TagResource	682
UntagResource	685
UpdateAgent	688
UpdateLocationAzureBlob	690
UpdateLocationEfs	695
UpdateLocationFsxLustre	699
UpdateLocationFsxOntap	702
UpdateLocationFsxOpenZfs	705
UpdateLocationFsxWindows	708
UpdateLocationHdfs	712
UpdateLocationNfs	718
UpdateLocationObjectStorage	721
UpdateLocationS3	727
UpdateLocationSmb	731
UpdateTask	738

UpdateTaskExecution	745
Data Types	747
AgentListEntry	750
AzureBlobSasConfiguration	752
CmkSecretConfig	753
CustomSecretConfig	755
Ec2Config	757
FilterRule	759
FsxProtocol	761
FsxProtocolNfs	762
FsxProtocolSmb	763
FsxUpdateProtocol	765
FsxUpdateProtocolSmb	767
HdfsNameNode	769
LocationFilter	771
LocationListEntry	773
ManagedSecretConfig	775
ManifestConfig	776
NfsMountOptions	778
OnPremConfig	780
Options	781
Platform	790
PrivateLinkConfig	791
QopConfiguration	793
ReportDestination	795
ReportDestinationS3	796
ReportOverride	798
ReportOverrides	799
ReportResult	801
S3Config	802
S3ManifestConfig	803
SmbMountOptions	805
SourceManifestConfig	807
TagListEntry	808
TaskExecutionFilesFailedDetail	809
TaskExecutionFilesListedDetail	811

TaskExecutionListEntry	813
TaskExecutionResultDetail	815
TaskFilter	818
TaskListEntry	820
TaskReportConfig	822
TaskSchedule	824
TaskScheduleDetails	826
Errores comunes	827
Parámetros comunes	829
Historial de documentos	832
AWS Glosario	848
.....	dcccxlx

¿Qué es AWS DataSync?

AWS DataSync es un servicio de transferencia de datos en línea que simplifica la migración de datos y le ayuda a transferir de forma rápida, fácil y segura los datos de sus archivos u objetos hacia, desde y entre AWS los servicios de almacenamiento.

Transferencias de almacenamiento en las instalaciones

DataSync funciona con los siguientes sistemas de almacenamiento local:

- [Sistema de archivos de red \(NFS\)](#)
- [Servidor de Server Message Block \(SMB\)](#)
- [Sistema de archivos distribuido de Hadoop \(HDFS\)](#)
- [Almacenamiento de objetos](#)

AWS transferencias de almacenamiento

DataSync funciona con los siguientes servicios AWS de almacenamiento:

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

Otras transferencias de almacenamiento en la nube

DataSync funciona con los siguientes servicios de almacenamiento en otras nubes:

- [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](#)

Transferencias de almacenamiento en la periferia

DataSync funciona con los siguientes dispositivos y servicios de almacenamiento perimetral:

- [Almacenamiento compatible con Amazon S3 en AWS Snowball Edge](#)

Casos de uso

Estos son algunos de los principales casos de uso de DataSync:

- **Migre datos:** transfiera conjuntos de datos activos rápidamente a través de la red a los servicios AWS de almacenamiento. DataSync incluye el cifrado automático y la validación de la integridad de los datos para garantizar que los datos lleguen de forma segura, intacta y lista para su uso.
- **Archivar datos inactivos:** traslade los datos inactivos guardados en el almacenamiento en las instalaciones directamente a clases de almacenamiento duraderas y seguras a largo plazo, como S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. De este modo, puede liberar capacidad de almacenamiento en las instalaciones y cerrar los sistemas heredados.
- **Replicar datos:** copie datos en cualquier clase de almacenamiento de Amazon S3 y elija la clase de almacenamiento más rentable según sus necesidades. También puede enviar datos a Amazon EFS, FSx para Windows File Server, FSx para Lustre o para OpenZFS FSx para un sistema de archivos en espera.
- **Transfiera datos para procesarlos oportunamente en la nube:** transfiera datos de entrada o salida para su procesamiento. AWS Este enfoque puede acelerar los flujos de trabajo críticos en la nube híbrida en mucho sectores. Esto incluye machine learning en ciencias de la vida, producción de vídeo en medios de comunicación y entretenimiento, análisis de macrodatos e investigación sísmica en la industria del petróleo y el gas.

Ventajas

Al usarlo DataSync, puede obtener los siguientes beneficios:

- **Automatice el movimiento de datos:** DataSync facilita la transferencia de datos a través de la red entre los sistemas y servicios de almacenamiento. DataSync automatiza tanto la gestión de los procesos de transferencia de datos como la infraestructura necesaria para una transferencia de datos segura y de alto rendimiento.
- **Transfiera datos de forma segura:** DataSync proporciona end-to-end seguridad, incluido el cifrado y la validación de la integridad de los datos, para garantizar que sus datos lleguen de forma segura, intactos y listos para su uso. DataSync accede al AWS almacenamiento mediante mecanismos de AWS seguridad integrados, como las funciones AWS Identity and Access Management (IAM). También es compatible con los puntos de conexión de la nube privada virtual (VPC), lo que le brinda la opción de transferir datos sin atravesar la internet pública y aumenta todavía más la seguridad de los datos copiados en línea.
- **Mueva los datos más rápido:** DataSync utiliza un protocolo de red especialmente diseñado y una arquitectura paralela de subprocesos múltiples para acelerar las transferencias. Este enfoque agiliza las migraciones, ejecutando flujos de procesamiento de datos para el análisis y el machine learning, y procesos de protección de datos.

Recursos adicionales

Le recomendamos que lea lo siguiente:

- [DataSync recursos](#): incluye blogs, vídeos y otros materiales de formación
- [AWS Re:post](#): consulte las últimas discusiones DataSync
- [Precios de AWS DataSync](#)

Cómo AWS DataSync funciona

Conozca los conceptos y la terminología clave relacionados con las AWS DataSync transferencias, incluida la forma en que se transfieren los datos desde ubicaciones locales y en la nube.

DataSync arquitectura de transferencia

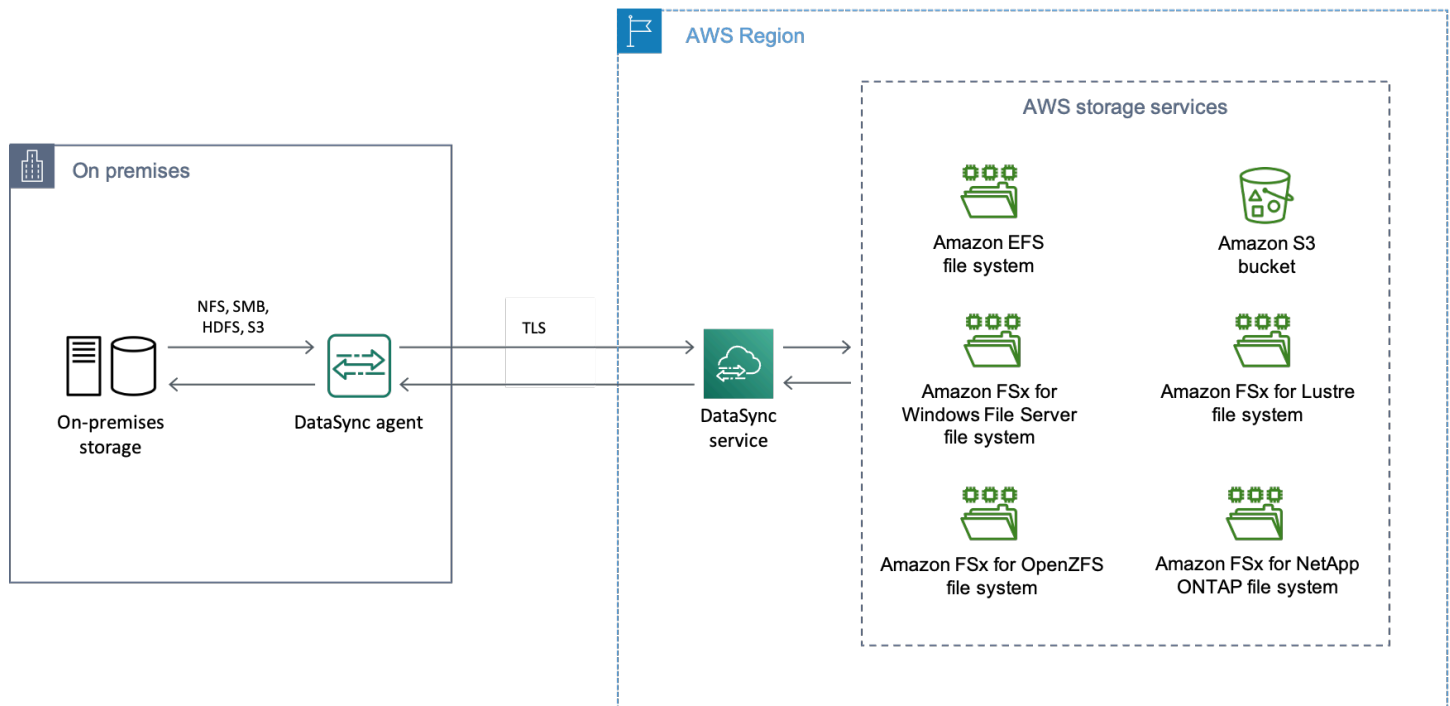
Los siguientes diagramas muestran cómo y dónde se transfieren DataSync habitualmente los datos de almacenamiento. Para obtener una lista completa de los sistemas y servicios de almacenamiento DataSync compatibles, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

Temas

- [Transferencia entre el almacenamiento en las instalaciones y AWS](#)
- [Transferencia entre servicios AWS de almacenamiento](#)
- [Transferencia entre servicios AWS de almacenamiento y sistemas de almacenamiento en otras nubes](#)

Transferencia entre el almacenamiento en las instalaciones y AWS

El siguiente diagrama muestra una descripción general de alto nivel de la DataSync transferencia de archivos entre sistemas de almacenamiento locales autogestionados y. Servicios de AWS

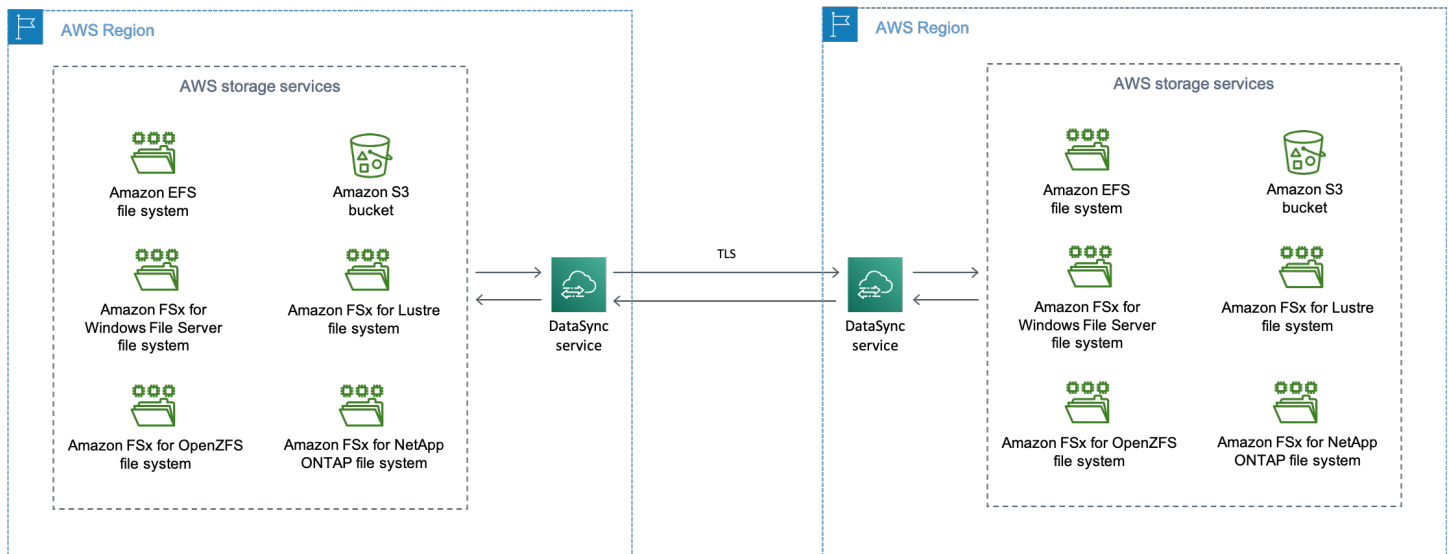


El diagrama ilustra un caso de DataSync uso común:

- Un DataSync agente que copia datos de un sistema de almacenamiento local.
- Los datos que se transfieren AWS y se cifran mediante Transport Layer Security (TLS).
- DataSync copiar datos a un servicio de AWS almacenamiento compatible.

Transferencia entre servicios AWS de almacenamiento

En el siguiente diagrama se muestra una descripción general de alto nivel de la DataSync transferencia de archivos entre Servicios de AWS los mismos Cuenta de AWS.



El diagrama ilustra un caso de DataSync uso común:

- DataSync copiar datos de un servicio AWS de almacenamiento compatible.
- Datos que se transfieren Regiones de AWS y se cifran mediante TLS.
- DataSync copiar datos a un servicio de AWS almacenamiento compatible.

Al realizar transferencias entre servicios AWS de almacenamiento (ya sea en el mismo servicio Región de AWS o entre Regiones de AWS ellos), los datos permanecen en la AWS red y no circulan por la red pública de Internet.

Important

Pagas por los datos que se transfieran entre Regiones de AWS ellos. Esto se factura como transferencia de datos de SALIDA desde la región de origen a la región de destino. Para obtener más información, consulte [Data transfer pricing](#).

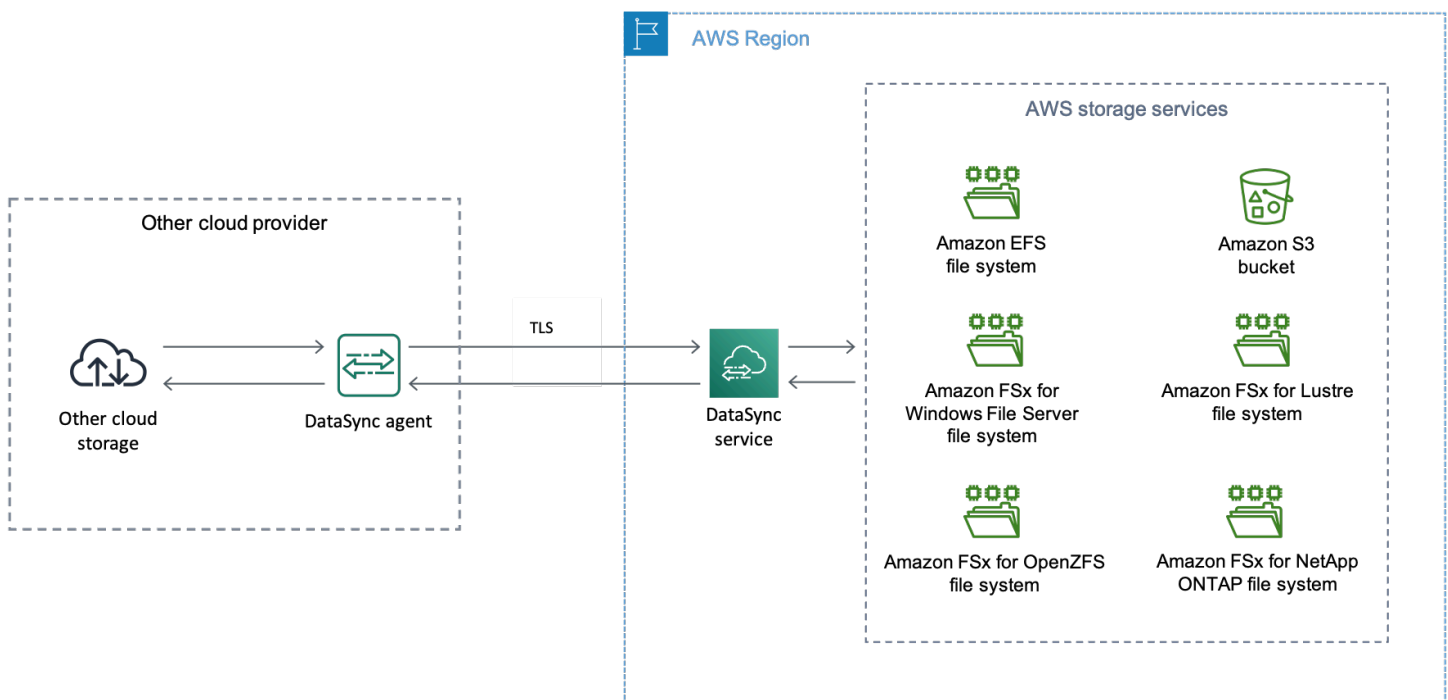
Transferencia entre servicios AWS de almacenamiento y sistemas de almacenamiento en otras nubes

Con DataSync, puede transferir datos entre otros sistemas de almacenamiento en la nube y Servicios de AWS. En este contexto, los sistemas de almacenamiento en la nube pueden ser:

- Sistemas de almacenamiento autoadministrados, como un servidor de archivos de NFS en su nube privada virtual (VPC) de AWS.
- Sistemas o servicios de almacenamiento alojados por otro proveedor de nube. Para obtener más información, consulte [Transferir hacia o desde otro almacenamiento en la nube con AWS DataSync](#).

DataSync puede copiar datos hacia y desde otras nubes con o sin el uso de un agente. Para obtener más información sobre cuándo usar un agente, consulte [¿Necesito un AWS DataSync agente?](#).

El siguiente diagrama muestra una descripción general de alto nivel de la DataSync transferencia de datos entre los servicios AWS de almacenamiento y otro proveedor de servicios en la nube.



Conceptos y terminología

Familiarícese con las funciones de DataSync transferencia.

Temas

- [Agente](#)
- [Ubicación](#)
- [Tarea](#)
- [Ejecución de tarea](#)

Agente

Un agente es un dispositivo de máquina virtual (VM) que se utiliza para leer y escribir en el almacenamiento durante una transferencia.

Puede implementar un agente en su entorno de almacenamiento en una máquina virtual basada en VMware ESXi el núcleo de Linux (KVM) o en hipervisores Microsoft Hyper-V. Para el almacenamiento en una nube privada virtual (VPC) AWS, puede implementar un agente como una instancia de Amazon EC2.

Para empezar, consulte [¿Necesito un AWS DataSync agente?](#).

Ubicación

Una ubicación describe el lugar desde o hacia el que se copian los datos. Cada DataSync transferencia (también conocida como tarea) tiene una ubicación de origen y de destino. Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

Tarea

Una tarea describe una DataSync transferencia. Identifica una ubicación de origen y destino, junto con detalles sobre cómo copiar datos entre esas ubicaciones. También puedes especificar cómo gestiona una tarea los metadatos, los archivos eliminados y los permisos.

Ejecución de tarea

La ejecución de una tarea es una ejecución individual de una tarea de DataSync transferencia. La ejecución de una tarea implica varias fases. Para obtener más información, consulte [Estados de ejecución de las tareas](#).

Cómo DataSync transfiere los archivos, objetos y directorios

Durante la [ejecución de una tarea](#), DataSync prepara, transfiere y verifica los datos. La forma en que se realizan estas acciones depende de cómo configure las opciones de la DataSync tarea, como el [modo de tarea](#). Las tareas del modo básico preparan, transfieren y verifican los datos de forma secuencial, mientras que las tareas del modo mejorado las realizan en paralelo.

Temas

- [¿Cómo DataSync se prepara la transferencia de datos](#)
- [¿Cómo se DataSync transfieren tus datos](#)
- [¿Cómo DataSync verifica la integridad de los datos](#)
- [¿Cómo DataSync funciona con los archivos abiertos y bloqueados](#)
- [Opciones de transferencia recurrentes](#)

¿Cómo DataSync se prepara la transferencia de datos

DataSync de forma predeterminada, prepara la transferencia examinando las ubicaciones de origen y destino para determinar qué transferir. Esto se hace escaneando el contenido y los metadatos de ambas ubicaciones para identificar las diferencias entre las dos.

Note

Si configuras tu tarea para [transferir todos los datos](#), no tendrás que prepararte para ello. Al iniciar la tarea, transfiere DataSync inmediatamente todo desde el origen hasta el destino sin comparar ubicaciones.

La forma en que DataSync se prepare la transferencia también depende del modo de tarea:

Preparación mejorada del modo	Preparación del modo básico
DataSync prepara los objetos a medida que se encuentran en la ubicación de origen. La preparación continúa durante la ejecución de la tarea hasta que no haya más objetos en la lista de origen.	La preparación puede tardar solo unos minutos, unas horas o incluso más, según la cantidad de archivos, objetos o directorios en ambas ubicaciones y el rendimiento del almacenamiento.
A diferencia del modo básico, DataSync puede preparar un número prácticamente ilimitado de objetos con cada ejecución de tarea.	Los elementos que se DataSync inventarian en el origen y en el destino se tienen en cuenta para las cuotas de tareas . Estas cuotas no se basan en la cantidad de elementos que se DataSync transfieren durante la ejecución de cada tarea.

DataSync puede omitir algunos archivos, objetos y directorios durante la preparación. Los motivos de esto pueden depender de varios factores, como la forma en que configure las tareas y los permisos del sistema de almacenamiento. Estos son algunos ejemplos:

- Uno de los archivos de la ubicación de origen existe en las ubicaciones de origen y de destino. El archivo del origen no se ha modificado desde la ejecución anterior de la tarea. Como [solo está transfiriendo datos que han cambiado](#), DataSync no transferirá ese archivo la próxima vez que ejecute la tarea.
- Un objeto que existe en ambas ubicaciones cambia en el origen. Al ejecutar la tarea, DataSync omite este objeto en el destino porque la tarea no [sobrescribe los datos del](#) destino.
- DataSync omite un objeto de la ubicación de origen que utiliza una [clase de almacenamiento de archivos y no](#) se restaura. Debe restaurar un objeto archivado para DataSync poder leerlo.
- DataSync omite un archivo, objeto o directorio de la ubicación de origen porque no puede leerlo. Si esto ocurre y no es lo esperado, comprueba los permisos de acceso del almacenamiento y asegúrate de que DataSync puede leer lo que se omitió.

¿Cómo se DataSync transfieren tus datos

DataSync copia los datos (incluidos los metadatos) del origen al destino en función de las opciones de la tarea. Por ejemplo, puede especificar qué [metadatos](#) se copiarán, [excluir](#) determinados archivos y limitar el DataSync uso del [ancho](#) de banda, entre otras opciones.

La forma en que se DataSync transfieren los datos también depende del modo de tarea:

Modo de transferencia mejorado	Modo básico de transferencia
DataSync transfiere cada objeto tan pronto como esté preparado.	Una DataSync vez preparados todos los datos, comienza la transferencia.

DataSync puede omitir algunos elementos durante la transferencia. Si configuras la tarea para [transferir todos los datos](#), esto puede ocurrir con un objeto de la ubicación de origen que utilice una [clase de almacenamiento de archivos](#) y no esté restaurado.

¿Cómo DataSync verifica la integridad de los datos

DataSync siempre realiza comprobaciones de integridad de sus datos durante una transferencia. Al final de una transferencia, también DataSync puede realizar comprobaciones adicionales solo

en los datos transferidos o en todo el conjunto de datos en ambas ubicaciones. Para obtener más información, consulte [Configurar cómo se AWS DataSync verifica la integridad de los datos](#).

Al comprobar la integridad de los datos, DataSync calcula y compara la suma de verificación y los metadatos de los archivos, objetos o directorios de sus ubicaciones. Si detecta DataSync diferencias entre las ubicaciones, la verificación no se realiza correctamente y se produce un error. Por ejemplo, es posible que veas errores como `Checksum failure`, `Metadata failure`, `Files were added`, o `Files were removed`.

El funcionamiento de la verificación depende del modo de tarea y de si la has configurado DataSync para comprobar la integridad de los datos al final de la transferencia.

Modo de verificación mejorado	Verificación del modo básico
DataSync verifica cada objeto a medida que se transfiere a su destino.	Al final de la transferencia, DataSync verifica la integridad de los datos.
Con el modo mejorado, DataSync verifica solo los datos transferidos .	En función de cómo configure la verificación de datos , esto puede llevar un tiempo considerable en el caso de conjuntos de datos de gran tamaño.

¿Cómo DataSync funciona con los archivos abiertos y bloqueados

Tenga en cuenta lo siguiente cuando intente transferir archivos que estén abiertos (en uso) o bloqueados:

- En general, DataSync puede transferir archivos abiertos sin ninguna limitación.
- Si un archivo está abierto y se está grabando en él durante una transferencia, DataSync puede detectar este tipo de incoherencia durante la fase de verificación de la tarea de transferencia. Para obtener la versión más reciente del archivo, debe volver a ejecutar la tarea.
- Si un archivo está bloqueado y el servidor DataSync impide abrirlo, lo DataSync omite durante la transferencia y registra un error.
- DataSync no puede bloquear ni desbloquear archivos.

Opciones de transferencia recurrentes

Además de las transferencias únicas, DataSync puede transferir datos de forma recurrente. Algunas de las opciones para estas situaciones son:

- [Programar](#) cuándo se ejecuta la tarea.
- Transferir [solo los datos que han cambiado](#) desde la ejecución anterior de la tarea.
- [Eliminar datos de la ubicación de destino](#) que ya no están presentes en el origen.

Empezar con AWS DataSync

Antes de empezar AWS DataSync, tienes que suscribirte a una Cuenta de AWS si no tienes una. También te recomendamos que averigües dónde se DataSync pueden usar tus datos y cuánto podría costar transferirlos.

Inscríbese en una Cuenta de AWS

Si no tiene una Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abrir <https://portal.aws.amazon.com/billing/registro>.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWS se crea uno. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar [tareas que requieren acceso de usuario raíz](#).

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a <https://aws.amazon.com/> y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión [AWS Management Console](#) como propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte [Iniciar sesión como usuario raíz](#) en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

Para obtener instrucciones, consulte [Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz \(consola\)](#) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en [Activar AWS IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte [Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la](#) Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte [Create a permission set](#) en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte [Add groups](#) en la Guía del usuario de AWS IAM Identity Center .

Permisos de IAM necesarios para usar DataSync

DataSync puede transferir sus datos a un bucket de Amazon S3, a un sistema de archivos Amazon EFS o a [otros servicios de AWS almacenamiento](#). Para llevar sus datos a donde quiera, necesita que se le concedan los permisos de IAM correctos para su identidad. Por ejemplo, la función de IAM que utilice DataSync necesita permiso para utilizar las operaciones de Amazon S3 necesarias para transferir datos a un bucket de S3.

Puede conceder estos permisos con las políticas de IAM proporcionadas por las suyas AWS o creando las suyas propias.

Contenido

- [AWS políticas gestionadas](#)
- [Políticas administradas por el cliente](#)

AWS políticas gestionadas

AWS proporciona las siguientes políticas administradas para casos de DataSync uso comunes:

- `AWSDataSyncReadOnlyAccess`— Proporciona acceso de solo lectura a DataSync
- `AWSDataSyncFullAccess`— Proporciona acceso total DataSync y acceso mínimo a sus dependencias.

Para obtener más información, consulte [AWS políticas gestionadas para AWS DataSync](#).

Políticas administradas por el cliente

Puede crear políticas de IAM personalizadas para usarlas con ellas. DataSync Para obtener más información, consulte [Políticas administradas por el cliente para AWS DataSync](#).

¿Dónde puedo utilizarlas? DataSync

Para obtener una lista de Regiones de AWS los puntos finales DataSync compatibles, consulte los [AWS DataSync puntos finales y las cuotas](#) en. Referencia general de AWS

¿Cómo puedo usarlo? DataSync

Hay varias maneras de usarlo DataSync:

- [DataSync consola](#), que forma parte de la AWS Management Console.
- [DataSync API](#) o la [AWS CLI](#) para configurar y administrar mediante programación. DataSync
- [AWS CloudFormation](#) o [Terraform](#) para aprovisionar sus recursos. DataSync
- [AWS SDKs](#) para crear aplicaciones que utilicen DataSync.

¿Cuánto va a DataSync costar?

En la página de [DataSync precios](#), crea una estimación personalizada con la cantidad de datos que planeas transferir.

Componentes de código abierto utilizados por DataSync

Para ver los componentes de código abierto que utiliza DataSync, descargue el siguiente enlace:

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

¿Necesito un AWS DataSync agente?

Para usarlo AWS DataSync, es posible que necesite un agente. Un agente es un dispositivo de máquina virtual (VM) que se implementa en el entorno de almacenamiento para la transferencia de datos.

La necesidad de un agente depende de varios factores, como el tipo de almacenamiento al que se transfiera o desde el que se transfiera, si se realiza la transferencia de un lugar a otro Cuentas de AWS y entre cuál se Regiones de AWS realiza la transferencia. Antes de seguir leyendo, [comprueba que DataSync sea compatible con la transferencia que te interesa](#).

Después de determinar si es DataSync compatible con tu escenario de transferencia, revisa la siguiente información para ayudarte a entender si necesitas un agente.

Situaciones en las que necesita un DataSync agente

La mayoría de las situaciones que requieren un DataSync agente implican un almacenamiento gestionado por usted o por otro proveedor de servicios en la nube.

- Transferencia entre servicios AWS de almacenamiento y almacenamiento local
- Transferencia entre Amazon EFS o Amazon FSx y almacenamiento en otras nubes
- Transferencia hacia o desde el almacenamiento en la periferia
- Transferencia entre algunos servicios AWS de almacenamiento Cuentas de AWS (cuando ninguno de los dos servicios de almacenamiento es Amazon S3)

Para obtener más información, consulte [Transferencias compatibles entre Cuentas de AWS](#).

- Transferencias entre un comercio Región de AWS y otro AWS GovCloud (US) en el que el origen y el destino son Amazon EFS o Amazon FSx.

Situaciones en las que no necesita un DataSync agente

Las situaciones en las que no es necesario contar con un agente se aplican tanto si realiza una transferencia en la [misma Región de AWS](#) como [entre regiones](#).

- Transferir entre servicios AWS de almacenamiento en el mismo Cuenta de AWS
- Transferencia entre Amazon S3 y un servicio AWS de almacenamiento diferente entre Cuentas de AWS
- Transferencia entre Amazon S3 y el almacenamiento de objetos en otras nubes
- Transferencia entre un centro comercial Región de AWS y otro AWS GovCloud (US) en el que el origen o el destino es Amazon S3

Uso de varios DataSync agentes

Si bien la mayoría de las transferencias solo necesitan un agente, el uso de varios agentes puede acelerar las transferencias de grandes conjuntos de datos con millones de archivos u objetos. En estas situaciones, recomendamos ejecutar las tareas de transferencia en paralelo. Este enfoque distribuye la carga de trabajo de transferencia entre varias tareas, y cada tarea utiliza su propio

agente. También ayuda a reducir el tiempo necesario DataSync para preparar y transferir los datos. Para obtener más información, consulte [Particionar grandes conjuntos de datos con múltiples tareas](#).

Otra opción, especialmente si tiene millones de archivos pequeños, es utilizar varios agentes con una ubicación de transferencia. Por ejemplo, puede conectar hasta cuatro agentes al servicio de archivos del sistema de archivos de red (NFS) en las instalaciones. Esta opción puede acelerar la transferencia, aunque el tiempo que se tarda en DataSync prepararla no cambia.

Con cualquiera de estos enfoques, tenga en cuenta que pueden aumentar las operaciones de E/S del almacenamiento y afectar al ancho de banda de la red. Para obtener más información sobre el uso de varios agentes para tus DataSync transferencias, consulta el [blog sobre AWS almacenamiento](#).

Si está pensando en utilizar varios agentes, recuerde lo siguiente:

- El uso de varios agentes con una ubicación no proporciona una alta disponibilidad. Todos los agentes asociados a una ubicación deben estar conectados antes de que pueda iniciar la tarea de transferencia. Si uno de los agentes está [desconectado](#), no podrá ejecutar la tarea.
- Si [utiliza un punto final del servicio de nube privada virtual \(VPC\) para comunicarse con el DataSync servicio](#), todos los agentes deben usar el mismo punto final y la misma subred.

Pasos a seguir a continuación

- Si necesita un agente, revise [los requisitos del agente](#) para saber qué es lo que mejor se adapta a su entorno de almacenamiento.
- Si no necesita un agente para la transferencia, puede empezar a [configurar la transferencia](#).

Requisitos para los agentes AWS DataSync

Antes de [implementar](#) un AWS DataSync agente en su entorno de almacenamiento, asegúrese de comprender los requisitos de recursos y del hipervisor del agente.

Requisitos del hipervisor

Puede ejecutar un DataSync agente en los siguientes hipervisores:

- VMware ESXi (versión 6.5, 6.7, 7.0 u 8.0): VMware ESXi está disponible en el sitio web de [Broadcom](#). También necesita un cliente VMware vSphere para conectarse al host.

- Máquina virtual basada en el kernel (KVM) de Linux: una tecnología de virtualización gratuita y de código abierto. El KVM está incluido en las versiones 2.6.20 y posteriores de Linux. DataSync está probado y es compatible con las distribuciones CentOS/RHEL 7 y 8, Ubuntu 16.04 LTS y Ubuntu 18.04 LTS. Puede haber otra distribución moderna de Linux que funcione, pero la funcionalidad o el rendimiento no están garantizados. Debe habilitar la virtualización acelerada por hardware en su host KVM para implementar su agente. DataSync

Recomendamos esta opción si ya tiene un entorno KVM en funcionamiento y ya está familiarizado con el funcionamiento de KVM.

No se admite la ejecución de KVM en Amazon EC2 y no se puede usar con DataSync agentes.

- Microsoft Hyper-V (versión 2012 R2, 2016 o 2019): para esta configuración, necesitará Microsoft Hyper-V Manager en un equipo cliente Microsoft Windows para conectarse al host.

El DataSync agente es una máquina virtual (VM) de primera generación. Para obtener más información sobre las diferencias entre las generaciones 1 y 2 VMs, consulte [¿Debo crear una máquina virtual de primera o segunda generación en Hyper-V?](#)

- Amazon EC2: DataSync proporciona una imagen de máquina de Amazon (AMI) que contiene la DataSync imagen. Consulte [Requisitos de las EC2 instancias de Amazon](#) para ver los tipos de instancias recomendadas.

Requisitos de agente para las DataSync transferencias

Para DataSync las transferencias, su agente debe cumplir con los siguientes requisitos de recursos.

Important

Tenga en cuenta que los requisitos del agente para trabajar con hasta 20 millones de archivos, objetos o directorios son directrices generales. Es posible que su agente necesite más recursos debido a otros factores, como el número de directorios que tenga y el tamaño de los metadatos de los objetos. Por ejemplo, es posible que la instancia m5.2xlarge de un EC2 agente de Amazon aún no sea suficiente para una transferencia de menos de 20 millones de archivos.

Contenido

- [Requisitos de la máquina virtual](#)

- [Requisitos de las EC2 instancias de Amazon](#)

Requisitos de la máquina virtual

Al implementar un DataSync agente que no está en una EC2 instancia de Amazon, la máquina virtual del agente requiere los siguientes recursos:

- Procesadores virtuales: cuatro procesadores virtuales asignados a la MV.
- Espacio de disco: 80 GB de espacio de disco para instalar los datos del sistema y la imagen de la MV.
- RAM: según la situación de transferencia, necesitará la siguiente cantidad de memoria:
 - 32 GB de RAM asignados a la máquina virtual para ejecutar tareas con hasta 20 millones de archivos, objetos o directorios.
 - 64 GB de RAM asignados a la máquina virtual para ejecutar tareas con más de 20 millones de archivos, objetos o directorios.

Requisitos de las EC2 instancias de Amazon

Al implementar un DataSync agente en una EC2 instancia de Amazon, el tamaño de la instancia debe ser de al menos 2 veces mayor.

Recomendamos utilizar uno de los siguientes tamaños de instancia:

- m5.2xlarge: para ejecutar tareas con hasta 20 millones de archivos, objetos o directorios.
- m5.4xlarge: para ejecutar tareas con más de 20 millones de archivos, objetos o directorios.

Requisitos de agente para las particiones Región de AWS

DataSync las imágenes de los agentes están asociadas a [Región de AWS particiones](#) específicas. Por ejemplo, de forma predeterminada, no puedes descargar un agente en un anuncio Región de AWS y, a continuación, activarlo en un AWS GovCloud (US) Region.

Requisitos de administración de agentes

Una vez que [actives](#) tu DataSync agente AWS , lo administrará por ti. Para obtener más información, consulte [Administrar a tu AWS DataSync agente](#).

Despliegue de su AWS DataSync agente

Al crear un AWS DataSync agente, el primer paso es implementarlo en su entorno de almacenamiento. Puede implementar un agente como una máquina virtual (VM) en VMware ESXi una máquina virtual basada en el núcleo de Linux (KVM) y en hipervisores Microsoft Hyper-V. También puede implementar un agente como una EC2 instancia de Amazon en una nube privada virtual (VPC) interna. AWS

Tip

Antes de empezar, confirme si [necesita un DataSync agente](#).

Despliegue de su agente en VMware

Puede descargar un agente desde la DataSync consola e implementarlo en su VMware entorno.

Antes de empezar: asegúrese de que su entorno de almacenamiento sea compatible con un DataSync agente. Para obtener más información, consulte [Requisitos de la máquina virtual](#).

Para implementar un agente en VMware

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, elija Agentes y luego, Crear agente.
3. Para Hypervisor, elija y VMWare ESXi, a continuación, elija Descargar la imagen.

El agente se descarga en un archivo .zip que contiene un archivo de imagen .ova.

4. Para minimizar la latencia de la red, despliegue el agente lo más cerca posible del sistema de almacenamiento al que DataSync necesita acceder (de ser posible, la misma red local). Para obtener más información, consulte [Requisitos de red para el almacenamiento autoadministrado en las instalaciones y otros tipos de almacenamiento periférico en la nube](#).

Si es necesario, consulte la documentación del hipervisor sobre cómo implementar un .ova archivo en un VMware host.

5. Encienda su hipervisor, inicie sesión en el agente de la VM y obtenga la dirección IP del agente. Necesitará esta dirección IP para activar el agente.

Las credenciales predeterminadas de la máquina virtual del agente son el nombre de inicio de sesión **admin** y la contraseña **password**. Si es necesario, cambie la contraseña a través de la [consola local de la máquina virtual](#).

Paso siguiente: [Elección de un punto de conexión de servicio para su agente de AWS DataSync](#)

Implementación del agente en KVM

Puede descargar un agente desde la DataSync consola e implementarlo en su entorno KVM.

Antes de empezar: asegúrese de que su entorno de almacenamiento sea compatible con un DataSync agente. Para obtener más información, consulte [Requisitos de la máquina virtual](#).

Cómo implementar un agente en KVM

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, elija Agentes y luego, Crear agente.
3. Para el hipervisor, elija Máquina virtual basada en el kernel (KVM) y, a continuación, elija Descargar la imagen.

El agente se descarga en un archivo .zip que contiene un archivo de imagen .qcow2.

4. Para minimizar la latencia de la red, despliegue el agente lo más cerca posible del sistema de almacenamiento al que DataSync necesita acceder (de ser posible, la misma red local). Para obtener más información, consulte [Requisitos de red para el almacenamiento autoadministrado en las instalaciones y otros tipos de almacenamiento periférico en la nube](#).
5. Ejecute el siguiente comando para instalar su imagen .qcow2.

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


Para obtener información sobre cómo administrar esta máquina virtual y su host de KVM, consulte la documentación del hipervisor.

6. Encienda su hipervisor, inicie sesión en la máquina virtual y obtenga la dirección IP del agente. Necesitará esta dirección IP para activar el agente.

Las credenciales predeterminadas de la máquina virtual del agente son el nombre de inicio de sesión **admin** y la contraseña **password**. Si es necesario, cambie la contraseña a través de la [consola local de la máquina virtual](#).

Paso siguiente: [Elección de un punto de conexión de servicio para su agente de AWS DataSync](#)

Implementación del agente en Microsoft Hyper-V

Puede descargar un agente de la DataSync consola e implementarlo en su entorno Microsoft Hyper-V.

Antes de empezar: asegúrese de que su entorno de almacenamiento sea compatible con un DataSync agente. Para obtener más información, consulte [Requisitos de la máquina virtual](#).

Cómo implementar un agente en Hyper-V

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, elija Agentes y luego, Crear agente.
3. Para Hipervisor, seleccione Microsoft Hyper-V y, a continuación, seleccione Descargar la imagen.

El agente se descarga en un archivo .zip que contiene un archivo de imagen .vhdx.

4. Para minimizar la latencia de la red, despliegue el agente lo más cerca posible del sistema de almacenamiento al que DataSync necesita acceder (de ser posible, la misma red local). Para obtener más información, consulte [Requisitos de red para el almacenamiento autoadministrado en las instalaciones y otros tipos de almacenamiento periférico en la nube](#).

Si es necesario, consulte la documentación del hipervisor sobre cómo implementar un archivo .vhdx en un host de Hyper-V.

 Warning

Si habilita la cola de máquinas virtuales (VMQ) en un host de Hyper-V que utilice un adaptador de red Broadcom, es posible que observe un rendimiento de red deficiente. Para obtener más información sobre soluciones alternativas, consulte la documentación de [Microsoft](#).

5. Encienda su hipervisor, inicie sesión en la máquina virtual y obtenga la dirección IP del agente. Necesitará esta dirección IP para activar el agente.

Las credenciales predeterminadas de la máquina virtual del agente son el nombre de inicio de sesión **admin** y la contraseña **password**. Si es necesario, cambie la contraseña a través de la [consola local de la máquina virtual](#).

Paso siguiente: [Elección de un punto de conexión de servicio para su agente de AWS DataSync](#)

Despliegue de su EC2 agente de Amazon

Puedes implementar un DataSync agente como EC2 instancia de Amazon al transferir datos entre:

- Un sistema de almacenamiento en la nube autogestionado (por ejemplo, un servidor de archivos NFS AWS) y un servicio AWS de almacenamiento.
- Un proveedor de almacenamiento en la nube (como Microsoft Azure Blob Storage o Google Cloud Storage) y un servicio AWS de almacenamiento.
- Un depósito de S3 en un anuncio Región de AWS y un depósito de S3 en un AWS GovCloud (US) Region.
- [Amazon S3 activado AWS Outposts](#) y un servicio AWS de almacenamiento.

 Warning

No recomendamos utilizar un EC2 agente de Amazon con almacenamiento local debido al aumento de la latencia de la red. En su lugar, implemente el agente como una VMware máquina virtual KVM o Hyper-V en su centro de datos lo más cerca posible de su almacenamiento local.

EC2 Despliegue de su agente

Para elegir el agente AMI para su Región de AWS

1. Abre un terminal y copia el siguiente AWS CLI comando para obtener el último ID de DataSync Amazon Machine Image (AMI) de la región en la que quieres implementar tu EC2 agente de Amazon.

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

2. Ejecute el comando . En el resultado, anote la "Value" propiedad con el ID de DataSync AMI.

Example Comando y salida de ejemplo

```
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 implementar tu EC2 agente de Amazon

Tip

Para evitar cargos por transferir entre zonas de disponibilidad, implemente su agente de forma que no requiera tráfico de red entre las zonas de disponibilidad. (Para obtener más información sobre los precios de transferencia de datos para todos Regiones de AWS, consulta los [precios de Amazon EC2 Data Transfer](#)).

Por ejemplo, implemente el agente en la zona de disponibilidad en la que está ubicado el sistema de almacenamiento en la nube autoadministrado.

1. Copie la siguiente URL:

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

- Sustituya el valor *agent-region* por la región en la que quiera implementar el agente.
- *ami-id* Sustitúyala por la ID de DataSync AMI que obtuviste.

2. Pegue la URL en un navegador.

Aparece la página de lanzamiento de la EC2 instancia de AWS Management Console Amazon.

3. Para el tipo de instancia, elige una de las [EC2 instancias de Amazon recomendadas](#) para DataSync.
4. En Par de claves, seleccione un par de claves existente o cree uno nuevo.
5. Para Configuración de red, elija Editar y realice lo siguiente:
 - a. En lo que respecta a la VPC, elija una VPC en la que quiera implementar el agente.
 - b. Para asignar automáticamente una IP pública, elija si quiere que el agente sea accesible desde la red Internet pública.

Utilizará la dirección IP pública o privada de la instancia más adelante para activar su agente.

- c. Para el firewall (grupos de seguridad), cree o seleccione un grupo de seguridad que haga lo siguiente:
 - Si es necesario, permite el tráfico entrante a la EC2 instancia de Amazon en el puerto 80 (HTTP). Algunas opciones para [obtener la clave de activación de un agente](#) requieren esta conexión.
 - Permite el tráfico entrante y saliente entre la EC2 instancia de Amazon y el sistema de almacenamiento desde o hacia el que se transfieren los datos. Para obtener más información, consulte [Requisitos de red para el almacenamiento autoadministrado en las instalaciones y otros tipos de almacenamiento periférico en la nube](#).

 Note

Hay puertos adicionales para configurar en función del tipo de [punto de conexión de servicio](#) que use su agente.

6. (Recomendado) Para aumentar el rendimiento al realizar transferencias desde un sistema de archivos basado en la nube, amplíe los detalles avanzados y elija un valor de grupo con ubicación en el que esté ubicado su almacenamiento.
7. Elige Launch instance para lanzar tu EC2 instancia de Amazon.
8. Una vez que el estado de la instancia sea En ejecución, selecciónela.
9. Si configuró su instancia para que sea accesible desde la red Internet pública, anote la dirección IP pública de la instancia. Si no, anote la dirección IP privada.

Necesitará esta dirección IP al [activar su agente](#).

Ejemplos: implementar su EC2 agente en un Región de AWS

La siguiente guía puede ayudar con los escenarios comunes si implementa un agente de DataSync en una Región de AWS.

Temas

- [Despliegue de su agente para las transferencias entre el almacenamiento en la nube y los servicios AWS de almacenamiento](#)
- [Implementación de su agente para las transferencias entre Amazon S3 y los sistemas de AWS archivos](#)

Despliegue de su agente para las transferencias entre el almacenamiento en la nube y los servicios AWS de almacenamiento

Para transferir datos entre Cuentas de AWS sistemas de almacenamiento en la nube o entre ellos, el DataSync agente debe estar ubicado en el mismo Región de AWS Cuenta de AWS lugar donde reside el sistema de archivos de origen. Este tipo de transferencia incluye los datos siguientes:

- Transfiere entre Amazon EFS o Amazon FSx al AWS almacenamiento en un lugar diferente Cuenta de AWS.

- Transferencias desde sistemas de archivos autogestionados a servicios AWS de almacenamiento.

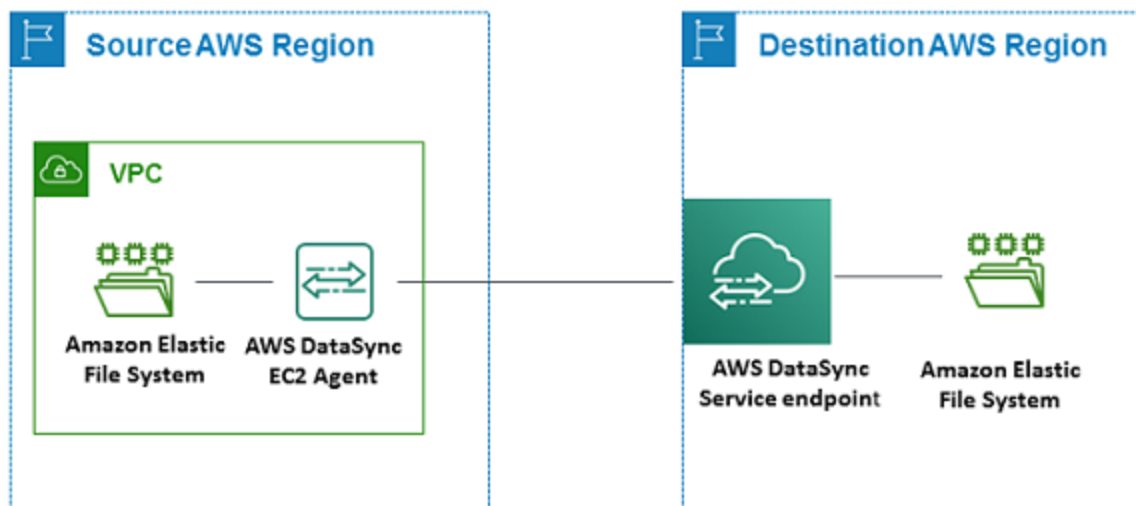
⚠ Important

Implemente su agente de forma que no requiera tráfico de red entre las zonas de disponibilidad (para evitar cargos por ese tráfico).

- Para acceder a su sistema de archivos Amazon EFS o FSx Windows File Server, implemente el agente en una zona de disponibilidad que tenga un destino de montaje para su sistema de archivos.
- En el caso de los sistemas de archivos autoadministrados, implemente el agente en la zona de disponibilidad en la que reside el sistema de archivos.

Para obtener más información sobre los precios de transferencia de datos para todos Regiones de AWS, consulta los [precios de Amazon EC2 On-Demand](#).

Por ejemplo, el siguiente diagrama muestra una vista de alto nivel de la DataSync arquitectura para transferir datos desde el Network File System (NFS) en la nube a NFS en la nube o Amazon S3.

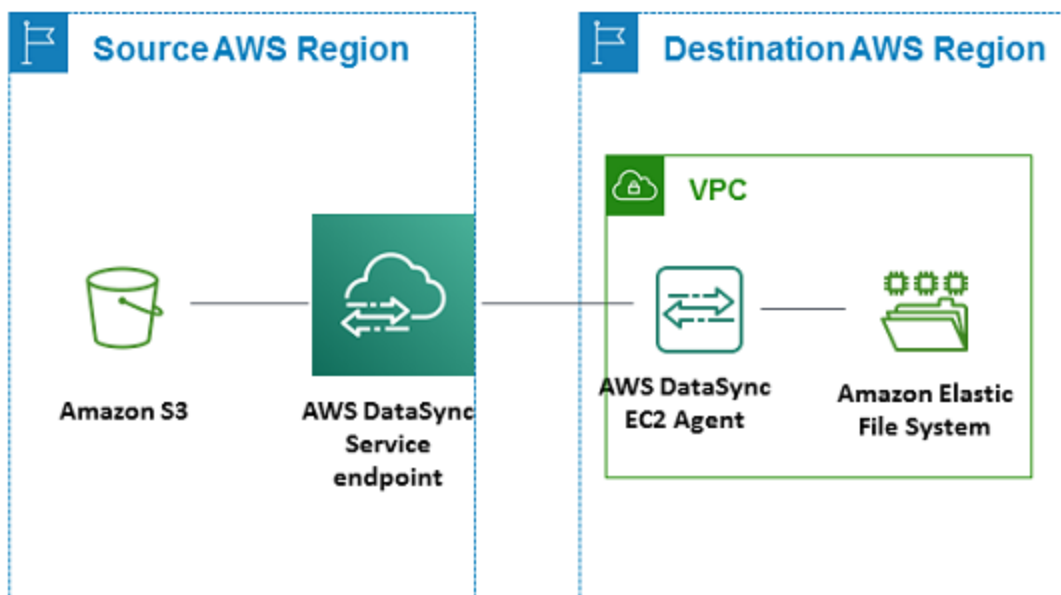


Recuerde lo siguiente al realizar transferencias entre Cuentas de AWS servicios AWS de almacenamiento:

- Al realizar transferencias entre sistemas de archivos Amazon EFS o sistemas de FSx archivos Amazon que utilizan el protocolo NFS, configure el sistema de archivos de origen como una ubicación [NFS](#).
- Al realizar transferencias entre sistemas de FSx archivos de Amazon mediante el protocolo SMB, configure el sistema de archivos de origen como una ubicación [SMB](#).

Implementación de su agente para las transferencias entre Amazon S3 y los sistemas de AWS archivos

El siguiente diagrama proporciona una vista de alto nivel de la DataSync arquitectura para transferir datos de Amazon S3 a un sistema de AWS archivos, como Amazon EFS o Amazon FSx. Puede utilizar esta arquitectura para transferir datos de uno Cuenta de AWS a otro o para transferir datos de Amazon S3 a un sistema de archivos en la nube autogestionado.



Implementación de su agente en AWS Snowball Edge

Para obtener más información e instrucciones, consulte [Crear un DataSync agente en su entorno de almacenamiento local](#) Almacenamiento compatible con Amazon S3.

Despliegue de su agente en AWS Outposts

Puedes lanzar una EC2 instancia de DataSync Amazon en tu Outpost. Para obtener más información sobre cómo lanzar una AMI en AWS Outposts, consulte [Lanzar una instancia en su Outpost](#) en la Guía del AWS Outposts usuario.

Cuando utilices el acceso DataSync a Amazon S3 en Outposts, debes lanzar el agente en una VPC a la que se le permita acceder a tu punto de acceso de Amazon S3 y activar el agente en la región principal del Outpost. El agente también debe poder enrutar al punto de conexión de Amazon S3 en Outposts del bucket. Para obtener más información sobre cómo trabajar con puntos de conexión de Amazon S3 en Outposts, consulte [Working with Amazon S3 on Outposts](#) en la Guía del usuario de Amazon S3.

Elección de un punto de conexión de servicio para su agente de AWS DataSync

Un [punto final de servicio](#) es la forma en que su AWS DataSync [agente se comunica con el DataSync](#) servicio. DataSync admite los siguientes tipos de puntos finales de servicio:

- Punto de conexión de servicio público: los datos se envían a través de Internet público.
- Punto de conexión de servicio del estándar federal de procesamiento de información (FIPS): los datos se envían a través de la Internet pública mediante procesos que cumplen con la FIPS.
- Punto de conexión de servicio de nube privada virtual (VPC): los datos se envían a través de su VPC en lugar de hacerlo a través de la red Internet pública, lo que aumenta la seguridad de los datos transferidos.

Necesita un punto de conexión de servicio para [activar el agente](#). Recuerde lo siguiente al elegir un punto de conexión de servicio:

- Un agente solo puede usar un tipo de punto de conexión. Si necesita transferir datos con distintos tipos de puntos de conexión, cree un agente para cada tipo.
- La forma en que [conecta su red de almacenamiento AWS](#) determina qué puntos de conexión de servicio puede utilizar.

Elegir un punto de conexión de servicio público

Si utiliza un punto final de servicio público, todas las comunicaciones entre su DataSync agente y el DataSync servicio se realizan a través de la Internet pública.

1. Determine el [punto final del servicio DataSync público](#) que quiere usar.
2. [Configure su red](#) para permitir el tráfico necesario para usar los puntos finales de servicio DataSync público.

Paso siguiente: [Activar su agente AWS DataSync](#)

Elegir un punto de conexión de servicio de FIPS

DataSync proporciona algunos puntos finales de servicio que cumplen con la FIPS. Para obtener más información, consulte los [puntos de conexión FIPS](#) en Referencia general de AWS.

1. Determine el [punto final del servicio DataSync FIPS](#) que desea usar.
2. [Configure su red](#) para permitir el tráfico necesario para usar los puntos finales del servicio DataSync FIPS.

Paso siguiente: [Activar su agente AWS DataSync](#)

Selección de un punto de conexión de servicio de VPC

Si utilizas un punto final de servicio de VPC, tus datos no se transfieren a través de la Internet pública. DataSync en su lugar, transfiere los datos a través de una VPC basada en el servicio Amazon VPC.

Contenido

- [Cómo trabajan DataSync los agentes con los puntos finales del servicio de VPC](#)
- [DataSync limitaciones con VPCs](#)
- [Creación de un punto final de servicio de VPC para DataSync](#)

Cómo trabajan DataSync los agentes con los puntos finales del servicio de VPC

Los puntos finales del servicio de VPC son proporcionados por AWS PrivateLink. Estos tipos de puntos finales le permiten conectarse de forma privada con Servicios de AWS su VPC. Cuando

utiliza un punto final de servicio de VPC con DataSync, toda la comunicación entre su DataSync agente y el DataSync servicio permanece en su VPC.

El punto final del servicio de VPC (junto con las [interfaces de red](#) que se DataSync crean para el tráfico de transferencia de datos) son direcciones IP privadas a las que solo se puede acceder desde la VPC. Para obtener más información, consulte [Conexión de la red para las AWS DataSync transferencias](#).

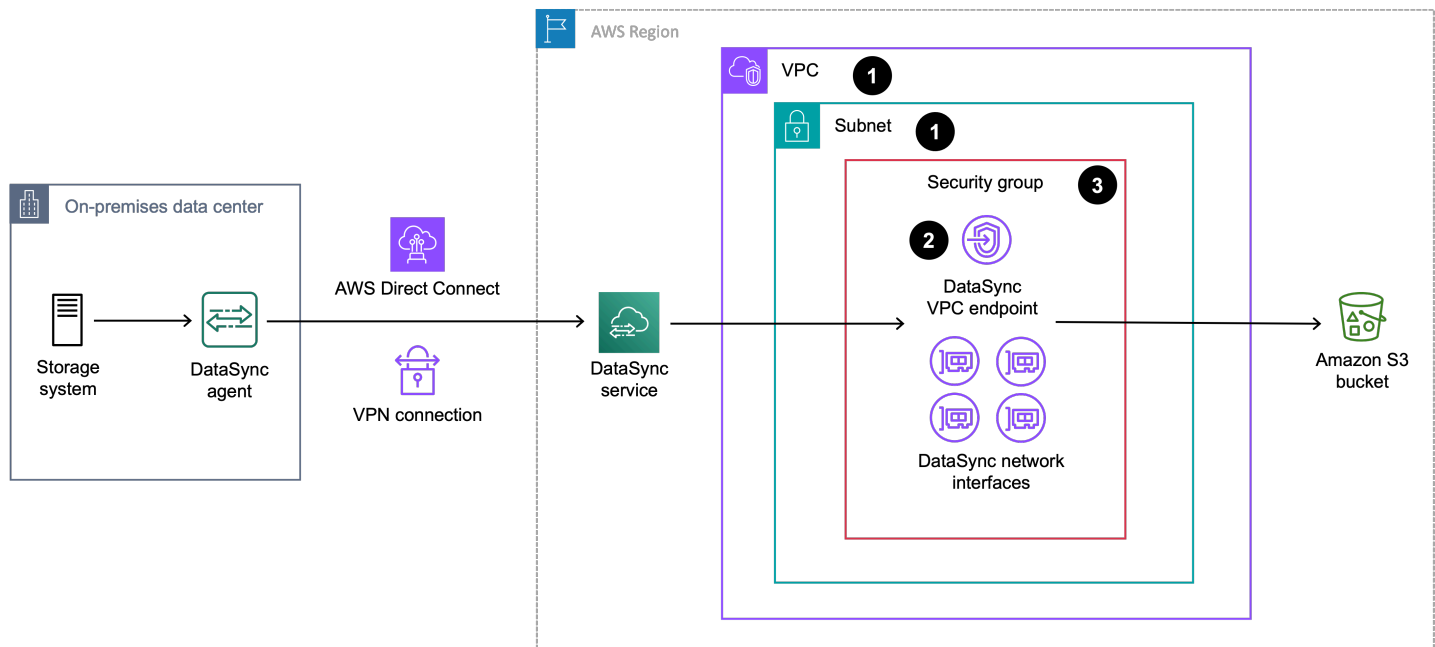
DataSync limitaciones con VPCs

- VPCs que utilice con DataSync debe tener un arrendamiento predeterminado. VPCs con un arrendamiento dedicado no son compatibles.
- DataSync no es compatible con lo [compartido VPCs](#).
- DataSync Solo son compatibles con los puntos finales del servicio de VPC. IPv4 [IPv6 y no se admiten las opciones de doble pila](#).

Creación de un punto final de servicio de VPC para DataSync

Debe crear un punto de enlace de servicio de VPC DataSync en una VPC que administre. El punto final del servicio, la VPC y el DataSync agente deben pertenecer al mismo sitio. Cuenta de AWS

En el siguiente diagrama se muestra un ejemplo del DataSync uso de un punto de enlace de servicio de VPC para la transferencia de un sistema de almacenamiento local a un bucket de Amazon S3. Las llamadas numeradas corresponden a los pasos para crear un punto de conexión de servicio de VPC.



Para crear un punto final de servicio de VPC para DataSync

1. [Cree](#) o determine una VPC y una subred en las que desee crear su punto de conexión de servicio de VPC.

Si realiza la transferencia hacia o desde un almacenamiento externo AWS, la VPC debe extenderse a ese entorno de almacenamiento (por ejemplo, su entorno de almacenamiento puede ser un centro de datos en el que se encuentra el servidor de archivos NFS local). Para ello, puede utilizar reglas de enrutamiento a través [AWS Direct Connect](#) de una VPN.

2. Cree un punto final de servicio de DataSync VPC de la siguiente manera:
 - a. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
 - b. En el panel de navegación de la izquierda, elija Puntos de conexión y, a continuación, elija Crear punto de conexión.
 - c. En Categoría de servicios, elija Servicios de AWS.
 - d. En el caso de los Servicios, busque **datasync** y elija el punto de conexión de la región en la que se encuentre (por ejemplo,). `com.amazonaws.us-east-1.datasync`
 - e. En VPC, seleccione la VPC en la que desee crear el punto de conexión de servicio de VPC.
 - f. Expanda Configuración adicional y desactive la casilla Habilitar nombre DNS privado para deshabilitar esta configuración.

Te recomendamos deshabilitar esta configuración en caso de que tengas agentes en la misma VPC que necesiten usar un punto de conexión de servicio público. Un agente no puede acceder a un [punto de conexión de servicio público](#) a través de la red cuando esta configuración está habilitada.

- g. En Subred, elija la subred en la que desea crear el punto de conexión del servicio de VPC. Tome nota del ARN de la subred (lo necesitará al activar su agente).
 - h. Elija Crear punto de conexión. Anote el ID del punto de conexión (lo necesitará al activar su agente).
3. En su VPC, configure un [grupo de seguridad](#) que permita el tráfico necesario para usar los puntos de enlace del servicio de DataSync [VPC](#). Tome nota del ARN del grupo de seguridad (lo necesitará al activar su agente).

El grupo de seguridad debe permitir que el agente se conecte con las direcciones IP privadas del punto de conexión de servicio de VPC y con [las interfaces de red](#) (que se crean al crear la tarea).

Paso siguiente: [Activar su agente AWS DataSync](#)

Activar su agente AWS DataSync

Para terminar de crear su AWS DataSync agente, debe activarlo. En este paso, se asocia el agente con el suyo Cuenta de AWS.

Note

No puedes activar un agente en más de uno Cuenta de AWS y Región de AWS a la vez.

Requisitos previos

Para activar a su DataSync agente, asegúrese de disponer de la siguiente información:

- El [punto final del DataSync servicio](#) con el que está activando su agente.

Si está utilizando un punto de conexión de VPC, necesita estos detalles:

- ID del punto de conexión de servicio de VPC

- Subred en la que se encuentra el punto de conexión de VPC.
- El grupo de seguridad que permite el tráfico necesario para usar los puntos finales del [servicio de DataSync VPC](#).
- Dirección IP o nombre de dominio de su agente.

La forma de encontrarlo depende del tipo de agente que [despliegue](#). Por ejemplo, si tu agente es una EC2 instancia de Amazon, puedes encontrar su dirección IP en la página de la instancia en la EC2 consola de Amazon.

Obtención de una clave de activación

Puedes obtener una clave de activación para tu DataSync agente desplegado de diferentes maneras. Algunas opciones requieren acceso al agente en el puerto 80 (HTTP). Si utiliza una de estas opciones, DataSync cierra el puerto una vez que active el agente.

Note

Las claves de activación del agente caducan en 30 minutos si no se utilizan.

DataSync console

Al [activar el agente en la DataSync consola](#), DataSync puede obtener la clave de activación automáticamente mediante la opción Obtener automáticamente la clave de activación del agente.

Para usar esta opción, su navegador debe poder comunicarse con su agente en el puerto 80.

Agent local console

A diferencia de las otras opciones para obtener una clave de activación, esta opción no requiere que se pueda acceder a su agente en el puerto 80.

1. Inicie sesión en la [consola local](#) de su máquina virtual (VM) de agente o EC2 instancia de Amazon.
2. En el menú principal AWS DataSync Activación - Configuración, introduzca **0** para obtener una clave de activación.
3. Introduzca el nombre en el Región de AWS que va a activar su agente.
4. Introduzca el tipo de punto de conexión de servicio que utiliza su agente.

5. Copie la clave de activación que aparece.

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

Debe especificar esta clave al [activar el agente](#).

CLI

Con las herramientas estándar de Unix, puede ejecutar una `curl` solicitud a la dirección IP de su agente para obtener su clave de activación.

Para usar esta opción, su cliente debe poder comunicarse con su agente en el puerto 80. Puede ejecutar el siguiente comando para realizar la comprobación:

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

Una vez que confirme que puede comunicarse con el agente, ejecute uno de los siguientes comandos en función del tipo de punto de conexión de servicio que esté utilizando:

- Puntos de conexión de servicio público:

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

- Puntos de conexión de servicio FIPS:

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

- Puntos de conexión de servicio de VPC:

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

Para encontrarlo *vpc-endpoint-ip-address*, abra la [consola de Amazon VPC](#), elija Endpoints y seleccione el punto de enlace del servicio de VPC DataSync. En la pestaña Subredes, busca la dirección IP de la subred del [punto de conexión de servicio de VPC](#). Esta es la dirección IP del punto de conexión.

Este comando devuelve una clave de activación. Por ejemplo:

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

Debe especificar esta clave al [activar el agente](#).

Activación de su agente de

Dispone de varias opciones para activar su agente. DataSync Una vez activado, AWS [administra el agente por usted](#).

DataSync console

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, elija Agentes y luego, Crear agente.
3. En la sección Punto de conexión de servicio, haga lo siguiente para especificar el punto de conexión de servicio para su agente:
 - Para un punto final de servicio público, seleccione Puntos finales de servicio público en ***your current Región de AWS***.
 - Para un punto final del servicio FIPS, seleccione los puntos finales del servicio FIPS en ***your current Región de AWS***.
 - Para un punto de conexión de servicio de VPC, haga lo siguiente:
 - Elija los puntos de conexión de VPC utilizando AWS PrivateLink.
 - En Punto de conexión de VPC, elija el punto de conexión de servicio de VPC que quiera que use el agente.
 - En Subred, elija la subred en la que se encuentra el punto de conexión de VPC.
 - En Grupo de seguridad, elija el grupo de seguridad que permita el tráfico necesario para usar los puntos finales del [servicio de DataSync VPC](#).
4. En la sección Clave de activación, realice una de las siguientes acciones para especificar la clave de activación de su agente:
 - Seleccione Obtener automáticamente la clave de activación de su agente DataSync para obtener la clave por usted.
 - En Dirección del agente, introduzca la dirección IP o el nombre de dominio.
 - Seleccione Obtener clave.

Si se produce un error en la activación, [compruebe la configuración de la red](#) en función del tipo de punto de conexión de servicio que utilice.

- Elija Introducir manualmente la clave de activación del agente si no desea una conexión entre el navegador y el agente.
 - [Obtenga la clave](#) desde la consola local del agente o mediante un `curl` comando.
 - De vuelta a la DataSync consola, introduzca la clave en el campo Clave de activación.
5. (Recomendado) Para el nombre del agente, asígnele un nombre que pueda recordar.
 6. (Opcional) En Etiquetas, introduzca los valores de los campos Clave y Valor para etiquetar su agente.

Las etiquetas le ayudan a administrar, filtrar y buscar sus recursos de AWS .

7. Elija Crear agente.
8. En la página Agentes, compruebe que el agente utiliza el tipo de punto de conexión de servicio.

 Note

En este punto, es posible que observe que su agente está desconectado. Esto ocurre poco después de la activación del agente.

AWS CLI

1. Cuando [obtenga la clave de activación](#), copia uno de los siguientes `create-agent` comandos en función del tipo de punto de conexión de servicio que utilice:

- Punto de conexión de servicio público o FIPS:

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

- Punto de conexión de servicio de VPC:

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



```
--vpc-endpoint-id vpc-endpoint-id \  
--subnet-arns subnet-arn \  
--security-group-arns security-group-arn
```

2. Para `--activation-key`, especifique la [clave de activación del agente](#).
3. (Recomendado) Para `--agent-name`, especifique un nombre para su agente que pueda recordar.
4. Si está utilizando un punto de conexión de VPC, especifique las siguientes opciones:
 - Para `--vpc-endpoint-id`, especifique el ID del punto de conexión de servicio de VPC que está utilizando.
 - Para `--subnet-arns`, especifique el ARN de la subred en la que se encuentra el punto de conexión de servicio de VPC.
 - Para `--security-group-arns`, especifique el ARN del grupo de seguridad que permite el tráfico necesario para usar los puntos finales del servicio de DataSync [VPC](#).
5. Ejecute el comando `create-agent`.

Obtendrá una respuesta con el ARN del agente que acaba de activar. Por ejemplo:

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

6. Compruebe que su agente esté activado ejecutando el `list-agents` comando:

```
aws datasync list-agents
```

Note

En este punto, es posible que observe que su agente Status está OFFLINE. Esto ocurre poco después de la activación del agente.

DataSync API

Una vez que [obtenga la clave de activación](#), active el agente mediante la operación. [CreateAgent](#)

 Note

Cuando haya terminado, es posible que observe que su agente está desconectado. Esto ocurre poco después de la activación del agente.

Pasos a seguir a continuación

- [Verifique la conexión de su agente](#) con el sistema de almacenamiento y el DataSync servicio.
- [Si tiene problemas al intentar activar su agente, solicite ayuda para solucionar el problema.](#)
- Cree la DataSync ubicación que desee usar con su agente. Puede ser una ubicación [local u otra ubicación](#) en la nube.

Verificación de las conexiones de red de su agente

Una vez activado el AWS DataSync agente, asegúrese de que el agente tenga conectividad de red con el sistema de almacenamiento y el DataSync servicio.

Acceso a la consola local de su agente

La forma de acceder a la consola local de su agente depende del tipo de agente que esté utilizando.

Acceso a la consola local (VMware ESXiLinux KVM o Microsoft Hyper-V)

Por motivos de seguridad, no puede conectarse remotamente a la consola local de la máquina virtual (VM) del DataSync agente.

- Si es la primera vez que utiliza la consola local, inicie sesión en la máquina virtual con las credenciales predeterminadas. El nombre de usuario y la contraseña predeterminados son **admin** y **password**, respectivamente.

 Note

Le recomendamos que cambie la contraseña predeterminada. Para ello, introduzca **5** (o **6** para VMware VMs) en el menú principal de la consola y ejecute el `passwd` comando para cambiar la contraseña.

Acceso a la consola local (Amazon EC2)

Para conectarte a la consola local de un EC2 agente de Amazon, debes usar SSH.

Antes de empezar: asegúrate de que el grupo de seguridad de la EC2 instancia permita el acceso mediante SSH (puerto TCP 22).

1. Abra un terminal y copie el siguiente comando ssh:

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

- Para */path/key-pair-name* ello, especifique la ruta y el nombre de archivo (.pem) de la clave privada necesaria para conectarse a la instancia.
 - En *instance-user-name*, especifique admin.
 - Para *instance-public-ip-address*, especifica la dirección IP pública de la instancia.
2. Ejecute el comando ssh para conectarse a la instancia.

Una vez conectado, se muestra el menú principal de la consola local del agente.

Verificación de la conexión de su agente con su sistema de Imacenamiento

Compruebe si su DataSync agente puede conectarse a su sistema de almacenamiento. Para obtener más información, consulte [1. Conexión de red entre el sistema de almacenamiento y el agente](#).

1. [Acceda a la consola local de su agente](#).
2. En el menú principal AWS DataSync Activación - Configuración, introduzca **3**.
3. Introduzca una de las siguientes opciones:
 - a. Introduzca **1** para probar una conexión a un servidor NFS.
 - b. Introduzca **2** para probar una conexión a un servidor SMB.
 - c. Introduzca **3** para probar una conexión a un servidor de almacenamiento de objetos.
 - d. Introduzca **4** para probar una conexión HDFS.
 - e. Introduzca **5** para probar una conexión Microsoft Azure Blob Storage.
4. Introduzca la dirección IP o el nombre de dominio del servidor de almacenamiento.

Recuerde lo siguiente al introducir la dirección IP o el nombre de dominio:

- No incluya un protocolo. Por ejemplo, introduzca **mystorage.com** en lugar de **https://mystorage.com**.
 - En el caso de HDFS, introduzca la dirección IP o el nombre de dominio del clúster de DataNode Hadoop NameNode o del clúster.
5. Si se le solicita, introduzca el puerto TCP para conectarse al servidor de almacenamiento (por ejemplo, **443**).

Verá si la prueba de conectividad tiene el estado APROBADO o NO_APROBADO.

Verificar la conexión de su agente al servicio DataSync

Comprueba si tu DataSync agente puede conectarse al DataSync servicio. Para obtener más información, consulte [2. Conexión de red entre el agente y DataSync el servicio](#).

1. [Acceda a la consola local de su agente](#).
2. En el menú principal AWS DataSync Activación y configuración, introduzca **2** para empezar a probar la conectividad de la red.

Si el agente está activado, se puede iniciar la opción Probar la conectividad de la red sin necesidad de que el usuario intervenga más, ya que la región y el tipo de punto de conexión se toman de la información del agente activado.

3. Introduzca el tipo de punto final de DataSync servicio que utiliza su agente:
 - a. Para los puntos finales de servicio público, introduzca **1** y Región de AWS dónde está activado su agente.
 - b. Para los puntos de conexión de servicio FIPS, introduzca **2** y la región en la que está activado su agente.
 - c. Para los puntos de conexión de servicio de VPC, introduzca **3**.

Aparece un mensaje APROBADO o FALLIDO.

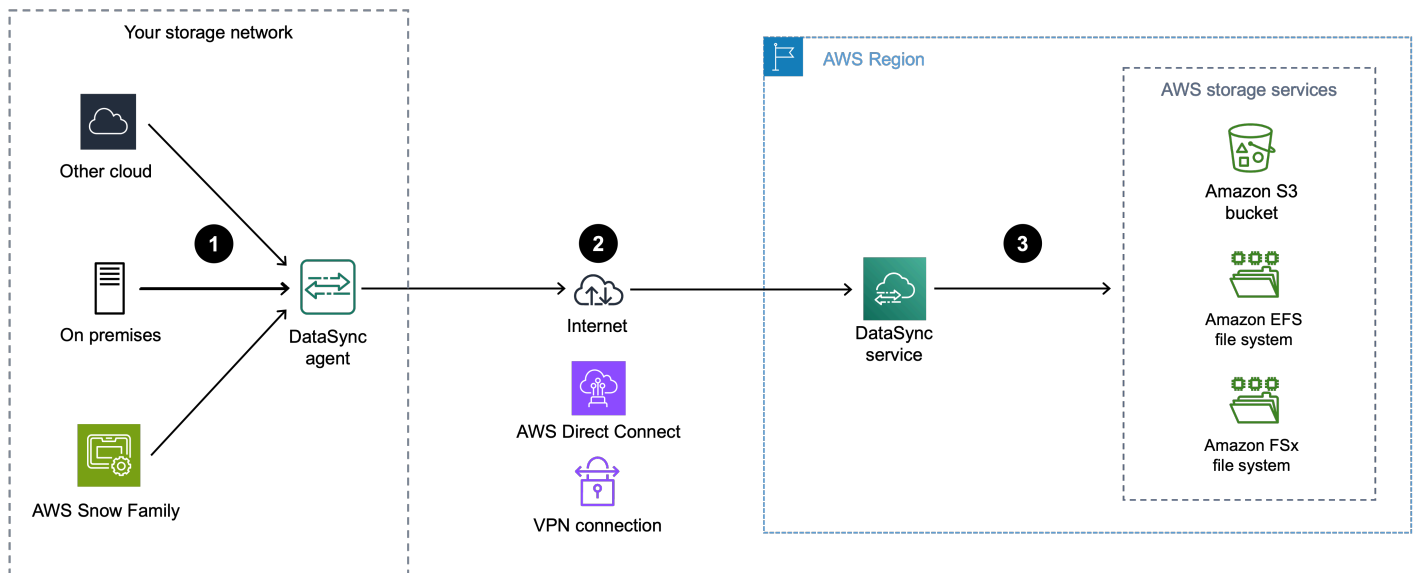
4. Si aparece un mensaje de error, compruebe la configuración de la red. Para obtener más información, consulte [AWS DataSync requisitos de red](#).

Pasos a seguir a continuación

Cree la DataSync ubicación que desee usar con su agente. Puede ser una ubicación [local u otra ubicación](#) en la nube.

Conexión de la red para las AWS DataSync transferencias

Si [necesita un AWS DataSync agente](#), debe establecer varias conexiones de red para la transferencia de datos. El siguiente diagrama muestra las tres conexiones de red en una DataSync transferencia desde un sistema de almacenamiento (que puede estar en las instalaciones, en otra nube o en la periferia) a un servicio AWS de almacenamiento.



1. Conexión de red entre el sistema de almacenamiento y el agente

DataSync El agente se conecta a un sistema de almacenamiento local, a otro sistema de almacenamiento en la nube o periférico. Para obtener más información, consulte [Requisitos de red para el almacenamiento autoadministrado en las instalaciones y otros tipos de almacenamiento periférico en la nube](#).

2. Conexión de red entre el agente y DataSync el servicio

La conexión de su agente con el DataSync servicio tiene algunos aspectos. En primer lugar, debe conectar su red de almacenamiento a AWS. En segundo lugar, su agente necesita un punto final de servicio con el que comunicarse DataSync.

Contenido

- [Conectar la red de almacenamiento a AWS](#)
- [Selección de un punto de conexión de servicio](#)

Conectar la red de almacenamiento a AWS

Cuando DataSync lo utilices, ten en cuenta las siguientes opciones para conectar tu red de almacenamiento a AWS:

- AWS Direct Connect- Con [Direct Connect](#), puede crear una conexión dedicada entre su red de almacenamiento y AWS. Desde un DataSync punto de vista, esto le permite:
 - Transfiera datos a través de una ruta privada a su nube privada virtual (VPC), lo que evita el enrutamiento a través del Internet público.
 - Obtenga una conexión más predecible que con una red privada virtual (VPN) para conectar su red de almacenamiento AWS (especialmente si su agente es una EC2 instancia de Amazon).
 - Utilice cualquier tipo de punto final de DataSync servicio, incluidos los puntos finales [públicos](#), del [Estándar Federal de Procesamiento de Información \(FIPS\)](#) o de [VPC](#).

Para obtener más información, consulte [DataSync ejemplos de arquitectura y enrutamiento con AWS Direct Connect](#).

- VPN: puede conectar su red de almacenamiento AWS mediante una VPN (por ejemplo). [AWS Site-to-Site VPN](#)
- Internet pública: puede conectar su red de almacenamiento directamente a DataSync través de Internet mediante un punto final de servicio [público](#) o [FIPS](#).

Selección de un punto de conexión de servicio

El agente utiliza un punto final de servicio para comunicarse con DataSync él. Para obtener más información, consulte [Elección de un punto de conexión de servicio para su agente de AWS DataSync](#).

3. Conexión de red entre el DataSync servicio y el servicio AWS de almacenamiento

Para conectarse DataSync a un servicio AWS de almacenamiento, solo tiene que asegurarse de que el DataSync servicio pueda acceder a su bucket o sistema de archivos S3. Para obtener más información, consulte [Requisitos de red para los servicios de almacenamiento de AWS](#).

Establezca redes cuando no necesite un DataSync agente

En el caso de las transferencias que [no requieren un DataSync agente](#), solo tienes que asegurarte de que el DataSync servicio pueda acceder a los sistemas de AWS almacenamiento entre los que realizas la transferencia. Para obtener más información, consulte [Requisitos de red para los servicios de almacenamiento de AWS](#).

Cómo y dónde fluye DataSync el tráfico a través de la red

DataSync tiene tráfico en el plano de datos y en el plano de control. Si desea separar el DataSync tráfico, es importante saber cómo fluye cada uno de ellos a través de la red.

- Tráfico del plano de datos: incluye los datos de archivos u objetos que se mueven entre las ubicaciones de almacenamiento. En la mayoría de los casos, el tráfico del plano de datos se enruta a través de [interfaces de red](#) que se generan y administran DataSync automáticamente al crear una tarea. El lugar donde se crean estas interfaces de red depende del tipo de servicio de AWS almacenamiento desde o hacia el que se transfiera y del punto final del servicio que utilice el DataSync agente.
- Tráfico en el plano de control: incluye actividades de administración de sus DataSync recursos. Este tráfico pasa a través del punto de conexión de servicio que utiliza el agente.

Seguridad de red para DataSync

Para obtener información sobre cómo se protegen los datos de almacenamiento (incluidos los metadatos) durante una transferencia, consulte [AWS DataSync cifrado en tránsito](#)

AWS DataSync requisitos de red

La configuración de la red es un paso importante para configurar AWS DataSync. La configuración de la red depende de varios factores, como el tipo de sistemas de almacenamiento con los que va a utilizar. También se basa en el tipo de punto final del DataSync servicio que vaya a utilizar.

Requisitos de red para el almacenamiento autoadministrado en las instalaciones y otros tipos de almacenamiento periférico en la nube

Los siguientes requisitos de red pueden aplicarse a los sistemas de almacenamiento en las instalaciones, autoadministrados, otros sistemas en la nube y en la periferia. Por lo general, se trata

de sistemas de almacenamiento que usted administra o que podría administrar otro proveedor de nube.

 Note

En función de la red, es posible que tengas que permitir el tráfico en puertos distintos de los que se indican aquí para que tu DataSync agente se conecte al almacenamiento.

De	Para	Protocolo	Puerto	Cómo lo usa DataSync
DataSync agente	Servidor de archivos NFS	TCP	2049 (para las versiones 4.1 y 4.0 de NFS) 111 y 2049 (para la versión 3.x de NFS)	Monta el servidor de archivos NFS. DataSync es compatible con las versiones 3.x, 4.0 y 4.1 de NFS.
DataSync agente	Servidor de archivos SMB	TCP	139 o 445	Monta el servidor de archivos SMB. DataSync es compatible con las versiones 1.0 y posteriores para SMB. Por motivos de seguridad, recomendamos utilizar la versión 3.0.2 o posterior para SMB. Las versiones anteriores, como SMB 1.0, contienen vulnerabilidades de seguridad conocidas que los atacantes

De	Para	Protocolo	Puerto	Cómo lo usa DataSync
				pueden aprovechar para comprometer sus datos.

De	Para	Protocolo	Puerto	Cómo lo usa DataSync
DataSync agente	Almacenamiento de objetos	TCP	443 (HTTPS) o 80 (HTTP)	Accede a tu almacenamiento de objetos compatible con Amazon S3 de forma local o en otras nubes.

 Note

En función del almacenamiento de objetos es posible que necesites permitir el tráfico en puertos HTTPS y HTTP no estándar (como 8443 o 8080).

De	Para	Protocolo	Puerto	Cómo lo usa DataSync
DataSync agente	Clúster de Hadoop	TCP	NameNode puerto (el predeterminado es 8020) En la mayoría de los clústeres, puede encontrar este número de puerto en el archivo <code>core-site.xml</code> situado en la propiedad <code>fs.default</code> o <code>fs.default.name</code> (según la distribución de Hadoop).	Accede al clúster NameNodes de Hadoop. Especifique el puerto utilizado al crear una ubicación HDFS.

De	Para	Protocolo	Puerto	Cómo lo usa DataSync
DataSync agente	Clúster de Hadoop	TCP	DataNode puerto (el predeterminado es 50010) En la mayoría de los clústeres, puede encontrar este número de puerto en el archivo <code>hdfs-site.xml</code> situado en la propiedad <code>dfs.datanode.address</code>.	Accede al clúster DataNodes de Hadoop. El DataSync agente determina automáticamente el puerto que se va a utilizar.
DataSync agente	Hadoop Key Management Server (KMS)	TCP	Puerto KMS (el predeterminado es 9600)	Accede al KMS de su clúster de Hadoop.

De	Para	Protocolo	Puerto	Cómo lo usa DataSync
DataSync agente	Servidor del centro de distribución de claves (KDC) Kerberos	TCP	Puerto KDC (el predeterminado es 88)	Se autentica con el dominio Kerberos. Este puerto solo se usa con ubicaciones HDFS y SMB que utilizan la autenticación Kerberos.
DataSync agente	Interfaz de administración del sistema de almacenamiento	TCP	Depende de su red	Se conecta a su sistema de almacenamiento.

Requisitos de red para los servicios de almacenamiento de AWS

Los puertos de red necesarios DataSync para conectarse a un servicio AWS de almacenamiento durante una transferencia varían.

De	Para	Protocolo	Puerto
DataSync servicio	Amazon EFS	TCP	2049
DataSync servicio	FSx para Windows File Server	Consulte el control de acceso al sistema de archivos FSx para Windows File Server .	
DataSync servicio	FSx para Lustre	Consulte el control de acceso al sistema de archivos FSx para Lustre .	
DataSync servicio	FSx para OpenZFS	Consulte el control de acceso al sistema de archivos FSx para OpenZFS .	
DataSync servicio	FSx para ONTAP	TCP	111, 635 y 2049 (NFS) 445 (SMB)

De	Para	Protocolo	Puerto
DataSync servicio	Amazon S3	N/A (DataSync se conecta a los buckets de S3 en su nombre)	

Requisitos de red para puntos de conexión de servicio públicos o FIPS

Su DataSync agente requiere el siguiente acceso a la red cuando utiliza puntos finales de servicio públicos o FIPS. Si utiliza un firewall o un enrutador para filtrar o limitar el tráfico de red, debe configurarlos de forma que estos puntos de conexión tengan permiso.

De	Para	Protocolo	Puerto	Modo de uso	Puntos de conexión a los que se ha accedido
El navegador web	DataSync agente	TCP	80 (HTTP)	Permite que su navegador obtenga la clave de activación del DataSync agente. Una vez activado, DataSync cierra el puerto 80 del agente. El agente no necesita que el puerto 80 esté accesible públicamente. El nivel de acceso exigido al puerto 80 depende de la	N/A

De	Para	Protocolo	Puerto	Modo de uso	Puntos de conexión a los que se ha accedido
				configuración de la red. Note Puede obtener la clave de activación sin necesidad de una conexión entre el navegador y el agente. Para obtener más información, consulte Obtención de una clave de activación.	

De	Para	Protocolo	Puerto	Modo de uso	Puntos de conexión a los que se ha accedido
DataSync agente	Amazon CloudFront	TCP	443 (HTTP)	Ayuda a iniciar el DataSync agente antes de la activación.	Regiones de AWS: - d3dvvaliwoko8h.cloudfront.net AWS GovCloud (US) Regiones: - s3.us-gov-west-1.amazonaws.com/fmrse-ndpoints-endpoints-bucket-go4p5gpna6sk
DataSync agente	AWS	TCP	443 (HTTP)	Activa tu DataSync agente y lo asocia a tu Cuenta de AWS. Puede bloquear los puntos de conexión públicos después de la activación.	Ahí activation-region es Región de AWS donde activas a tu DataSync agente. Activar los puntos de conexión públicos: - activation.datasyncc.activation-region.amazonaws.com Activar los puntos de conexión de FIPS: - activation.datasyncc-fips.activation-region.amazonaws.com

De	Para	Protocolo	Puerto	Modo de uso	Puntos de conexión a los que se ha accedido
DataSync agente	AWS	TCP	443 (HTTP)	Permite la comunicación entre el DataSync agente y el punto final DataSync del servicio. Para obtener información, consulte Elección de un punto de conexión de servicio para su agente de AWS DataSync.	Ahí <i>activation-region</i> es Región de AWS donde se activa el DataSync agente. En función del uso que utilice DataSync , es posible que no necesite permitir el acceso a todos los terminales que se indican aquí. DataSync puntos finales del plano de control: • Punto de conexión público: <code>cp.datasync.<i>activation-region</i>.amazonaws.com</code> • Punto de conexión de FIPS: <code>cp.datasync-fips.<i>activation-region</i>.amazonaws.com</code> DataSync punto final del plano de datos (solo para tareas de transferencia): • <code><i>your-task-id</i>.datasync-dp.<i>activation-region</i>.amazonaws.com</code>

De	Para	Protocolo	Puerto	Modo de uso	Puntos de conexión a los que se ha accedido
Su cliente	AWS	TCP	443 (HTTP)	Le permite realizar solicitudes a DataSync la API.	Aquí <i>activation-region</i> es Región de AWS donde activas tu DataSync agente. Punto de conexión público: • <code>datasync.<i>activation-region</i>.amazonaws.com</code> Punto de conexión FIPS: • <code>datasync-fips.<i>activation-region</i>.amazonaws.com</code>
DataSync agente	AWS	TCP	443 (HTTP)	Permite al DataSync agente recibir actualizaciones de AWS. Para obtener más información, consulte Administrar a tu AWS DataSync agente .	Aquí <i>activation-region</i> es Región de AWS donde activas a tu DataSync agente. • <code>amazonlinux.default.amazonaws.com</code> • <code>cdn.amazonlinux.com</code> • <code>amazonlinux-2-repos-<i>activation-region</i>.s3.dualstack.<i>activation-region</i>.amazonaws.com</code> • <code>amazonlinux-2-repos-<i>activation-region</i>.s3.<i>activation-region</i>.amazonaws.com</code> • <code>*.s3.<i>activation-region</i>.amazonaws.com</code>

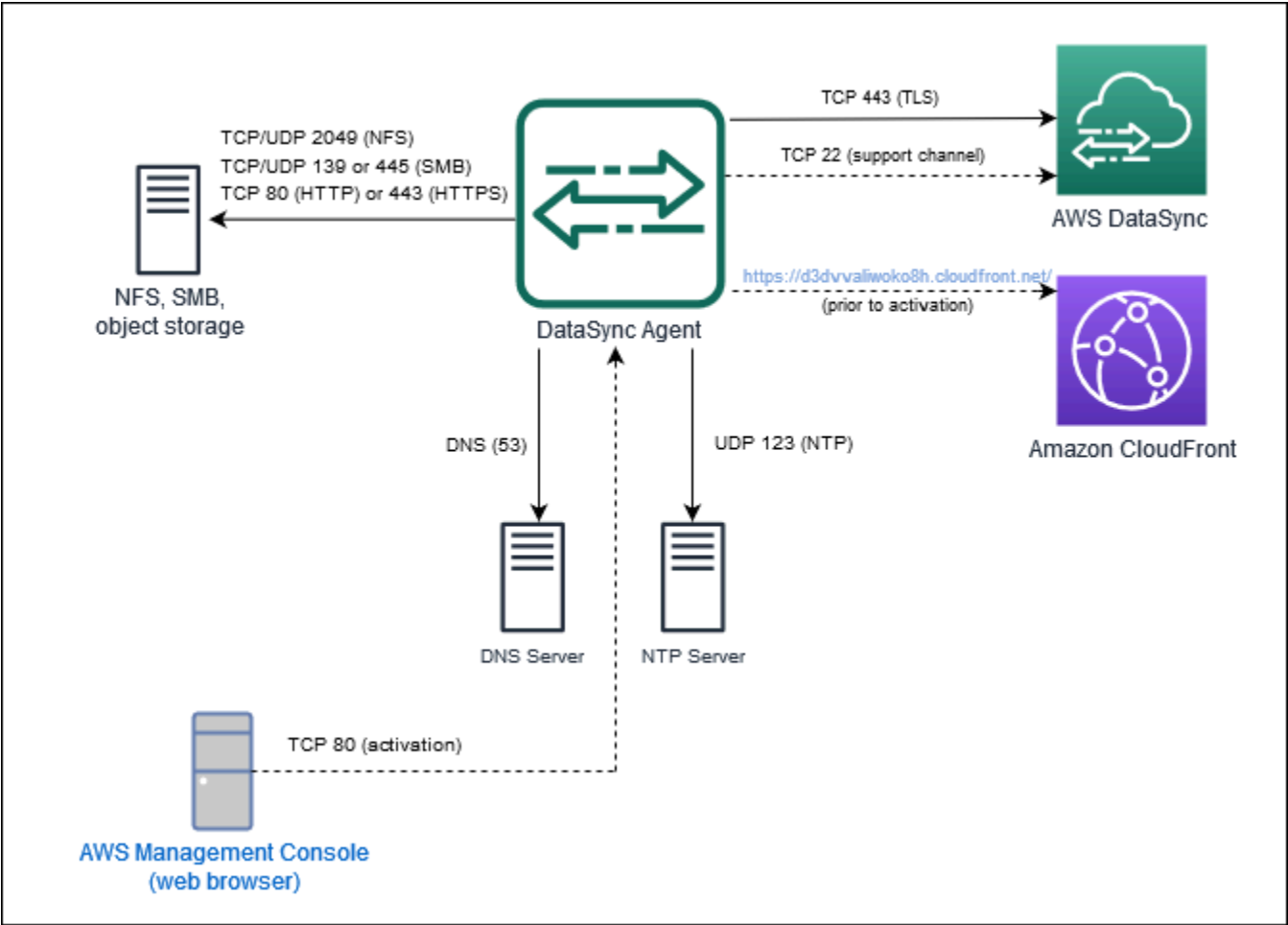
De	Para	Protocolo	Puerto	Modo de uso	Puntos de conexión a los que se ha accedido
DataSync agente	Servidor DNS (Domain Name Service)	TCP/UDP	53 (DNS)	Permite la comunicación entre el DataSync agente y el servidor DNS.	N/A
DataSync agente	AWS	TCP	22 (canal de soporte)	Permite acceder AWS Support a su DataSync agente para ayudarle a solucionar problemas. No necesita que este puerto esté abierto para un funcionamiento normal.	AWS Support canal: • 54.201.223.107

De	Para	Protocolo	Puerto	Modo de uso	Puntos de conexión a los que se ha accedido
DataSync agente	Servidor de Network Time Protocol (NTP)	UDP	123 (NTP)	Permite a los sistemas locales sincronizar la hora de la MV con la hora del host.	NTP: • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org

 **Note**

Para cambiar la configuración NTP predeterminada del agente de la máquina virtual y utilizar otro servidor NTP a través de la consola local, consulte [Sincronizar la hora de su agente VMware](#).

El siguiente diagrama muestra los puertos necesarios DataSync cuando se utilizan puntos finales de servicio público o FIPS.



Requisitos de red para puntos de conexión de servicio de VPC

Un punto final de nube privada virtual (VPC) proporciona una conexión privada entre su agente y AWS no cruza Internet ni utiliza direcciones IP públicas. Esto también ayuda a evitar que los paquetes entren o salgan de la red. Para obtener más información, consulte [Selección de un punto de conexión de servicio de VPC](#).

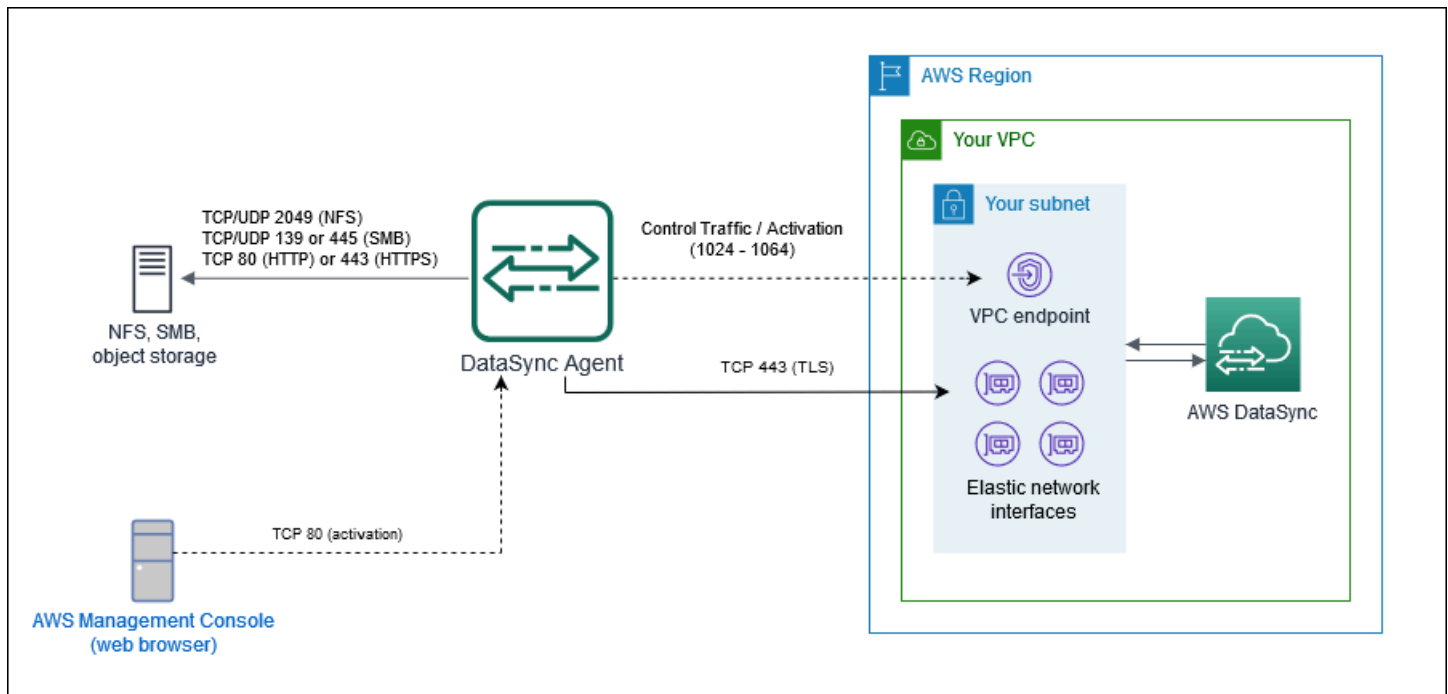
DataSync requiere los siguientes puertos para que su agente utilice un punto final de servicio de VPC.

De	Para	Protocolo	Puerto	Modo de uso
El navegador web	¿Tu agente DataSync	TCP	80 (HTTP)	Permite que su navegador obtenga la clave de activación del agente. Una vez activado,

De	Para	Protocolo	Puerto	Modo de uso
				DataSync cierra el puerto 80 del agente. El agente no necesita que el puerto 80 esté accesible públicamente. El nivel de acceso exigido al puerto 80 depende de la configuración de la red. Note Puede obtener la clave de activación sin necesidad de una conexión entre el navegador y el agente. Para obtener más información, consulte Obtención de una clave de activación.

De	Para	Protocolo	Puerto	Modo de uso
DataSync agente	Su punto final DataSync de servicio de VPC Para encontrar la dirección IP del punto de conexión, abra la consola de Amazon VPC, elija Endpoints y seleccione el punto de enlace del servicio de VPC DataSync . En la pestaña Subredes, busca la dirección IP de la subred del punto de conexión de servicio de VPC. Esta es la dirección IP del punto de conexión.	TCP	1024–1064	Para el tráfico del plano de control .
DataSync agente	Las interfaces de red de su DataSync tarea Para encontrar las direcciones IP de estas interfaces, consulte Visualización de las interfaces de red.	TCP	443 (HTTPS)	Para el tráfico del plano de datos .
DataSync agente	Su punto final DataSync de servicio de VPC	TCP	22 (canal de soporte)	Para permitir AWS Support el acceso a su DataSync agente para solucionar problemas. No necesita que este puerto esté abierto para un funcionamiento normal.

En el siguiente diagrama, se muestran los puertos que se requieren DataSync cuando se utilizan los puntos finales del servicio de VPC.



Interfaces de red para transferencias de AWS DataSync

Para cada tarea que cree, genera y administra AWS DataSync automáticamente las [interfaces de red](#) para el tráfico de transferencia de datos. El número de interfaces de red que DataSync cree y dónde se crean depende de los siguientes detalles sobre la tarea de transferencia:

- Si su tarea [requiere un DataSync agente](#).
- Sus ubicaciones de origen y destino (desde y hacia las que copia los datos).
- El tipo de punto de conexión de servicio que utiliza el agente.

Cada interfaz de red utiliza una única dirección IP en la subred (cuantas más interfaces de red haya, más direcciones IP necesitará). Utilice las siguientes tablas para garantizar que la subred tiene suficientes direcciones IP para la tarea.

Interfaces de red para transferencias con agentes

En general, se necesita un DataSync agente para copiar datos entre un servicio de AWS almacenamiento y un sistema de almacenamiento que no lo sea AWS.

Ubicación	Interfaces de red creadas de forma predeterminada	Dónde se crean las interfaces de red cuando se utiliza un punto de conexión público o FIPS	Dónde se crean las interfaces de red cuando se utiliza un punto de conexión privado (VPC)
Amazon S3	4	N/A ¹	La subred que especifique al activar el DataSync agente.
Amazon EFS	4	La subred que especifique al crear la ubicación de Amazon EFS.	
Servidor FSx de archivos Amazon para Windows	4	La misma subred que el servidor de archivos preferido del sistema de archivos.	
Amazon FSx para Lustre	4	La misma subred que el sistema de archivos.	
Amazon FSx para OpenZFS	4	La misma subred que el sistema de archivos.	
Amazon FSx para NetApp ONTAP	4	La misma subred que el sistema de archivos.	

¹ No se necesitan interfaces de red porque el DataSync servicio se comunica directamente con el bucket S3.

Interfaces de red para transferencias sin agentes

No necesita un DataSync agente para copiar datos entre ellas Servicios de AWS.

La cantidad total de interfaces de red depende de las DataSync ubicaciones de la transferencia. Por ejemplo, la transferencia entre Amazon EFS y FSx los sistemas de archivos Lustre requiere cuatro interfaces de red. Mientras tanto, la transferencia entre FSx un servidor de archivos de Windows y un bucket de S3 requiere dos interfaces de red.

Ubicación	Interfaces de red creadas de forma predeterminada	Dónde se crean las interfaces de red
Amazon S3	N/A ¹	N/A ¹
Amazon EFS	2	La subred que especifique al crear la ubicación de Amazon EFS.
FSx para Windows File Server	2	La misma subred que el servidor de archivos preferido para el sistema de archivos.
FSx para Lustre	2	La misma subred que el sistema de archivos.
FSx para OpenZFS	2	La misma subred que el sistema de archivos.
FSx para ONTAP	2	La misma subred que el sistema de archivos.

¹ No se necesitan interfaces de red porque el DataSync servicio se comunica directamente con el bucket S3.

Visualización de las interfaces de red

Para ver las interfaces de red asignadas a la tarea de DataSync transferencia, realice una de las siguientes acciones:

- Utilice la operación [DescribeTask](#). La operación devuelve SourceNetworkInterfaceArns y DestinationNetworkInterfaceArns con respuestas parecidas a las siguientes:

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

En este ejemplo, el ID de la interfaz de red es eni-f012345678abcdef0.

- En la EC2 consola de Amazon, busca tu ID de tarea (por ejemplo task-f012345678abcdef0) para encontrar sus interfaces de red.

DataSync ejemplos de arquitectura y enrutamiento con AWS Direct Connect

Tenga en cuenta las siguientes arquitecturas de red cuando utilice [AWS Direct Connect](#) con sus transferencias de AWS DataSync .

Tip

Si su red utiliza una puerta de enlace de tránsito, le recomendamos separar la ruta lógica de la DataSync transferencia para optimizar los costes (especialmente si va a migrar una gran cantidad de datos).

Por ejemplo, si la utiliza [AWS Transit Gateway](#) para el tráfico normal entre las redes locales y las nubes privadas virtuales (VPCs), puede configurar la red de modo que el DataSync tráfico evite la pasarela de tránsito y sus gastos de procesamiento de datos.

Uso de Direct Connect con un punto final de servicio de DataSync VPC

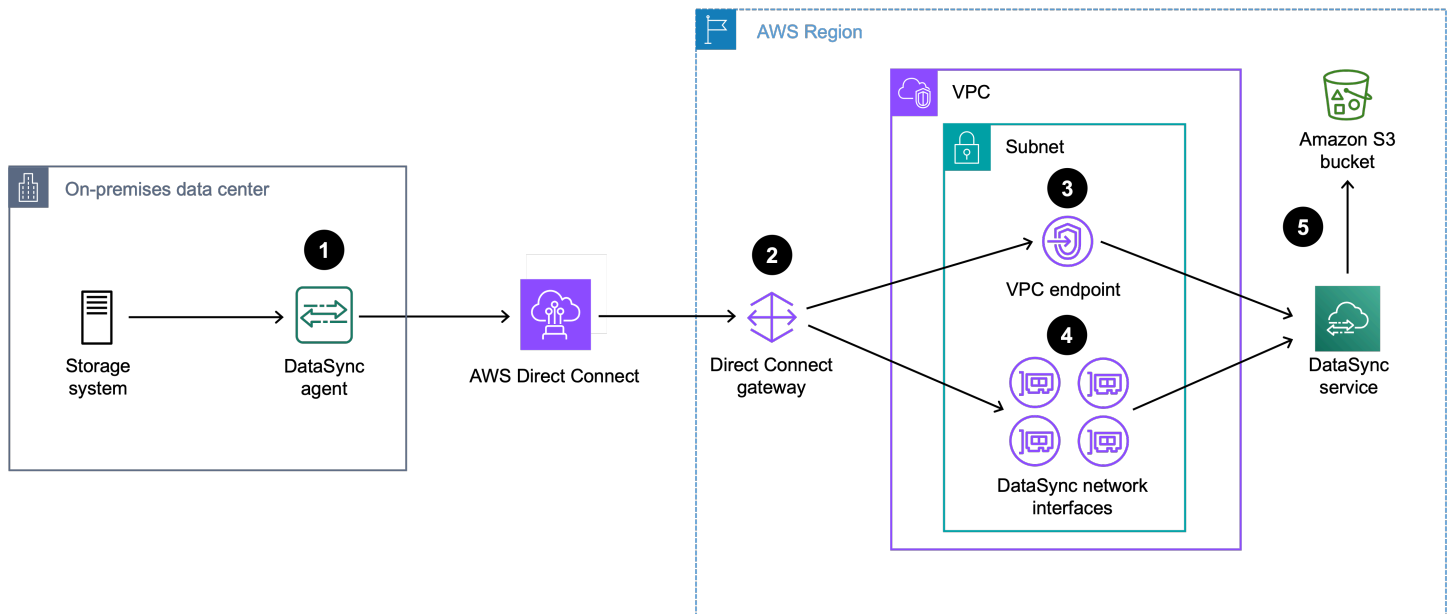
Si su DataSync agente usa un [punto final de servicio de VPC](#), necesitará una [puerta de enlace Direct Connect](#) para conectarse a su VPC.

Contenido

- [Arquitectura de Direct Connect con punto de conexión de VPC y destino en S3](#)
- [Arquitectura de Direct Connect con punto de conexión de VPC y destino del sistema de archivos en la misma subred](#)
- [Arquitectura de Direct Connect con punto de conexión de VPC y destino del sistema de archivos en subredes distintas](#)

Arquitectura de Direct Connect con punto de conexión de VPC y destino en S3

La siguiente arquitectura de Direct Connect muestra una DataSync transferencia desde un sistema de almacenamiento local a un bucket de S3.

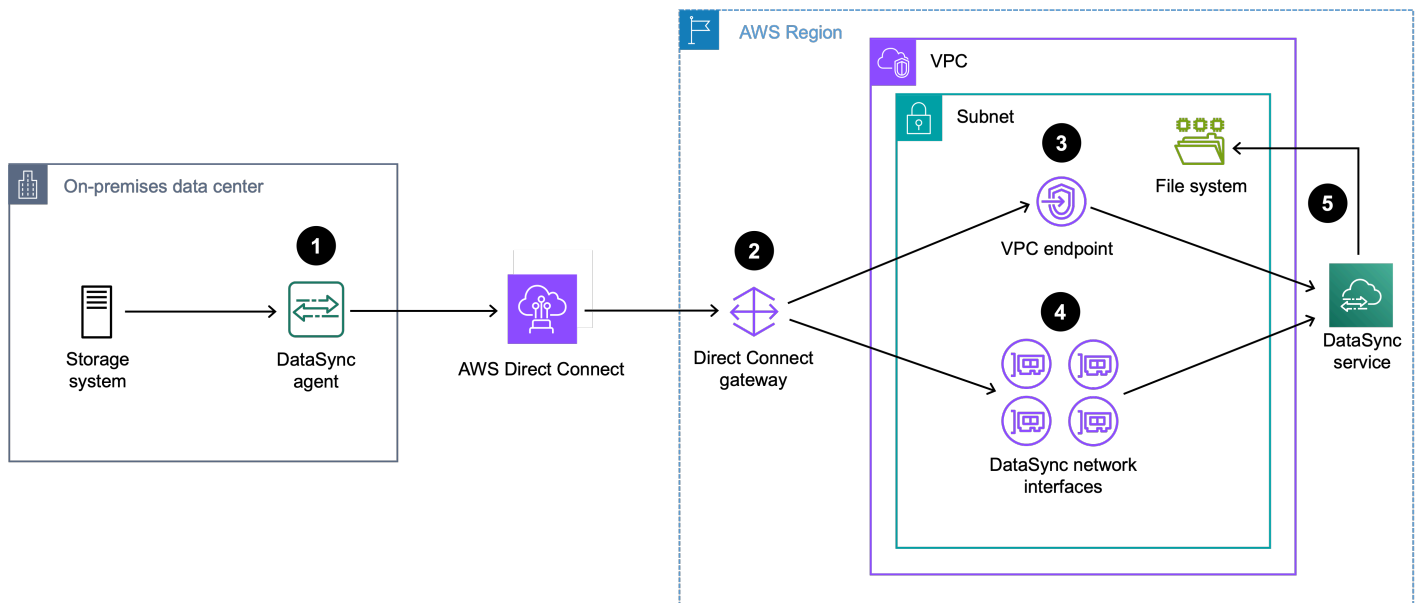


1. El DataSync agente enruta el DataSync tráfico desde el sistema de almacenamiento local (ubicación de origen) a la conexión Direct Connect.
2. DataSync rutas de tráfico a una puerta de enlace de Direct Connect que se utiliza para tu transferencia. Para configurar esto, debe:
 - a. Asociar la puerta de enlace de Direct Connect con una [puerta de enlace privada virtual](#) de la VPC. [Esta es la VPC donde se encuentra el punto final de la DataSync VPC y donde la DataSync tarea crea las interfaces de red.](#)
 - b. Crear una [interfaz virtual privada](#) que conecta esta VPC con la puerta de enlace de Direct Connect.
3. DataSync el tráfico (plano de control) se enruta a través del punto final de la DataSync VPC.
4. DataSync el tráfico (plano de datos) se enruta a través de las interfaces de DataSync red de la subred que especificó al [crear el DataSync agente](#).
5. DataSync el tráfico se enruta a través del DataSync servicio hasta el bucket de S3 (ubicación de destino).

Arquitectura de Direct Connect con punto de conexión de VPC y destino del sistema de archivos en la misma subred

Al realizar transferencias a o desde un sistema de FSx archivos Amazon EFS o Amazon, el sistema de archivos y el punto de conexión de DataSync VPC pueden estar en la misma subred.

La siguiente arquitectura de Direct Connect muestra una DataSync transferencia desde un sistema de almacenamiento local a un Amazon EFS o un sistema de FSx archivos Amazon.

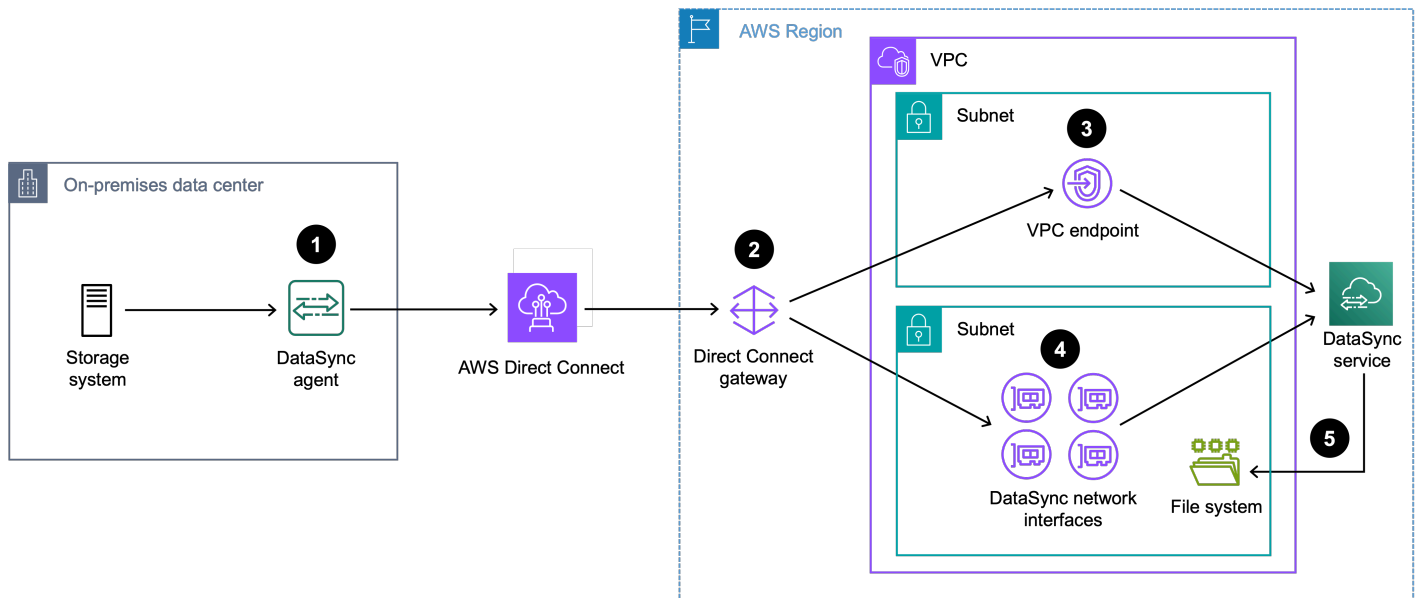


1. El DataSync agente enruta el DataSync tráfico desde el sistema de almacenamiento local (ubicación de origen) a la conexión Direct Connect.
2. DataSync rutas de tráfico a una puerta de enlace de Direct Connect que se utiliza para tu transferencia. Para configurar esto, debe:
 - a. Asociar la puerta de enlace de Direct Connect con una [puerta de enlace privada virtual](#) de la VPC. Esta es la VPC donde se encuentra el punto final de la DataSync VPC y donde la DataSync tarea crea las [interfaces de red](#) para el sistema de archivos (ubicación de destino).
 - b. Crear una [interfaz virtual privada](#) que conecta esta VPC con la puerta de enlace de Direct Connect.
3. DataSync el tráfico (plano de control) se enruta a través del punto final de la DataSync VPC.
4. DataSync el tráfico (plano de datos) se enruta a través de las interfaces de DataSync red de la subred del sistema de archivos. Es la misma subred en la que se encuentra el punto final de la DataSync VPC.
5. DataSync el tráfico se enruta a través del DataSync servicio hasta el sistema de archivos (ubicación de destino).

Arquitectura de Direct Connect con punto de conexión de VPC y destino del sistema de archivos en subredes distintas

Al realizar transferencias a o desde un sistema de FSx archivos Amazon EFS o Amazon, el sistema de archivos y el punto de conexión de DataSync VPC pueden estar en subredes diferentes.

La siguiente arquitectura de Direct Connect muestra una DataSync transferencia desde un sistema de almacenamiento local a un Amazon EFS o un sistema de FSx archivos Amazon.



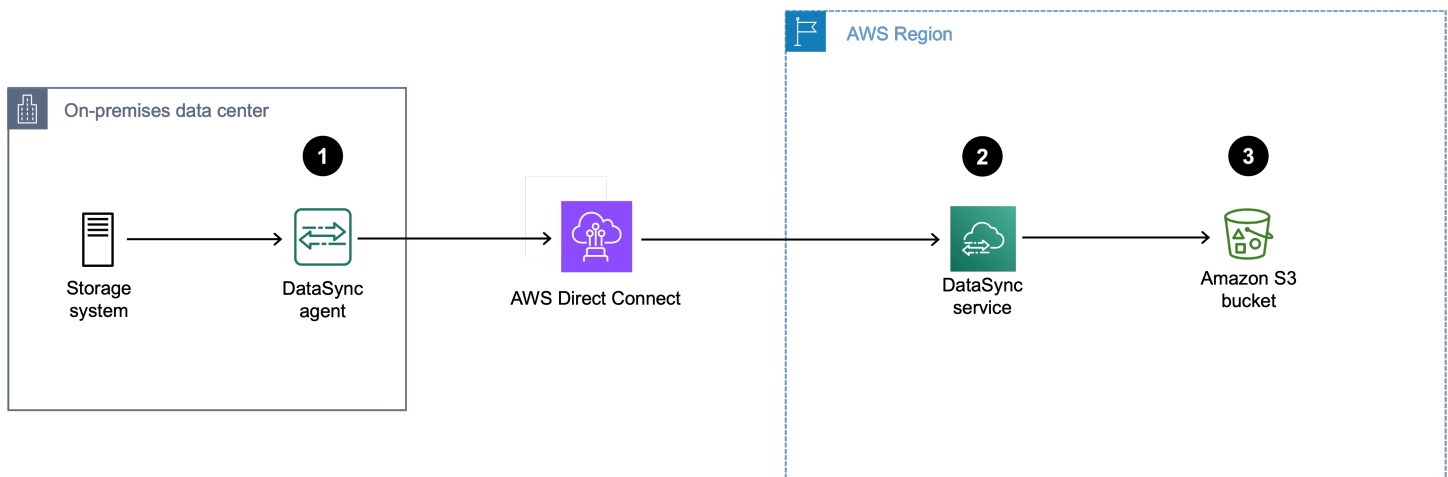
1. El DataSync agente enruta el DataSync tráfico desde el sistema de almacenamiento local (ubicación de origen) a la conexión Direct Connect.
2. DataSync rutas de tráfico a una puerta de enlace de Direct Connect que se utiliza para tu transferencia. Para configurar esto, debe:
 - a. Asociar la puerta de enlace de Direct Connect con una [puerta de enlace privada virtual](#) de la VPC. Esta es la VPC donde se encuentra el punto final de la DataSync VPC y donde la DataSync tarea crea las [interfaces de red](#) para el sistema de archivos (ubicación de destino).
 - b. Cree una [interfaz virtual privada](#) que los conecte VPCs a la puerta de enlace Direct Connect.
3. DataSync el tráfico (plano de control) se enruta a través del punto final de la DataSync VPC.
4. DataSync el tráfico (plano de datos) se enruta a través de las interfaces de DataSync red de la subred del sistema de archivos. Se trata de una subred diferente a la del punto final de la DataSync VPC.
5. DataSync el tráfico se enruta a través del DataSync servicio hasta el sistema de archivos (ubicación de destino).

Uso de Direct Connect con un punto DataSync final de servicio público o FIPS

Si su DataSync agente utiliza un punto final de servicio [público](#) o del [Estándar Federal de Procesamiento de Información \(FIPS\)](#), puede enrutar el tráfico de transferencia de datos a través de una conexión Direct Connect mediante una [interfaz virtual pública](#).

Si bien Direct Connect anuncia todos los Región de AWS prefijos locales y remotos de forma predeterminada, puede usar [etiquetas de comunidad BGP](#) para controlar el alcance (regional o global) y la preferencia de ruta del tráfico en la interfaz virtual pública. Debe anunciar al menos un prefijo público para crear su agente. DataSync

La siguiente arquitectura de Direct Connect muestra una DataSync transferencia desde un sistema de almacenamiento local a través de un punto final público o FIPS a un bucket de S3.



1. El DataSync agente enruta el DataSync tráfico desde el sistema de almacenamiento local (ubicación de origen) a la conexión Direct Connect.
2. DataSync el tráfico se dirige al DataSync servicio a través de una interfaz virtual pública.
3. DataSync tráfico al depósito S3 (ubicación de destino).

Pasos a seguir a continuación

Si [necesita un DataSync agente](#) y aún no lo ha creado, [despléguelo](#), [elija un punto de enlace de servicio](#) para el agente y, a continuación, [actívelo](#).

Una vez que haya creado el agente, podrá [configurar su red](#) para DataSync.

Configurar tu AWS DataSync agente para múltiples NICs

Si configura el AWS DataSync agente para que utilice varios adaptadores de red (NICs), podrá acceder al agente desde más de una dirección IP. Es posible que desee hacerlo en las siguientes situaciones:

- Maximización del rendimiento: quizá desee maximizar el rendimiento para un agente cuando los adaptadores de red sean un cuello de botella.
- Aislamiento de la red: su sistema de archivos de red (NFS), el bloque de mensajes del servidor (SMB), el sistema de archivos distribuido de Hadoop (HDFS) o el servidor de almacenamiento de objetos pueden residir en una LAN virtual (VLAN) que no tenga conectividad a Internet por motivos de seguridad.

En un caso de uso típico de varios adaptadores, un adaptador se configura como la ruta por la que se comunica el agente AWS (como agente predeterminado). Excepto para este adaptador, las ubicaciones de NFS, SMB, HDFS o almacenamientos de objetos autoadministrados deben estar en la misma subred que el adaptador que se conecta a ellas.

De lo contrario, puede que la comunicación con las ubicaciones de NFS, SMB, HDFS o almacenamientos de objetos autoadministrados deseadas no sea posible. En algunos casos, puede configurar una ubicación de almacenamiento NFS, SMB, HDFS o de objetos en el mismo adaptador con el que se utiliza para la comunicación. AWS En estos casos, el tráfico de NFS, SMB, HDFS o almacenamiento de objetos para ese servidor y AWS el tráfico fluye a través del mismo adaptador.

En algunos casos, puede configurar un adaptador para que se conecte a la AWS DataSync consola y, a continuación, añadir un segundo adaptador. En tal caso, configura DataSync automáticamente la tabla de enrutamiento para usar el segundo adaptador como ruta preferida.

Transferencia de datos con AWS DataSync

Con AWS DataSync, puede transferir datos a o desde un almacenamiento local, interno AWS, en otras nubes y periférico.

La configuración de una DataSync transferencia generalmente implica los siguientes pasos:

1. Determina si DataSync [es compatible con tu transferencia](#).
2. Si [necesita un DataSync agente](#) para la transferencia, despliegue y active un agente lo más cerca posible de uno de sus sistemas de almacenamiento.

Por ejemplo, si realiza la transferencia desde un servidor de archivos del sistema de archivos de red (NFS) en las instalaciones, implemente el agente lo más cerca posible de ese servidor de archivos.

3. Proporcione DataSync acceso a su sistema de almacenamiento.

DataSync necesita permiso para leer o escribir en tu almacenamiento (dependiendo de si el almacenamiento es una ubicación de origen o de destino). Por ejemplo, aprenda a [proporcionar DataSync acceso a los servidores de archivos NFS](#).

4. [Conecte su red](#) para el tráfico entre su sistema de almacenamiento y DataSync.
5. Cree una ubicación para su sistema de almacenamiento mediante la DataSync consola o la DataSync API. AWS CLI

Por ejemplo, aprenda a [crear una ubicación de NFS](#) o una [ubicación de Amazon S3](#).

6. Repita los pasos 3-5 para crear la otra ubicación de su transferencia.
7. [Cree e inicie una tarea de DataSync transferencia](#) que incluya las ubicaciones de origen y destino.

Temas

- [¿Dónde puedo transferir mis datos con AWS DataSync?](#)
- [Transferir hacia o desde el almacenamiento local con AWS DataSync](#)
- [Transferir al AWS almacenamiento o desde él con AWS DataSync](#)
- [Transferir hacia o desde otro almacenamiento en la nube con AWS DataSync](#)
- [Transferencia a o desde un almacenamiento compatible con S3 en Snowball Edge](#)
- [Crear una tarea para transferir sus datos](#)

- [Iniciar una tarea para transferir los datos](#)

¿Dónde puedo transferir mis datos con AWS DataSync?

El lugar al que puede transferir sus datos AWS DataSync depende de los siguientes factores:

- Las [ubicaciones](#) de origen y destino de su transferencia
- Si sus ubicaciones están en ubicaciones diferentes Cuentas de AWS
- Si sus ubicaciones están en diferentes Regiones de AWS

Transferencias admitidas en la misma Cuenta de AWS

DataSync admite transferencias entre los siguientes recursos de almacenamiento que están asociados a los mismos Cuenta de AWS.

Origen (Desde)	Destino (A)
• NFS • SMB • HDFS • Almacenamiento de objetos	• Amazon S3 (en Regiones de AWS) • Amazon EFS • Servidor FSx de archivos Amazon para Windows • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP
• Amazon S3 (en Regiones de AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	• NFS • SMB • HDFS • Almacenamiento de objetos
• Google Cloud Storage • Microsoft Azure Blob Storage • Microsoft Azure Files	• Amazon S3 (en Regiones de AWS) • Amazon EFS • Servidor FSx de archivos Amazon para Windows

Origen (Desde)	Destino (A)
• 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	• FSx para Lustre • FSx para OpenZFS • FSx para ONTAP
• Amazon S3 (en Regiones de AWS) • Amazon EFS • Servidor FSx de archivos 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
• Almacenamiento compatible con Amazon S3 en AWS Snowball Edge	• Amazon S3 (en Regiones de AWS) • Amazon EFS • Servidor FSx de archivos Amazon para Windows • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP

Origen (Desde)	Destino (A)
• Amazon S3 (en Regiones de AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	• Almacenamiento compatible con Amazon S3 en Snowball Edge
• Amazon S3 (en Regiones de AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	• Amazon S3 (en Regiones de AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP
• Amazon S3 (en AWS regiones)	• Amazon S3 en AWS Outposts
• Amazon S3 en AWS Outposts	• Amazon S3 (en Regiones de AWS)

Transferencias compatibles entre Cuentas de AWS

DataSync admite algunas transferencias entre recursos de almacenamiento que están asociados a diferentes Cuentas de AWS.

Origen (Desde)	Destino (A)
• Amazon EFS¹ • FSx para Windows File Server²	• Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP

Origen (Desde)	Destino (A)
• Amazon S3 (en Regiones de AWS)	• Amazon S3 (en Regiones de AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP
• Amazon S3 (en Regiones de AWS) • Amazon EFS • FSx para Windows File Server • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP	• Amazon S3 (en Regiones de AWS)
• NFS • SMB • HDFS • Almacenamiento de objetos	• Amazon S3 (en Regiones de AWS)

¹ Configurado como una [ubicación NFS](#).

² Configurado como una [ubicación de SMB](#).

Transferencias admitidas en la misma Región de AWS

No hay restricciones a la hora de transferir datos dentro de la misma Región de AWS (incluidas las [regiones opcionales](#)). Para obtener más información, consulte [Regiones de AWS con el apoyo de DataSync](#).

Transferencias compatibles entre Regiones de AWS

Tenga en cuenta lo siguiente cuando transfiera datos entre [Regiones de AWS dispositivos compatibles con DataSync](#):

- Al realizar transferencias entre servicios AWS de almacenamiento situados en diferentes ubicaciones Regiones de AWS, una de las dos ubicaciones debe estar en la región en la que se utiliza DataSync.
- No puede realizar transferencias entre regiones con una ubicación de NFS, SMB, HDFS o de almacenamientos de objetos. En estas situaciones, las dos ubicaciones de transferencia deben estar en la misma región en la que [activaste tu DataSync agente](#).
- Con AWS GovCloud (US) Regions, puede:
 - Transfiere entre las regiones AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste).
 - Transfiere entre una AWS GovCloud (US) región y una zona comercial Región de AWS, como EE. UU. Este (Virginia del Norte). Este tipo de transferencia requiere un [agente](#) cuando se realiza una transferencia entre Amazon EFS o Amazon FSx file systems.

Important

Usted paga por los datos transferidos entre ellos Regiones de AWS. Esta transferencia se factura como transferencia de datos de salida desde la región de origen a la región de destino. Para más información, consulte [Precios de AWS DataSync](#).

Determinar si su transferencia requiere un DataSync agente

Según el escenario de tu transferencia, es posible que necesites un DataSync agente. Para obtener más información, consulte [¿Necesito un AWS DataSync agente?](#)

Transferir hacia o desde el almacenamiento local con AWS DataSync

Con AWS DataSync, puedes transferir archivos y objetos entre varios sistemas de almacenamiento locales o autogestionados y los siguientes servicios de almacenamiento: AWS

- [Amazon S3](#)

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

Temas

- [Configuración de AWS DataSync transferencias con un servidor de archivos NFS](#)
- [Configurar las AWS DataSync transferencias con un servidor de archivos SMB](#)
- [Configuración de AWS DataSync transferencias con un clúster HDFS](#)
- [Configurar DataSync las transferencias con un sistema de almacenamiento de objetos](#)

Configuración de AWS DataSync transferencias con un servidor de archivos NFS

Con AWS DataSync, puede transferir datos entre el servidor de archivos del Network File System (NFS) y uno de los siguientes servicios de AWS almacenamiento:

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

Para configurar este tipo de transferencia, cree una [ubicación](#) de transferencia para su servicios de archivos de NFS. Puede usar esta ubicación como origen o destino de la transferencia.

Proporcionar DataSync acceso a los servidores de archivos NFS

[Para acceder DataSync a su servidor de archivos NFS, necesita un DataSync agente.](#) El agente monta una exportación en su servidor de archivos mediante el protocolo NFS.

Temas

- [Configuración de su exportación a NFS](#)
- [Versiones NFS compatibles](#)

Configuración de su exportación a NFS

La exportación DataSync necesaria para la transferencia depende de si el servidor de archivos NFS es una ubicación de origen o de destino y de la configuración de los permisos del servidor de archivos.

Si su servidor de archivos es una ubicación de origen, DataSync solo tiene que leer y recorrer sus archivos y carpetas. Si es una ubicación de destino, DataSync necesita acceso root para escribir en la ubicación y establecer la propiedad, los permisos y otros metadatos de los archivos y carpetas que va a copiar. Puede usar la opción `no_root_squash` para permitir el acceso root para su exportación.

En los siguientes ejemplos, se describe cómo configurar una exportación de NFS a la que se proporciona acceso DataSync.

Cuando el servidor de archivos NFS es una ubicación de origen (acceso root)

Configure la exportación mediante el siguiente comando, que proporciona permisos de DataSync solo lectura (`ro`) y acceso root (`()`): `no_root_squash`

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

Cuando el servidor de archivos NFS es una ubicación de destino

Configure la exportación mediante el siguiente comando, que proporciona permisos de DataSync escritura (`rw`) y acceso root (`no_root_squash`):

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

Cuando el servidor de archivos NFS es una ubicación de origen (sin acceso root)

Configure la exportación mediante el siguiente comando, que especifica el ID de usuario (UID) y el ID de grupo (GID) de POSIX que sabe que proporcionarían permisos de DataSync solo lectura para la exportación:

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

Versiones NFS compatibles

De forma predeterminada, usa la versión 4.1 de DataSync NFS. DataSync también es compatible con NFS 4.0 y 3.x.

Configuración de la red para transferencias NFS

Para la DataSync transferencia, debe configurar el tráfico para algunas conexiones de red:

1. Permita el tráfico de su DataSync agente a su servidor de archivos NFS en los siguientes puertos:

- Para NFS versiones 4.1 y 4.0: puerto TCP 2049
- Para la versión 3.x de NFS: puertos TCP 111 y 2049

Los demás clientes NFS de su red deberían poder montar la exportación a NFS que usted utiliza para transferir datos. Asegúrese de que la exportación también sea accesible sin la autenticación de Kerberos.

2. Configure el tráfico para su [conexión de punto de conexión de servicio](#) (como un punto de enlace de VPC, público o FIPS).
3. Permita el tráfico del DataSync servicio al servicio de [AWS almacenamiento](#) desde o hacia el que está realizando la transferencia.

Creación de la ubicación de transferencia NFS

Antes de comenzar, tenga en cuenta lo siguiente:

- Necesita un servidor de archivos NFS desde el que quiera transferir datos.
- Necesitas un DataSync agente que pueda [acceder a tu servidor de archivos](#).
- DataSync no admite la copia de las listas de control de acceso de la versión 4 de NFS (ACLs).

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en. <https://console.aws.amazon.com/datasync/>
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.

3. En Tipo de ubicación, elija Sistema de archivos de red (NFS).
4. En el caso de los agentes, elija el DataSync agente que se pueda conectar a su servidor de archivos NFS.

Puede elegir más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

5. En el caso del servidor NFS, introduzca el nombre del sistema de nombres de dominio (DNS) o la dirección IP del servidor de archivos NFS al que se conecta el DataSync agente.
6. En Ruta de montaje, introduzca la ruta de exportación de NFS que desee DataSync montar.

Esta ruta (o un subdirectorio de la ruta) es DataSync desde donde se transfieren los datos hacia o desde. Para obtener más información, consulte [Configuración de su exportación a NFS](#).

7. (Opcional) Amplíe la configuración adicional y elija una versión de NFS específica para DataSync utilizarla al acceder al servidor de archivos.

Para obtener más información, consulte [Versiones NFS compatibles](#).

8. (Opcional) Seleccione Añadir etiqueta para etiquetar su ubicación de NFS.

Las etiquetas son pares de clave-valor que le ayudan a administrar, filtrar y buscar sus recursos de DataSync. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

9. Seleccione Crear ubicación.

Usando el AWS CLI

- Utilice el siguiente comando para crear una ubicación de NFS.

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

Para obtener más información sobre la creación de la ubicación, consulte [Proporcionar DataSync acceso a los servidores de archivos NFS](#).

DataSync elige automáticamente la versión de NFS que utiliza para leer desde una ubicación de NFS. Para especificar una versión de NFS, utilice el parámetro `Version` opcional en la operación de la API [NfsMountOptions](#).

Este comando devuelve el nombre de recurso de Amazon (ARN) de la ubicación de NFS, que es similar al ARN que se muestra a continuación.

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

Para asegurarse de que el directorio se puede montar, puede conectarse a cualquier equipo que tenga la misma configuración de red que su agente y ejecutar el siguiente comando.

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

A continuación, se muestra un ejemplo del 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
```

Configurar las AWS DataSync transferencias con un servidor de archivos SMB

Con AWS DataSync, puede transferir datos entre su servidor de archivos del bloque de mensajes del servidor (SMB) y uno de los siguientes servicios de AWS almacenamiento:

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

Para configurar este tipo de transferencia, cree una [ubicación](#) de transferencia para su servicios de archivos de SMB. Puede usar esto como origen o destino de la transferencia.

Proporcionar DataSync acceso a servidores de archivos SMB

DataSync se conecta al servidor de archivos mediante el protocolo SMB y puede autenticarse con NTLM o Kerberos.

Temas

- [Versiones compatibles de SMB](#)
- [Uso de la autenticación NTLM](#)
- [Uso de la autenticación Kerberos](#)
- [Permisos necesarios](#)
- [Espacios de nombres de DFS](#)

Versiones compatibles de SMB

De forma predeterminada, elige DataSync automáticamente una versión del protocolo SMB en función de la negociación con el servidor de archivos SMB.

También puede configurarlo DataSync para usar una versión SMB específica, pero le recomendamos que lo haga solo si DataSync tiene problemas para negociar automáticamente con el servidor de archivos SMB. DataSync es compatible con las versiones 1.0 y posteriores para SMB. Por motivos de seguridad, recomendamos utilizar la versión 3.0.2 o posterior para SMB. Las versiones anteriores, como SMB 1.0, contienen vulnerabilidades de seguridad conocidas que los atacantes pueden aprovechar para comprometer sus datos.

Consulta la siguiente tabla para ver una lista de las opciones de la DataSync consola y la API:

Opción de la consola	Opción de la API	Descripción
Automático	AUTOMATIC	DataSync y el servidor de archivos SMB negocian la versión más alta de SMB que admiten mutuamente, entre la 2.1 y la 3.1.1. Esta es la opción predeterminada y recomendada. Si, por el contrario, elige una versión específica que el servidor de archivos no admite, es posible que aparezca un error <code>Operation Not Supported</code> .

Opción de la consola	Opción de la API	Descripción
SMB 3.0.2	SMB3	Restringe la negociación del protocolo solo a la versión 3.0.2 de SMB.
SMB 2.1	SMB2	Restringe la negociación del protocolo solo a la versión 2.1 de SMB.
SMB 2.0	SMB2_0	Restringe la negociación del protocolo solo a la versión 2.0 de SMB.
SMB 1.0	SMB1	Restringe la negociación del protocolo solo a la versión 1.0 de SMB.

Uso de la autenticación NTLM

Para usar la autenticación NTLM, debe proporcionar un nombre de usuario y una contraseña que le permitan acceder DataSync al servidor de archivos SMB desde o hacia el que está realizando la transferencia. El usuario puede ser un usuario local en su servidor de archivos o un usuario de dominio en su Microsoft Active Directory.

Uso de la autenticación Kerberos

Para usar la autenticación Kerberos, debe proporcionar un archivo principal de Kerberos, un archivo de tabla de claves (keytab) de Kerberos y un archivo de configuración de Kerberos que le permitan acceder DataSync al servidor de archivos SMB desde o hacia el que está realizando la transferencia.

Temas

- [Requisitos previos](#)
- [DataSync opciones de configuración para Kerberos](#)

Requisitos previos

Debe crear un par de artefactos de Kerberos y configurar la red para que DataSync pueda acceder al servidor de archivos SMB.

- [Cree un archivo keytab de Kerberos mediante la utilidad ktpass o kutil.](#)

En el siguiente ejemplo, se crea un archivo keytab mediante. `ktpass` El dominio de Kerberos que especifique (`MYDOMAIN.ORG`) debe estar en mayúscula.

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

- Prepare una versión simplificada del archivo de configuración de Kerberos (`krb5.conf`). Incluya información sobre el dominio, la ubicación de los servidores de administración del dominio y las asignaciones de los nombres de host a un dominio de Kerberos.

Compruebe que el `krb5.conf` contenido esté formateado con la combinación correcta de mayúsculas y minúsculas para los dominios y los nombres de dominio. Por ejemplo:

```
[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
```

- En la configuración de red, asegúrese de que el puerto del servidor del Centro de distribución de claves (KDC) de Kerberos esté abierto. El puerto KDC suele ser el puerto TCP 88.

DataSync opciones de configuración para Kerberos

Al crear una ubicación SMB que utilice Kerberos, configure las siguientes opciones.

Opción de la consola	Opción de la API	Descripción
Servidor SMB	<code>ServerHostName</code>	El nombre de dominio del servidor de archivos SMB que

Opción de la consola	Opción de la API	Descripción
		montará su DataSync agente. En el caso de Kerberos, no puede especificar la dirección IP del servidor de archivos.
Kerberos principal	KerberosPrincipal	Una identidad de su dominio de Kerberos que tiene permiso para acceder a los archivos, las carpetas y los metadatos de los archivos de su servidor de archivos SMB. Un principal de Kerberos podría tener un aspecto similar. HOST/kerberosuser@MYDOMAIN.ORG Los nombres principales distinguen entre mayúsculas y minúsculas.
Archivo Keytab	KerberosKeytab	Un archivo de tabla de claves de Kerberos (keytab), que incluye las asignaciones entre las claves principales y de cifrado de Kerberos.
Archivo de configuración de Kerberos	KerberosKrbConf	Un <code>krb5.conf</code> archivo que define la configuración del dominio de Kerberos.

Opción de la consola	Opción de la API	Descripción
Direcciones IP DNS (opcionales)	DnsIpAddresses	Las IPv4 direcciones de los servidores DNS a los que pertenece su servidor de archivos SMB. Si tiene varios dominios en su entorno, al configurarlos se asegura de que DataSync se conecten al servidor de archivos SMB correcto.

Permisos necesarios

La identidad que proporcione DataSync debe tener permiso para montar y acceder a los archivos, carpetas y metadatos de archivos de su servidor de archivos SMB.

Si proporciona una identidad en su Active Directory, debe ser miembro de un grupo de Active Directory con uno o ambos de los siguientes derechos de usuario (según los [metadatos que desee DataSync copiar](#)):

Derecho de usuario	Descripción
Restaurar archivos y directorios (SE_RESTORE_NAME)	Permite DataSync copiar la propiedad de los objetos, los permisos, los metadatos de los archivos y las listas de acceso discrecional de NTFS (DACLs). Este derecho de usuario se suele conceder a los miembros de los grupos Domain Admins y Backup Operators (ambos grupos predeterminados de Active Directory).
Administre el registro de auditoría y seguridad (SE_SECURITY_NAME)	Permite copiar DataSync las listas de control de acceso al sistema NTFS (SACLs)

Derecho de usuario	Descripción
	Este derecho de usuario se suele conceder a los miembros del grupo de administradores de dominio.

Si desea copiar Windows ACLs y realiza una transferencia entre un servidor de archivos SMB y otro sistema de almacenamiento que utilice SMB (como Amazon FSx for Windows File Server o FSx ONTAP), la identidad que proporcione DataSync debe pertenecer al mismo dominio de Active Directory o tener una relación de confianza de Active Directory entre sus dominios.

Espacios de nombres de DFS

DataSync no admite los espacios de nombres del Sistema de archivos distribuido (DFS) de Microsoft. En su lugar, se recomienda especificar un servidor de archivos subyacente o un recurso compartido al crear la ubicación. DataSync

Creación de la ubicación de transferencia de SMB

Antes de empezar, necesita un servidor de archivos SMB desde el que quiera transferir datos.

Mediante la consola de DataSync

1. Abre la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. En Location type (Tipo de ubicación), elija Server Message Block (SMB).

Puede configurar esta ubicación como origen o destino posteriormente.

4. En el caso de los agentes, elija el DataSync agente que se pueda conectar a su servidor de archivos SMB.

Puede elegir más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

5. Para el servidor SMB, introduzca el nombre de dominio o la dirección IP del servidor de archivos SMB que montará su DataSync agente.

Recuerde lo siguiente con esta configuración:

- No puede especificar una dirección IP de versión 6 (IPv6).
 - Si utiliza la autenticación Kerberos, debe especificar un nombre de dominio.
6. En Nombre del recurso compartido, introduzca el nombre del recurso compartido exportado por el servidor de archivos SMB donde DataSync se leerán o escribirán los datos.

Puede incluir un subdirectorio en la ruta del recurso compartido (por ejemplo, /path/to/subdirectory). Asegúrese de que otros clientes de SMB de la red también puedan montar esta ruta.

Para copiar todos los datos del subdirectorio, DataSync debe poder montar el recurso compartido SMB y acceder a todos sus datos. Para obtener más información, consulte [Permisos necesarios](#).

7. (Opcional) Amplíe la configuración adicional y elija una versión SMB para utilizarla DataSync al acceder al servidor de archivos.

De forma predeterminada, elige DataSync automáticamente una versión en función de la negociación con el servidor de archivos SMB. Para obtener información, consulte [Versiones compatibles de SMB](#).

8. Para el tipo de autenticación, elija NTLM o Kerberos.
9. Realice una de las siguientes acciones en función del tipo de autenticación:

NTLM

- En Usuario, especifique el nombre del usuario que puede montar su servidor de archivos SMB y que tiene permiso para acceder a los archivos y carpetas que intervienen en la transferencia.

Para obtener más información, consulte [Permisos necesarios](#).

- En Contraseña, introduzca la contraseña del usuario que puede montar su servidor de archivos SMB y que tiene los permisos para acceder a los archivos y carpetas que intervienen en la transferencia.
- (Opcional) En Dominio, ingrese el nombre del dominio de Windows al que pertenece su servidor de archivos SMB.

Si tiene varios dominios en su entorno, al configurar esta configuración se asegura de que DataSync se conecte al servidor de archivos SMB correcto.

Kerberos

- En el caso del servidor principal de Kerberos, especifique un principal de su dominio de Kerberos que tenga permiso para acceder a los archivos, las carpetas y los metadatos de los archivos de su servidor de archivos SMB.

Un principal de Kerberos podría tener este aspecto. HOST/
kerberosuser@MYDOMAIN.ORG

Los nombres principales distinguen entre mayúsculas y minúsculas. La ejecución de la DataSync tarea fallará si el principal que especifique para esta configuración no coincide exactamente con el principal que utilizó para crear el archivo keytab.

- En el caso del archivo Keytab, cargue un archivo keytab que incluya las asignaciones entre la clave principal y la clave de cifrado de Kerberos.
- Para el archivo de configuración de Kerberos, cargue un **krb5.conf** archivo que defina la configuración del dominio de Kerberos.
- (Opcional) Para las direcciones IP de DNS, especifique hasta dos IPv4 direcciones para los servidores DNS a los que pertenece el servidor de archivos SMB.

Si tiene varios dominios en su entorno, la configuración de este parámetro garantiza que DataSync se conecte al servidor de archivos SMB correcto.

10. (Opcional) Seleccione Añadir etiqueta para etiquetar su ubicación de SMB.

Las etiquetas son pares de clave-valor que le ayudan a administrar, filtrar y buscar sus recursos de DataSync. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

11. Seleccione Crear ubicación.

Mediante el AWS CLI

Las siguientes instrucciones describen cómo crear ubicaciones SMB con la autenticación NTLM o Kerberos.

NTLM

1. Copie el siguiente 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 el DataSync agente que se puede conectar al servidor de archivos SMB.

Puede elegir más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

3. Para `--server-hostname`, especifique el nombre de dominio o la IPv4 dirección del servidor de archivos SMB que montará el DataSync agente.
4. Para `--subdirectory`, especifique el nombre del recurso compartido exportado por el servidor de archivos SMB en el que se DataSync leerán o escribirán los datos.

Puede incluir un subdirectorio en la ruta del recurso compartido (por ejemplo, `/path/to/subdirectory`). Asegúrese de que otros clientes de SMB de la red también puedan montar esta ruta.

Para copiar todos los datos del subdirectorio, DataSync debe poder montar el recurso compartido SMB y acceder a todos sus datos. Para obtener más información, consulte [Permisos necesarios](#).

5. Para `--user` ello, especifique un nombre de usuario que pueda montar su servidor de archivos SMB y que tenga permiso para acceder a los archivos y carpetas implicados en la transferencia.

Para obtener más información, consulte [Permisos necesarios](#).

6. Para `--password` ello, especifique la contraseña del usuario que puede montar el servidor de archivos SMB y que tiene permiso para acceder a los archivos y carpetas implicados en la transferencia.
7. (Opcional) Para `--domain`, especifique el nombre de dominio de Windows al que pertenece su servidor de archivos SMB.

Si tiene varios dominios en su entorno, al configurar esta configuración se asegura de que DataSync se conecte al servidor de archivos SMB correcto.

8. (Opcional) Añada la `--version` opción si desea DataSync utilizar una versión SMB específica. Para obtener más información, consulte [Versiones compatibles de SMB](#).
9. Ejecute el comando `create-location-smb`.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la ubicación que creó. Por ejemplo:

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

Kerberos

1. Copie el siguiente 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 el DataSync agente que se puede conectar a su servidor de archivos SMB.

Puede elegir más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

3. Para `--server-hostname`, especifique el nombre de dominio del servidor de archivos SMB que montará el DataSync agente.
4. Para `--subdirectory`, especifique el nombre del recurso compartido exportado por el servidor de archivos SMB en el que se DataSync leerán o escribirán los datos.

Puede incluir un subdirectorio en la ruta del recurso compartido (por ejemplo, `/path/to/subdirectory`). Asegúrese de que otros clientes de SMB de la red también puedan montar esta ruta.

Para copiar todos los datos del subdirectorio, DataSync debe poder montar el recurso compartido SMB y acceder a todos sus datos. Para obtener más información, consulte [Permisos necesarios](#).

5. Para las opciones de Kerberos, haga lo siguiente:

- `--kerberos-principal`: especifique una entidad principal de su dominio de Kerberos que tenga permiso para acceder a los archivos, las carpetas y los metadatos de los archivos de su servidor de archivos SMB.

Un principal de Kerberos podría tener este aspecto. `HOST/kerberosuser@MYDOMAIN.ORG`

Los nombres principales distinguen entre mayúsculas y minúsculas. La ejecución de la DataSync tarea fallará si el principal que especifique para esta opción no coincide exactamente con el principal que utilizó para crear el archivo keytab.

- `--kerberos-keytab`: especifique un archivo keytab que incluya las asignaciones entre la clave principal y la clave de cifrado de Kerberos.
- `--kerberos-krb5-conf`: especifique un `krb5.conf` archivo que defina la configuración de su dominio de Kerberos.
- (Opcional) `--dns-ip-addresses`: especifique hasta dos IPv4 direcciones para los servidores DNS a los que pertenece su servidor de archivos SMB.

Si tiene varios dominios en su entorno, la configuración de este parámetro garantiza que DataSync se conecte al servidor de archivos SMB correcto.

6. (Opcional) Añada la `--version` opción si desea DataSync utilizar una versión SMB específica. Para obtener más información, consulte [Versiones compatibles de SMB](#).

7. Ejecute el comando `create-location-smb`.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la ubicación que creó. Por ejemplo:

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

Configuración de AWS DataSync transferencias con un clúster HDFS

Con él AWS DataSync, puede transferir datos entre el clúster del sistema de archivos distribuido de Hadoop (HDFS) y uno de los siguientes servicios de almacenamiento: AWS

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

Para configurar este tipo de transferencia, cree una [ubicación](#) de transferencia para su clúster de HDFS. Puede usar esta ubicación como origen o destino de la transferencia.

Proporcionar DataSync acceso a los clústeres de HDFS

Para conectarse al clúster de HDFS, DataSync utilice un [agente que se implemente lo](#) más cerca posible del clúster de HDFS. El DataSync agente actúa como un cliente HDFS y se comunica con el clúster NameNodes y dentro de él DataNodes .

Al iniciar una tarea de transferencia, DataSync consulta las ubicaciones NameNode de los archivos y carpetas del clúster. Si configura la ubicación de HDFS como ubicación de origen, DataSync lee los datos de archivos y carpetas del clúster y copia esos datos DataNodes en el destino. Si configura la ubicación de HDFS como ubicación de destino, DataSync graba los archivos y carpetas del origen DataNodes en el clúster.

Autenticación

Al conectarse a un clúster HDFS, DataSync admite la autenticación simple o la autenticación Kerberos. Para usar una autenticación simple, proporcione el nombre de usuario de un usuario con derechos de lectura y escritura en el clúster de HDFS. Para usar la autenticación Kerberos, proporcione un archivo de configuración de Kerberos, un archivo de tabla de claves de Kerberos (keytab) y un nombre de entidad principal de Kerberos. Las credenciales de la entidad principal de Kerberos deben estar en el archivo keytab proporcionado.

Cifrado

Cuando se utiliza la autenticación Kerberos, DataSync admite el cifrado de los datos a medida que se transmiten entre el DataSync agente y el clúster HDFS. Cifre sus datos mediante los ajustes de configuración de calidad de protección (QOP) del clúster de HDFS y especificando los ajustes de QOP al crear la ubicación de HDFS. La configuración de QOP incluye ajustes para la protección de la transferencia de datos y la protección de llamada a procedimiento remoto (RPC).

DataSync admite los siguientes tipos de cifrado 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`

También se pueden configurar clústeres de HDFS para el cifrado en reposo mediante el cifrado de datos transparente (TDE). Cuando se utiliza una autenticación simple, DataSync lee y escribe en clústeres habilitados para TDE. Si va DataSync a copiar datos a un clúster compatible con TDE, primero configure las zonas de cifrado del clúster HDFS. DataSync no crea zonas de cifrado.

Características de HDFS no admitidas

Las siguientes capacidades de HDFS no son compatibles DataSync actualmente con:

- Cifrado de datos transparente (TDE) cuando se utiliza la autenticación Kerberos
- Configuración de varios NameNodes
- Hadoop HDFS por HTTP (HttpFS)

- Listas de control de acceso POSIX () ACLs
- Atributos extendidos de HDFS (xattrs)
- Clústeres HDFS que utilizan Apache HBase

Creación de su ubicación de transferencia HDFS

Puede utilizar su ubicación como origen o destino de la DataSync transferencia.

Antes de empezar: compruebe la conectividad de red entre el agente y el clúster de Hadoop de la siguiente manera:

- Pruebe el acceso a los puertos TCP que figuran en [Requisitos de red para el almacenamiento autoadministrado en las instalaciones y otros tipos de almacenamiento periférico en la nube](#).
- Pruebe el acceso entre su agente local y su clúster de Hadoop. Para obtener instrucciones, consulte [Verificación de la conexión de su agente con su sistema de almacenamiento](#).

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. En Tipo de ubicación, elija sistema de archivos distribuido de Hadoop (HDFS).

Puede configurar esta ubicación como origen o destino posteriormente.

4. En Agentes, elija el agente que se pueda conectar con su clúster de HDFS.

Puede elegir más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

5. Para NameNode, proporcione el nombre de dominio o la dirección IP del clúster HDFS principal NameNode.
6. En Carpeta, introduzca una carpeta del clúster HDFS que desee utilizar DataSync para la transferencia de datos.

Si la ubicación de HDFS es una fuente, DataSync copia los archivos de esta carpeta en el destino. Si su ubicación es un destino, graba DataSync los archivos en esta carpeta.

7. Para establecer el Tamaño del bloque o el Factor de replicación, seleccione Ajustes adicionales.

El tamaño de bloque predeterminado es 128 MB. Los tamaños de los bloques que indique deben ser múltiplos de 512 bytes.

El factor de replicación predeterminado es tres DataNodes cuando se transfiere al clúster HDFS.

8. En la sección Seguridad, elija el Tipo de autenticación utilizado en el clúster de HDFS.

- Simple: para el usuario, especifique el nombre de usuario con los siguientes permisos en el clúster de HDFS (según su caso de uso):
 - Si planea usar esta ubicación como ubicación de origen, especifique un usuario que solo tenga permisos de lectura.
 - Si planea usar esta ubicación como ubicación de destino, especifique un usuario que solo tenga permisos de escritura.

Opcionalmente, especifique el URI de Key Management Server (KMS) del clúster de HDFS.

- Kerberos: especifique la entidad principal de Kerberos con acceso al clúster de HDFS. A continuación, proporcione el KeyTabarchivo que contiene el principal Kerberos proporcionado. A continuación, proporcione el archivo de configuración de Kerberos. Por último, especifique el tipo de protección de cifrado en tránsito en las listas desplegables de Protección RPC y Protección de transferencia de datos.

9. (Opcional) Seleccione Añadir etiqueta para etiquetar su ubicación de HDFS.

Las etiquetas son pares de clave-valor que le ayudan a administrar, filtrar y buscar sus recursos de DataSync. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

10. Seleccione Crear ubicación.

Usando el AWS CLI

1. Copie el siguiente 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 el `--name-nodes` parámetro, especifique el nombre de host o la dirección IP del clúster HDFS principal NameNode y el puerto TCP en el que NameNode se escucha.
3. Para el parámetro `--authentication-type`, especifique el tipo de autenticación que se utilizará para conectarse al clúster de Hadoop. Puede especificar `SIMPLE` o `KERBEROS`.

Si utiliza la autenticación `SIMPLE`, utilice el parámetro `--simple-user` para especificar el nombre de usuario del usuario. Si utiliza la autenticación `KERBEROS`, utilice los parámetros `--kerberos-principal`, `--kerberos-keytab` y `--kerberos-krb5-conf`. Para obtener más información, consulte [create-location-hdfs](#).

4. Para el `--agent-arns` parámetro, especifique el ARN del DataSync agente que se puede conectar al clúster HDFS.

Puede elegir más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

5. (Opcional) Para el `--subdirectory` parámetro, especifique una carpeta del clúster HDFS que desee utilizar DataSync para la transferencia de datos.

Si la ubicación de HDFS es una fuente, DataSync copia los archivos de esta carpeta en el destino. Si su ubicación es un destino, graba DataSync los archivos en esta carpeta.

6. Ejecute el comando `create-location-hdfs`.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la ubicación que creó. Por ejemplo:

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

Configurar DataSync las transferencias con un sistema de almacenamiento de objetos

Con AWS DataSync, puede transferir datos entre su sistema de almacenamiento de objetos y uno de los siguientes servicios AWS de almacenamiento:

- [Amazon S3](#)
- [Amazon EFS](#)

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

Para configurar este tipo de transferencia, cree una [ubicación](#) para su sistema de almacenamiento de objetos. Puede usar esta ubicación como origen o destino de la transferencia. La transferencia de datos hacia o desde su almacenamiento de objetos local requiere un DataSync agente.

Requisitos previos

Su sistema de almacenamiento de objetos debe ser compatible con las siguientes [operaciones de la API de Amazon S3](#) DataSync para poder conectarse a él:

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

Creación de la ubicación de transferencia de almacenamiento de objetos

Antes de comenzar, necesita un sistema de almacenamiento de objetos desde o hacia el que planea transferir datos.

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. En Tipo de ubicación, seleccione Almacenamiento de objetos.

Puede configurar esta ubicación como origen o destino posteriormente.

4. En Servidor, especifique el nombre de dominio o la dirección IP del servidor de almacenamiento de objetos.
5. En Nombre del bucket, especifique el nombre del bucket de almacenamiento de objetos que intervienen en la transferencia.
6. En Carpeta, introduzca un prefijo de objeto.

DataSync solo copia objetos con este prefijo.

7. Si la transferencia requiere un agente, selecciona Usar agentes y, a continuación, elige el DataSync agente que se conecte al sistema de almacenamiento de objetos.

Algunas transferencias no requieren agentes. En otros casos, es posible que desee utilizar más de un agente. Para obtener más información, consulte [Situaciones en las que no necesita un DataSync agente](#) y [Uso de varios DataSync agentes](#).

8. Para configurar la conexión al servidor de almacenamiento de objetos, expanda Ajustes adicionales y haga lo siguiente:
 - a. En Protocolo del servidor, elija HTTP o HTTPS.
 - b. En Puerto del servidor, utilice un puerto predeterminado (80 para HTTP o 443 para HTTPS) o especifique un puerto personalizado si es necesario.
 - c. En el caso del Certificado, si el sistema de almacenamiento de objetos utiliza una entidad de certificación (CA) privada o autofirmada, seleccione Elegir archivo y especifique un único .pem archivo con una cadena de certificados completa.

La cadena de certificados puede incluir:

- El certificado del sistema de almacenamiento de objetos
- Todos los certificados intermedios (si los hay)
- El certificado raíz de la CA firmante

Puede concatenar sus certificados en un archivo `.pem` (que puede tener un máximo de 32 768 bytes antes de la codificación base64). El siguiente comando `cat` de ejemplo crea un archivo `object_storage_certificates.pem` que incluye tres certificados:

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

9. Si el servidor de almacenamiento de objetos requiere credenciales para acceder, seleccione **Requiere credenciales** e introduzca la clave de acceso que utiliza para acceder al depósito. A continuación, introduzca la clave secreta directamente o especifique un AWS Secrets Manager secreto que contenga la clave. Para obtener más información, consulte [Proporcionar credenciales para las ubicaciones de almacenamiento](#).

La clave de acceso y la clave secreta pueden ser un nombre de usuario y una contraseña, respectivamente.

10. (Opcional) Seleccione **Añadir etiqueta** para etiquetar su ubicación.

Las etiquetas son pares de clave-valor que le ayudan a administrar, filtrar y buscar sus recursos de DataSync. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

11. Seleccione **Crear ubicación**.

Uso del AWS CLI

1. Copie el siguiente 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 los parámetros en el comando de la siguiente manera:

- `--server-hostname`: especifique el nombre de dominio o la dirección IP del servidor de almacenamiento de objetos.
 - `--bucket-name`: especifique el nombre del bucket del servidor de almacenamiento de objetos al que va a transferir o desde el que va a realizar la transferencia.
3. (Opcional) Añada cualquiera de los siguientes parámetros al comando:
- `--agent-arns`— Especifique los DataSync agentes que desea conectar al servidor de almacenamiento de objetos.
 - `--server-port`: especifica el puerto en el que el servidor de almacenamiento de objetos acepta el tráfico de red entrante (por ejemplo, el puerto 443).
 - `--server-protocol`: especifica el protocolo (HTTP oHTTPS) que usa el servidor de almacenamiento de objetos para comunicarse.
 - `--access-key`: especifica la clave de acceso (por ejemplo, un nombre de usuario) si se requieren credenciales para autenticarse en el servidor de almacenamiento de objetos.
 - `--secret-key`: especifica la clave secreta (por ejemplo, una contraseña) si se requieren credenciales para autenticarse en el servidor de almacenamiento de objetos.

También puede proporcionar parámetros adicionales para proteger sus claves mediante AWS Secrets Manager. Para obtener más información, consulte [Proporcionar credenciales para las ubicaciones de almacenamiento](#).

- `--server-certificate`— Especifica una cadena de certificados DataSync para autenticarse en el sistema de almacenamiento de objetos si el sistema utiliza una autoridad de certificación (CA) privada o autofirmada. Debe especificar un único archivo `.pem` con una cadena de certificados completa (por ejemplo, `file:///home/user/.ssh/object_storage_certificates.pem`).

La cadena de certificados puede incluir:

- El certificado del sistema de almacenamiento de objetos
- Todos los certificados intermedios (si los hay)
- El certificado raíz de la CA firmante

Puede concatenar sus certificados en un archivo `.pem` (que puede tener un máximo de 32 768 bytes antes de la codificación base64). El siguiente comando `cat` de ejemplo crea un archivo `object_storage_certificates.pem` que incluye tres certificados:


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

- `--subdirectory`: especifica el prefijo de objeto del servidor de almacenamiento de objetos.

DataSync solo copia los objetos con este prefijo.

- `--tags`: especifica el par clave-valor que representa una etiqueta que desea agregar al recurso.

Las etiquetas le ayudan a administrar, filtrar y buscar sus recursos. Le recomendamos crear una etiqueta de nombre para su ubicación.

4. Ejecute el comando `create-location-object-storage`.

Recibirá una respuesta que le mostrará el ARN de ubicación que acaba de crear.

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

Transferir al AWS almacenamiento o desde él con AWS DataSync

Con AWS DataSync, puede transferir datos hacia o desde varios servicios de AWS almacenamiento. Para obtener más información, consulta [¿Dónde puedo transferir mis datos DataSync?](#)

Temas

- [Configuración de AWS DataSync transferencias con Amazon S3](#)
- [Configuración de AWS DataSync transferencias con Amazon EFS](#)
- [Configurar las transferencias con el servidor FSx de archivos de Windows](#)
- [Configurar DataSync las transferencias con FSx for Lustre](#)
- [Configuración de DataSync transferencias con Amazon FSx para OpenZFS](#)
- [Configuración de transferencias con Amazon FSx para NetApp ONTAP](#)

Configuración de AWS DataSync transferencias con Amazon S3

Para transferir datos a o desde su bucket de Amazon S3, debe crear una ubicación de AWS DataSync transferencia. DataSync puede usar esta ubicación como fuente o destino para transferir datos.

Proporcionar DataSync acceso a los depósitos de S3

DataSync necesita acceder al depósito de S3 al que se está transfiriendo o desde el que se está transfiriendo. Para ello, debe crear un rol AWS Identity and Access Management (de IAM) que DataSync asuma los permisos necesarios para acceder al bucket. A continuación, debe especificar este rol al [crear su ubicación de Amazon S3 para DataSync](#).

Contenido

- [Permisos necesarios](#)
- [Crear un rol de IAM para acceder DataSync a su ubicación de Amazon S3](#)
- [Acceso a buckets de S3 mediante el cifrado del servidor](#)
- [Acceso a buckets S3 restringidos](#)
- [Acceso a los buckets de S3 con acceso restringido a la VPC](#)

Permisos necesarios

Los permisos que necesita su función de IAM pueden depender de si el bucket es una ubicación de DataSync origen o de destino. Amazon S3 en Outposts requiere un conjunto de permisos diferente.

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"
    }
]
}

```

Crear un rol de IAM para acceder DataSync a su ubicación de Amazon S3

Al [crear su ubicación de Amazon S3](#) en la consola, DataSync puede crear y asumir automáticamente una función de IAM que normalmente tenga los permisos adecuados para acceder a su bucket de S3.

En algunas situaciones, es posible que tengas que crear este rol manualmente (por ejemplo, accediendo a los buckets con niveles de seguridad adicionales o realizando una transferencia desde o hacia un bucket situado en otro Cuentas de AWS).

Crear manualmente un rol de IAM para DataSync

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación situado a la izquierda, en Administración de acceso, elija Roles y luego Crear rol.
3. En la página Seleccionar entidad de confianza, en Tipo de entidad de confianza, elija Servicio de AWS.
4. En Caso de uso, elija una opción DataSync en la lista desplegable y seleccione. DataSync Elija Siguiente.
5. En la página Agregar permisos, elija Siguiente. Introduzca un nombre de rol y elija Crear rol.
6. En la página Roles, busque el rol que acaba de crear y seleccione el nombre.

7. En la página de detalles del rol, elija la pestaña Permisos. Elija Agregar permisos y luego Crear política insertada.
8. Seleccione la pestaña JSON y [añada los permisos necesarios](#) para acceder a su bucket en el editor de políticas.
9. Elija Siguiente. Escriba un nombre para la política y elija Crear política.
10. (Recomendado) Para evitar el [problema del suplente confuso entre servicios](#), haga lo siguiente:
 - a. En la página de detalles del rol, elija la pestaña Relaciones de confianza. Elija Editar la política de confianza.
 - b. Actualice la política de confianza mediante el siguiente ejemplo, que incluye las claves de contexto de condición global de `aws:SourceArn` y `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. Elija Actualizar política.

Puede especificar este rol al crear su ubicación de Amazon S3.

Acceso a buckets de S3 mediante el cifrado del servidor

DataSync puede transferir datos a o desde depósitos de [S3 que utilizan cifrado del lado del servidor](#). El tipo de clave de cifrado que utiliza un depósito puede determinar si se necesita una política personalizada que permita acceder DataSync al depósito.

Cuando lo utilices DataSync con buckets de S3 que utilizan cifrado del lado del servidor, recuerda lo siguiente:

- Si su depósito de S3 está cifrado con una clave AWS gestionada, DataSync podrá acceder a los objetos del depósito de forma predeterminada si todos sus recursos se encuentran en los mismos recursos. Cuenta de AWS
- Si el bucket de S3 está cifrado con una clave gestionada por el cliente AWS Key Management Service (AWS KMS) (SSE-KMS), la [política de la clave](#) debe incluir la función de IAM que se DataSync utiliza para acceder al bucket.
- Si el bucket de S3 está cifrado con una clave SSE-KMS gestionada por el cliente y se encuentra en otra Cuenta de AWS, DataSync necesitará permiso para acceder al bucket de la otra. Cuenta de AWS Para hacerlo, haga lo siguiente:
 - En la función de IAM que DataSync utilice, debe especificar la clave SSE-KMS del depósito multicuenta mediante el nombre de recurso de Amazon (ARN) completo de la clave. Se trata del mismo ARN de clave que se utiliza para configurar el [cifrado predeterminado](#) del bucket. En esta situación, no puede especificar el ID de la clave, el nombre de alias o el ARN del alias.

El siguiente es un ejemplo de clave de ARN:

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

Para obtener más información sobre cómo especificar las claves de KMS en las declaraciones de política de IAM, consulte la [Guía para desarrolladores de AWS Key Management Service](#).

- [En la política de claves de SSE-KMS, especifique la función de IAM que utiliza. DataSync](#)
- Si el bucket de S3 está cifrado con una AWS KMS clave gestionada por el cliente (DSSE-KMS) para el cifrado de doble capa en el servidor, la [política de la clave debe incluir la función de IAM](#) que se utiliza para acceder al bucket. DataSync (Tenga en cuenta que DSSE-KMS no admite las [claves de bucket de S3](#), lo que puede reducir los costes de las solicitudes). AWS KMS
- Si su depósito de S3 está cifrado con una clave de cifrado proporcionada por el cliente (SSE-C), no podrá acceder a este depósito. DataSync

Ejemplo: política de claves SSE-KMS para DataSync

El siguiente ejemplo es una [política de claves](#) para una clave SSE-KMS administrada por el cliente. La política está asociada a un bucket de S3 que utiliza cifrado del servidor.

Si quiere usar este ejemplo, sustituya estos valores por los suyos:

- *account-id*— Tu. Cuenta de AWS
- *admin-role-name*— El nombre del rol de IAM que puede administrar la clave.
- *datasync-role-name*— El nombre de la función de IAM que permite DataSync utilizar la clave al acceder al 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": "*"
}
]
}

```

Acceso a buckets S3 restringidos

Si necesita realizar una transferencia hacia o desde un bucket de S3 que normalmente deniega todo acceso, puede editar la política del bucket para que solo DataSync pueda acceder al bucket durante la transferencia.

Ejemplo: permitir el acceso en función de los roles de IAM

1. Copie la siguiente política de bucket de S3.

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. En la política, sustituya los valores siguientes:

- *amzn-s3-demo-bucket*: especifique el nombre del bucket de S3 restringido.
- *datasync-iam-role-id*— Especifique el ID del [rol de IAM que se DataSync utiliza](#) para acceder al bucket.

Ejecute el siguiente AWS CLI comando para obtener el ID del rol de IAM:

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

En el resultado, busque el valor RoleId:

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

- *your-iam-role-id*— Especifique el ID del rol de IAM que utilizará para crear la DataSync ubicación del bucket.

Ejecute el siguiente comando para obtener la ID del rol de IAM:

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

En el resultado, busque el valor RoleId:

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

3. [Añada esta política](#) a la política de su bucket de S3.
4. Cuando termines de usar DataSync el segmento restringido, elimina las condiciones para ambos roles de IAM de la política del segmento.

Acceso a los buckets de S3 con acceso restringido a la VPC

Un bucket de Amazon S3 que [limite el acceso a puntos de enlace de nube privada virtual \(VPC\) específicos o VPCs que impida](#) la transferencia hacia o DataSync desde ese bucket. Para habilitar las transferencias en estas situaciones, puede actualizar la política del bucket para incluir la función de IAM que [especifique](#) en su ubicación. DataSync

Option 1: Allowing access based on DataSync location role ARN

En la política de bucket de S3, puede especificar el nombre de recurso de Amazon (ARN) de la función de IAM de su DataSync ubicación.

El siguiente ejemplo es una política de bucket de S3 que deniega el acceso a todas las personas excepto a dos VPCs (`vpc-1234567890abcdef0` y `vpc-abcdef01234567890`). Sin embargo, la política también incluye la clave [ArnNotLikeIfExists](#) condition y [aws: PrincipalArn](#) condition, que permiten que el ARN de un rol de DataSync ubicación acceda al 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

En la política de bucket de S3, puede especificar una etiqueta asociada a la función de IAM de su DataSync ubicación.

El siguiente ejemplo es una política de bucket de S3 que deniega el acceso a todas las personas excepto a dos VPCs (`vpc-1234567890abcdef0` y `vpc-abcdef01234567890`). Sin embargo, la política también incluye la clave `StringNotEqualsIfExists` condition y `aws: PrincipalTag` condition, que permiten al principal disponer de la clave `exclude-from-vpc-restriction` y el valor de la etiqueta `true`. Puedes probar un enfoque similar en tu política de segmentos especificando una etiqueta asociada a tu rol de DataSync ubicación.

```
{
  "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"
        }
      }
    }
  ]
}
```

}

Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3

Cuando Amazon S3 es su ubicación de destino, DataSync puede transferir sus datos directamente a una [clase de almacenamiento de Amazon S3](#) específica.

Algunas clases de almacenamiento tienen comportamientos que pueden afectar los costos de almacenamiento de Amazon S3. Cuando se utilizan clases de almacenamiento que pueden generar cargos adicionales por sobrescribir, eliminar o recuperar objetos, los cambios en los datos o metadatos de los objetos conllevan dichos cargos. Para obtener más información, consulte [Precios de Amazon S3](#).

Important

Los objetos nuevos transferidos a una ubicación de destino de Amazon S3 se almacenan con la clase de almacenamiento que especificó al [crear la ubicación](#).

De forma predeterminada, DataSync conserva la clase de almacenamiento de los objetos existentes en la ubicación de destino, a menos que configure la tarea para [transferir todos los datos](#). En esas situaciones, la clase de almacenamiento que especifique al crear la ubicación se utilizará para todos los objetos.

Clase de almacenamiento de Amazon S3	Consideraciones
S3 Standard	Elija Estándar de S3 para almacenar los archivos de acceso frecuente de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente. Este es el valor predeterminado si no especifica ninguna clase de almacenamiento.
S3 Intelligent-Tiering	Elija S3 Intelligent-Tiering para optimizar los costos de almacenamiento moviendo automáticamente los datos a la capa de acceso de almacenamiento más rentable.

Clase de almacenamiento de Amazon S3	Consideraciones
	Se paga un cargo mensual por objeto almacenado en la clase de almacenamiento S3 Intelligent-Tiering. Este cargo de Amazon S3 incluye la supervisión de los patrones de acceso a los datos y el movimiento de objetos entre niveles.
S3 Standard-IA	Elija S3 Standard-IA para almacenar los objetos a los que se accede con poca frecuencia de forma redundante en varias zonas de disponibilidad que se encuentran distanciadas geográficamente. Los objetos almacenados en la clase de almacenamiento S3 Standard-IA pueden incurrir en cargos adicionales de sobreescritura, eliminación o recuperación. Considere la frecuencia con la que estos objetos cambian, el tiempo que tiene previsto conservar estos objetos y la frecuencia con la que necesita obtener acceso a ellos. Los cambios en los datos o metadatos del objeto equivalen a eliminar un objeto y crear uno nuevo para reemplazarlo. Esto se traduce en cargos adicionales por los objetos almacenados en la clase de almacenamiento S3 Standard-IA. Los objetos de menos de 128 KB son menores que el cargo de capacidad mínimo por objeto en la clase de almacenamiento S3 Standard-IA. Estos objetos se almacenan en la clase de almacenamiento S3 Standard.

Clase de almacenamiento de Amazon S3	Consideraciones
S3 One Zone-IA	Elija S3 One Zone-IA para almacenar los objetos a los que se accede con poca frecuencia en una única zona de disponibilidad. Los objetos almacenados en la clase de almacenamiento S3 One Zone-IA pueden incurrir en cargos adicionales de sobreescritura, eliminación o recuperación. Considere la frecuencia con la que estos objetos cambian, el tiempo que tiene previsto conservar estos objetos y la frecuencia con la que necesita obtener acceso a ellos. Los cambios en los datos o metadatos del objeto equivalen a eliminar un objeto y crear uno nuevo para reemplazarlo. Esto se traduce en cargos adicionales por los objetos almacenados en la clase de almacenamiento S3 One Zone-IA. Los objetos de menos de 128 KB son menores que el cargo de capacidad mínimo por objeto en la clase de almacenamiento S3 One Zone-IA. Estos objetos se almacenan en la clase de almacenamiento S3 Standard.

Clase de almacenamiento de Amazon S3	Consideraciones
S3 Glacier Instant Retrieval	Elija S3 Glacier Instant Retrieval para archivar los objetos a los que se accede con poca frecuencia, pero que requieren recuperación en milisegundos. Los datos almacenados en la clase de almacenamiento S3 Glacier Instant Retrieval ofrecen un ahorro de costos en comparación con la clase de almacenamiento S3 Standard-IA, con la misma latencia y rendimiento. Aunque S3 Glacier Instant Retrieval tiene costos de acceso a datos más altos que S3 Standard-IA. Los objetos almacenados en S3 Glacier Instant Retrieval pueden incurrir en cargos adicionales de sobrescritura, eliminación o recuperación. Considere la frecuencia con la que estos objetos cambian, el tiempo que tiene previsto conservar estos objetos y la frecuencia con la que necesita obtener acceso a ellos. Los cambios en los datos o metadatos del objeto equivalen a eliminar un objeto y crear uno nuevo para reemplazarlo. Esto se traduce en cargos adicionales por los objetos almacenados en la clase de almacenamiento S3 Glacier Instant Retrieval. Los objetos de menos de 128 KB son menores que el cargo de capacidad mínimo por objeto en la clase de almacenamiento S3 Glacier Instant Retrieval. Estos objetos se almacenan en la clase de almacenamiento S3 Standard.

Clase de almacenamiento de Amazon S3	Consideraciones
S3 Glacier Flexible Retrieval	Elija S3 Glacier Flexible Retrieval para ver más archivos activos. Los objetos almacenados en S3 Glacier Flexible Retrieval pueden incurrir en cargos adicionales de sobreescritura, eliminación o recuperación. Considere la frecuencia con la que estos objetos cambian, el tiempo que tiene previsto conservar estos objetos y la frecuencia con la que necesita obtener acceso a ellos. Los cambios en los datos o metadatos del objeto equivalen a eliminar un objeto y crear uno nuevo para reemplazarlo. Esto se traduce en cargos adicionales por los objetos almacenados en la clase de almacenamiento S3 Glacier Flexible Retrieval. La clase de almacenamiento S3 Glacier Flexible Retrieval requiere 40 KB de metadatos adicionales por cada objeto archivado. DataSync coloca los objetos de menos de 40 KB en la clase de almacenamiento S3 Standard. Debe restaurar los objetos archivados en esta clase de almacenamiento para DataSync poder leerlos. Para obtener más información, consulte Trabajar con objetos archivados en la Guía del usuario de Amazon S3. Cuando utilice S3 Glacier Flexible Retrieval, elija la opción de tarea Verificar solo los datos transferidos para comparar las sumas de comprobación de datos y metadatos al final de la transferencia. No se puede usar la opción Verificar todos los datos del destino en esta clase de almacenamiento, ya que requiere recuperar todos los objetos actuales del destino.

Clase de almacenamiento de Amazon S3	Consideraciones
S3 Glacier Deep Archive	Elija S3 Glacier Deep Archive para archivar los objetos para la retención de datos y la conservación digital a largo plazo donde se accede a los datos una o dos veces al año. Los objetos almacenados en S3 Glacier Deep Archive pueden incurrir en cargos adicionales de sobreescritura, eliminación o recuperación. Considere la frecuencia con la que estos objetos cambian, el tiempo que tiene previsto conservar estos objetos y la frecuencia con la que necesita obtener acceso a ellos. Los cambios en los datos o metadatos del objeto equivalen a eliminar un objeto y crear uno nuevo para reemplazarlo. Esto se traduce en cargos adicionales por los objetos almacenados en la clase de almacenamiento S3 Glacier Deep Archive. La clase de almacenamiento S3 Glacier Deep Archive requiere 40 KB de metadatos adicionales por cada objeto archivado. DataSync coloca los objetos de menos de 40 KB en la clase de almacenamiento S3 Standard. Debe restaurar los objetos archivados en esta clase de almacenamiento para DataSync poder leerlos. Para obtener más información, consulte Trabajar con objetos archivados en la Guía del usuario de Amazon S3. Cuando utilice S3 Glacier Deep Archive, elija la opción de tarea Verificar solo los datos transferidos para comparar las sumas de comprobación de datos y metadatos al final de la transferencia. No se puede usar la opción Verificar todos los datos del destino en esta clase de almacenamiento, ya que requiere recuperar todos los objetos actuales del destino.
S3 Outposts	La clase de almacenamiento para Amazon S3 en Outposts.

Evaluar los costos de las solicitudes de S3 al usar DataSync

Con las ubicaciones de Amazon S3, incurrirá en costos relacionados con las solicitudes de API de S3 realizadas por DataSync. Esta sección puede ayudarle a entender cómo se DataSync utilizan estas solicitudes y cómo pueden afectar a sus [costes de Amazon S3](#).

Temas

- [Solicitudes de S3 realizadas por DataSync](#)
- [Consideraciones sobre costos](#)

Solicitudes de S3 realizadas por DataSync

En la siguiente tabla se describen las solicitudes de S3 que se DataSync pueden realizar al copiar datos a o desde una ubicación de Amazon S3.

Solicitud de S3	¿Cómo lo DataSync usa
ListObjectV2	DataSync hace al menos una LIST solicitud para cada objeto que termine en una barra diagonal (/) para enumerar los objetos que comienzan con ese prefijo. Esta solicitud se invoca durante la fase de preparación de una tarea.
HeadObject	DataSync realiza HEAD solicitudes para recuperar los metadatos de los objetos durante las fases de preparación y verificación de una tarea. Puede haber varias HEAD solicitudes por objeto en función de cómo desee DataSync verificar la integridad de los datos que transfiere .
GetObject	DataSync realiza GET solicitudes para leer datos de un objeto durante la fase de transferencia de una tarea. Puede haber varias solicitudes GET de objetos grandes.
GetObjectTagging	Si configuras la tarea para copiar etiquetas de objetos , DataSync realiza estas GET solicitudes para comprobar si hay etiquetas de objetos durante las fases de preparación y transferencia de la tarea.

Solicitud de S3	¿Cómo lo DataSync usa
PutObject	DataSync realiza PUT solicitudes para crear objetos y prefijos en un bucket de S3 de destino durante la fase de transferencia de una tarea. Como DataSync utiliza la función de carga multiparte de Amazon S3 , puede haber varias PUT solicitudes de objetos grandes. Para minimizar los costos de almacenamiento, le recomendamos que utilice una configuración de ciclo de vida para detener las cargas incompletas de varias partes.
PutObjectTagging	Si sus objetos de origen tienen etiquetas y usted configura su tarea para copiar las etiquetas de los objetos , DataSync realiza estas PUT solicitudes al transferirlas .
CopyObject	DataSync COPYsolicita crear una copia de un objeto solo si los metadatos de ese objeto cambian. Esto puede suceder si originalmente copió los datos al bucket de S3 con otro servicio o herramienta que no transfirió sus metadatos.

Consideraciones sobre costos

DataSync realiza solicitudes de S3 en depósitos de S3 cada vez que ejecuta la tarea. Esto puede provocar que los cargos se acumulen en determinadas situaciones. Por ejemplo:

- Con frecuencia transfiere objetos desde o hacia un bucket de S3.
- Puede que no transfiera muchos datos, pero su bucket de S3 contiene muchos objetos. En este escenario, los cargos seguirán siendo elevados, ya DataSync que realiza solicitudes de S3 en cada uno de los objetos del bucket.
- Estás realizando transferencias entre depósitos de S3, al igual que DataSync las solicitudes de S3 en el origen y en el destino.

Para ayudar a minimizar los costos relacionados con las solicitudes de S3 DataSync, tenga en cuenta lo siguiente:

Temas

- [¿Qué clases de almacenamiento de S3 utilizo?](#)
- [¿Con qué frecuencia debo transferir mis datos?](#)

¿Qué clases de almacenamiento de S3 utilizo?

Los cargos por solicitud de S3 pueden variar en función de la clase de almacenamiento de Amazon S3 que estén utilizando sus objetos, en particular en el caso de las clases que archivan objetos (como S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval y S3 Glacier Deep Archive).

A continuación, se muestran algunos escenarios en los que las clases de almacenamiento pueden afectar a los cargos por solicitudes de S3 cuando se utilizan DataSync:

- Cada vez que ejecuta una tarea, DataSync realiza HEAD solicitudes para recuperar los metadatos del objeto. Estas solicitudes generan cargos incluso si no se mueve ningún objeto. El impacto de estas solicitudes en tu factura depende de la clase de almacenamiento que utilicen tus objetos y del número de objetos que DataSync escanees.
- Si ha trasladado objetos a la clase de almacenamiento S3 Glacier Instant Retrieval (directamente o mediante una configuración del ciclo de vida de un bucket), las solicitudes en los objetos de esta clase son más caras que las de los objetos en otras clases de almacenamiento.
- Si configura la DataSync tarea para [verificar que las ubicaciones de origen y destino estén completamente sincronizadas](#), habrá GET solicitudes para cada objeto en todas las clases de almacenamiento (excepto S3 Glacier Flexible Retrieval y S3 Glacier Deep Archive).
- Además de las solicitudes GET, se incurre en costos de recuperación de datos para los objetos de la clase de almacenamiento S3 Standard-IA, S3 One Zone-IA o S3 Glacier Instant Retrieval.

Para obtener más información, consulte [Precios de Amazon S3](#).

¿Con qué frecuencia debo transferir mis datos?

Si necesita mover datos de forma periódica, piense en un [cronograma](#) que no ejecute más tareas de las que necesita.

También puede considerar limitar el alcance de sus transferencias. Por ejemplo, puede configurarlo DataSync para centrarse en los objetos con determinados prefijos o [filtrar los datos que](#) se

transfieren. Estas opciones pueden ayudar a reducir la cantidad de solicitudes de S3 que se realizan cada vez que ejecuta la DataSync tarea.

Consideraciones de objetos con las transferencias de Amazon S3

- Si va a realizar una transferencia desde un bucket de S3, utilice la [Lente de almacenamiento de S3](#) para determinar cuántos objetos va a mover.
- Al realizar transferencias entre depósitos de S3, le recomendamos que utilice el [modo de tareas mejorado](#), ya que no está sujeto a [las cuotas](#) de DataSync tareas.
- DataSync es posible que no transfiera un objeto cuyo nombre contenga caracteres no estándares. Para obtener más información, consulte [object key naming guidelines](#) en la Guía del usuario de Amazon S3.
- Cuando lo utilice DataSync con un bucket de S3 que utilice el control de [versiones](#), recuerde lo siguiente:
 - Al transferirlo a un bucket de S3, DataSync crea una nueva versión de un objeto si ese objeto se modifica en el origen. Esto se traduce en cargos adicionales.
 - Un objeto tiene una versión diferente IDs en los buckets de origen y destino.
- Tras transferir inicialmente los datos de un bucket de S3 a un sistema de archivos (por ejemplo, NFS o Amazon FSx), las siguientes ejecuciones de la misma DataSync tarea no incluirán objetos que se hayan modificado pero que tengan el mismo tamaño que tenían durante la primera transferencia.

Crear la ubicación de transferencia para un depósito de uso general de Amazon S3

Para crear una ubicación para su transferencia, necesita un depósito de uso general de S3 existente. Si no tiene uno, consulte la [Guía del usuario de Amazon S3](#).

Important

Antes de crear su ubicación, asegúrese de leer las siguientes secciones:

- [Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3](#)
- [Evaluar los costos de las solicitudes de S3 al usar DataSync](#)

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. Para el tipo de ubicación, elija Amazon S3 y, a continuación, elija Bucket de uso general.
4. En el caso del URI de S3, introduzca o elija el depósito y el prefijo que desee utilizar para su ubicación.

Warning

DataSync no puede transferir objetos con un prefijo que comience con una barra (/) o que incluya ///./, o patrones ././ Por ejemplo:

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

5. Para la clase de almacenamiento S3, cuando se utilice como destino, elija la clase de almacenamiento que desee que usen sus objetos cuando Amazon S3 sea un destino de transferencia.

Para obtener más información, consulte [Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3](#).

6. En Rol de IAM, realice una de las operaciones siguientes:
 - Elija Generar automáticamente DataSync para crear automáticamente un rol de IAM con los permisos necesarios para acceder al bucket de S3.

Si DataSync anteriormente creó un rol de IAM para este bucket de S3, ese rol se elige de forma predeterminada.

 - Elija un rol de IAM personalizado que haya creado. Para obtener más información, consulte [Crear un rol de IAM para acceder DataSync a su ubicación de Amazon S3](#).
7. (Opcional) Selecciona Añadir nueva etiqueta para etiquetar tu ubicación de Amazon S3.

Las etiquetas le ayudan a administrar, filtrar y buscar sus recursos. Le recomendamos crear una etiqueta de nombre para su ubicación.

8. Seleccione Crear ubicación.

Usando el AWS CLI

1. Copie el siguiente 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. Para `--s3-bucket-arn`, especifique el ARN del bucket de S3 que desea usar como ubicación.
3. Para `--s3-storage-class`, especifique la clase de almacenamiento que desea que utilicen los objetos cuando Amazon S3 sea un destino de transferencia.
4. Para `--s3-config`, especifique el ARN del rol de IAM que DataSync necesita acceder a su bucket.

Para obtener más información, consulte [Crear un rol de IAM para acceder DataSync a su ubicación de Amazon S3](#).

5. Para `--subdirectory` ello, especifique un prefijo en el depósito de S3 que DataSync lea o escriba en él (en función de si el depósito es una ubicación de origen o de destino).

Warning

DataSync no puede transferir objetos con un prefijo que comience con una barra (/) o que incluya `///`, `./`, o patrones `/. ./`. Por ejemplo:

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

6. Ejecute el comando `create-location-s3`.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la ubicación que creó. Por ejemplo:

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

Puede utilizar esta ubicación como origen o destino de la tarea. DataSync

Crear tu ubicación de transferencia para un bucket de S3 en Outposts

Para crear una ubicación para tu transferencia, necesitas un depósito existente de Amazon S3 on Outposts. Si no tienes uno, consulta la Guía del [usuario de Amazon S3 on Outposts](#).

También necesita un DataSync agente. Para obtener más información, consulte [Despliegue de su agente en AWS Outposts](#).

Al realizar una transferencia desde un prefijo de bucket de S3 en Outposts que contiene un conjunto de datos grande (como cientos de miles o millones de objetos), es posible que se agote el tiempo de espera de tu DataSync tarea. Para evitarlo, considera la posibilidad de usar un [DataSync manifiesto](#), que te permita especificar los objetos exactos que necesitas transferir.

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. Para el tipo de ubicación, elige Amazon S3 y, a continuación, elige el bucket Outposts.
4. Para el bucket de S3, elige un punto de acceso de Amazon S3 que pueda acceder a tu bucket de S3 on Outposts.

Para obtener más información, consulte la [Guía del usuario de Amazon S3](#).

5. Para la clase de almacenamiento S3, cuando se utilice como destino, elija la clase de almacenamiento que desee que usen sus objetos cuando Amazon S3 sea un destino de transferencia.

Para obtener más información, consulte [Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3](#). DataSync de forma predeterminada, utiliza la clase de almacenamiento S3 Outposts para Amazon S3 en Outposts.

6. En el caso de los agentes, especifique el nombre de recurso de Amazon (ARN) del DataSync agente en su Outpost.
7. En Carpeta, introduzca un prefijo en el bucket de S3 que DataSync lea o escriba en (dependiendo de si el bucket es una ubicación de origen o de destino).

 Warning

DataSync no puede transferir objetos con un prefijo que comience con una barra (/) o que incluya ///./, o patrones. /./ Por ejemplo:

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

8. En Rol de IAM, realice una de las operaciones siguientes:
 - Elija Generar automáticamente DataSync para crear automáticamente un rol de IAM con los permisos necesarios para acceder al bucket de S3.

Si DataSync anteriormente creó un rol de IAM para este bucket de S3, ese rol se elige de forma predeterminada.

- Elija un rol de IAM personalizado que haya creado. Para obtener más información, consulte [Crear un rol de IAM para acceder DataSync a su ubicación de Amazon S3](#).
9. (Opcional) Selecciona Añadir nueva etiqueta para etiquetar tu ubicación de Amazon S3.

Las etiquetas le ayudan a administrar, filtrar y buscar sus recursos. Le recomendamos crear una etiqueta de nombre para su ubicación.

10. Seleccione Crear ubicación.

Usando el AWS CLI

1. Copie el siguiente 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 el ARN de un punto de acceso de Amazon S3 que pueda acceder a su bucket de S3 on Outposts.

Para obtener más información, consulte la [Guía del usuario de Amazon S3](#).

3. Para `--s3-storage-class`, especifique la clase de almacenamiento que desea que utilicen los objetos cuando Amazon S3 sea un destino de transferencia.

Para obtener más información, consulte [Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3](#). DataSync de forma predeterminada, usa la clase de almacenamiento S3 Outposts para S3 en Outposts.

4. Para `--s3-config`, especifique el ARN del rol de IAM que DataSync necesita acceder a su bucket.

Para obtener más información, consulte [Crear un rol de IAM para acceder DataSync a su ubicación de Amazon S3](#).

5. Para `--subdirectory` ello, especifique un prefijo en el depósito de S3 que DataSync lea o escriba en él (en función de si el depósito es una ubicación de origen o de destino).

Warning

DataSync no puede transferir objetos con un prefijo que comience con una barra (/) o que incluya `///./`, o patrones `/. ./`. Por ejemplo:

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

6. Para `--agent-arns`, especifique el ARN del DataSync agente en su puesto de avanzada.

7. Ejecute el comando `create-location-s3`.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la ubicación que creó. Por ejemplo:

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

Puede usar esta ubicación como origen o destino para su DataSync tarea.

Amazon S3 transfiere entre Cuentas de AWS

Con DataSync ella, puede mover datos hacia o desde depósitos de S3 en [diferentes Cuentas de AWS](#) ubicaciones. Para obtener más información, consulte los siguientes tutoriales:

- [Transferencia de datos desde el almacenamiento local a Amazon S3 a través de Cuentas de AWS](#)
- [Transferencia de datos de Amazon S3 a Amazon S3 a través Cuentas de AWS](#)

Amazon S3 transfiere entre operaciones comerciales y AWS GovCloud (US) Regions

De forma predeterminada, DataSync no se transfiere entre depósitos de S3 en depósitos comerciales y AWS GovCloud (US) Regions. Sin embargo, puede seguir configurando este tipo de transferencia creando una ubicación de almacenamiento de objetos para uno de los buckets de S3 de su transferencia. Puedes realizar este tipo de transferencia con o sin un agente. Si utiliza un agente, la tarea debe estar configurada para el modo básico. Para realizar la transferencia sin un agente, debe utilizar el modo mejorado.

Antes de empezar: asegúrese de entender las implicaciones financieras de la transferencia entre regiones. Para más información, consulte [Precios de AWS DataSync](#).

Contenido

- [Proporcionar DataSync acceso al depósito de tu ubicación de almacenamiento de objetos](#)
- [Crear su DataSync agente \(opcional\)](#)
- [Creación de una ubicación de almacenamiento de objetos para su bucket de S3](#)

Proporcionar DataSync acceso al depósito de tu ubicación de almacenamiento de objetos

Al crear la ubicación de almacenamiento de objetos para esta transferencia, debe proporcionar DataSync las credenciales de un usuario de IAM con permiso para acceder al depósito de S3 de la ubicación. Para obtener más información, consulte [Permisos necesarios](#).

 Warning

Los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo de seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

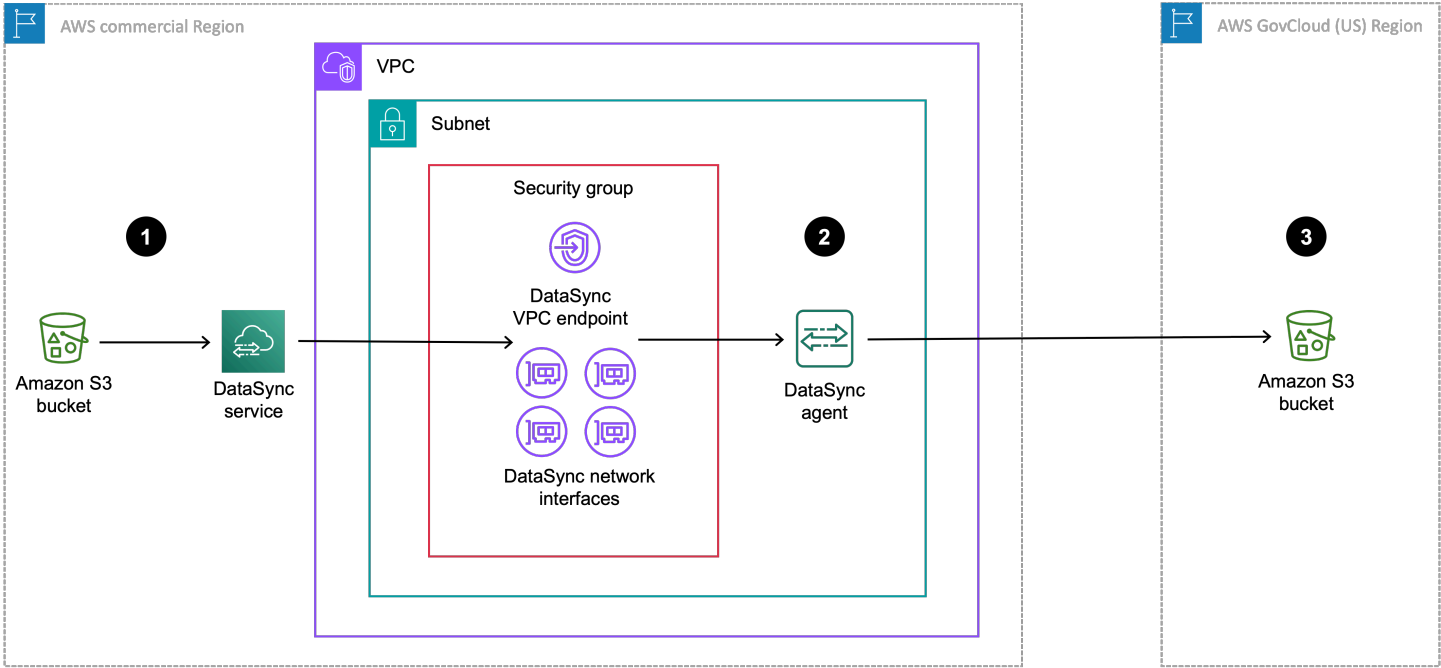
Crear su DataSync agente (opcional)

Si quieres ejecutar tu transferencia en el modo Básico, necesitarás usar un agente. Como te estás transfiriendo de un comercial a otro AWS GovCloud (US) Region, despliegas a tu DataSync agente como una EC2 instancia de Amazon en una de las regiones. Recomendamos que su agente utilice un punto de conexión de servicio de VPC para evitar cargos por transferencia de datos a la Internet pública. Para obtener más información, consulta los [precios EC2 de Amazon Data Transfer](#).

Elija uno de los siguientes escenarios que describen cómo crear un agente en función de la región en la que planea ejecutar la DataSync tarea.

Al ejecutar una DataSync tarea en una región comercial

El siguiente diagrama muestra una transferencia en la que la DataSync tarea y el agente se encuentran en la región comercial.



Referencia	Descripción
1	En la región comercial en la que ejecuta una DataSync tarea, los datos se transfieren desde el depósito de S3 de origen. El bucket de origen está configurado como una ubicación de Amazon S3 en la región comercial.
2	Los datos se transfieren a través del DataSync agente, que se encuentra en la misma VPC y subred donde se encuentran el punto final del servicio de la VPC y las interfaces de red.
3	Los datos se transfieren al bucket de S3 de destino en la AWS GovCloud (US) Region. El bucket de destino está configurado como una ubicación de almacenamiento de objetos en la región comercial.

También puede utilizar esta misma configuración para realizar transferencias en la dirección opuesta de la región AWS GovCloud (US) Region a la comercial.

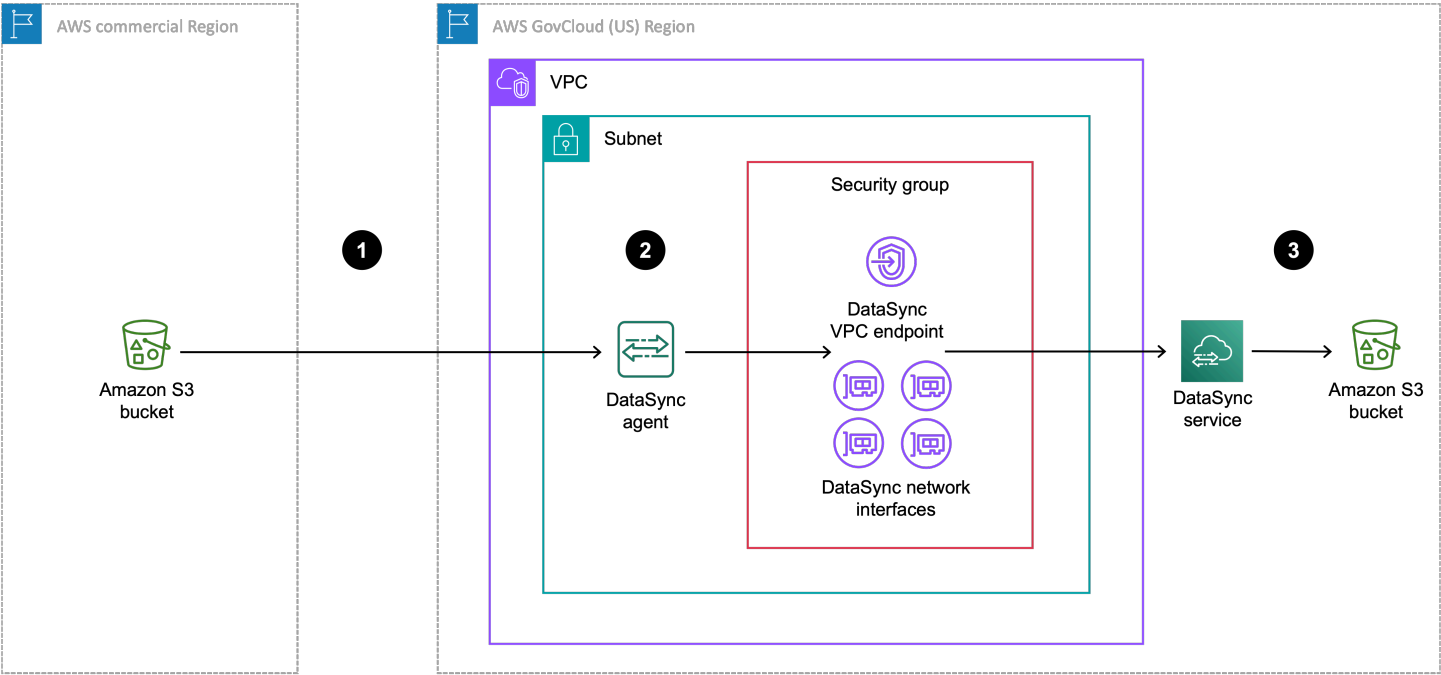
Para crear tu DataSync agente

1. [Despliega un EC2 agente de Amazon](#) en tu región comercial.

2. Configure su agente para que utilice un [punto de conexión de servicio de VPC](#).
3. [Activación del agente](#).

Al ejecutar una DataSync tarea en una región GovCloud (EE. UU.)

El siguiente diagrama muestra una transferencia en la que se encuentran la DataSync tarea y el agente AWS GovCloud (US) Region.



Referencia	Descripción
1	Los datos se transfieren desde el depósito de S3 de origen en la región comercial al AWS GovCloud (US) Region lugar en el que se ejecuta la DataSync tarea. El bucket de origen está configura do como una ubicación de almacenamiento de objetos en el AWS GovCloud (US) Region.
2	En el AWS GovCloud (US) Region, los datos se transfieren a través del DataSync agente en la misma VPC y subred donde se encuentran el punto final del servicio de la VPC y las interfaces de red.
3	Los datos se transfieren al bucket de S3 de destino en la AWS GovCloud (US) Region. El bucket de destino está configurado

Referencia	Descripción
	como una ubicación de Amazon S3 en la AWS GovCloud (US) Region.

También puede utilizar esta misma configuración para realizar transferencias en la dirección opuesta de la región AWS GovCloud (US) Region a la comercial.

Para crear tu DataSync agente

1. [Despliega un EC2 agente de Amazon](#) en tu AWS GovCloud (US) Region.
2. Configure su agente para que utilice un [punto de conexión de servicio de VPC](#).
3. [Activación del agente](#).

Si su conjunto de datos es altamente comprimible, es posible que consiga reducir los costes si crea su agente en una región comercial y ejecuta una tarea en una AWS GovCloud (US) Region. La creación de este agente requiere más de lo normal, incluida la preparación del agente para su uso en una región comercial. Para obtener información sobre cómo crear un agente para esta configuración, consulta el AWS DataSync blog Cómo [introducir y sacar datos AWS GovCloud \(US\) con](#).

Creación de una ubicación de almacenamiento de objetos para su bucket de S3

Necesita una ubicación de almacenamiento de objetos para el depósito de S3 que se encuentre en la región en la que no está ejecutando la DataSync tarea.

Mediante la consola de DataSync

1. Abre la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. Asegúrese de estar en la misma región en la que tiene previsto ejecutar la tarea.
3. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
4. En Tipo de ubicación, seleccione Almacenamiento de objetos.
5. En el caso de los agentes, elige el DataSync agente que creaste para esta transferencia.
6. Para Server, introduzca un punto de conexión de Amazon S3 para su bucket mediante uno de los siguientes formatos:
 - Bucket de región comercial: `s3.your-region.amazonaws.com`

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

Para una lista de puntos de conexión de Amazon S3, consulte la [Referencia general de AWS](#).

7. Para el nombre del bucket, escriba el nombre del bucket de S3.
8. En Carpeta, introduzca un prefijo en el depósito de S3 que DataSync lea o escriba en él (en función de si el depósito es una ubicación de origen o de destino).

 Warning

DataSync no puede transferir objetos con un prefijo que comience con una barra (/) o que incluya `///`, `./`, o patrones `/. ./`. Por ejemplo:

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

9. Seleccione Requiere credenciales y haga lo siguiente:
 - En Clave de acceso, introduzca la clave de acceso de un [usuario de IAM](#) que pueda acceder al bucket.
 - En Clave secreta, introduzca la clave secreta del mismo usuario de IAM.
10. (Opcional) Elija Añadir etiqueta para etiquetar su ubicación.

Las etiquetas le ayudan a administrar, filtrar y buscar sus recursos. Le recomendamos crear una etiqueta de nombre para su ubicación.

11. Seleccione Crear ubicación.

Uso de AWS CLI

1. Copie el siguiente comando `create-location-object-storage`:

```
aws datasync create-location-object-storage \  
  --server-hostname s3-endpoint \  
  --bucket-name amzn-s3-demo-bucket \  
  --location-name my-location
```

```
--agent-arns arn:aws:datasync:your-region:123456789012:agent/  
agent-01234567890deadfb
```

2. Para el parámetro `--server-hostname`, especifique un punto de conexión de Amazon S3 para su bucket mediante uno de los siguientes formatos:

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

En el caso de la región del punto de conexión, asegúrese de especificar la misma región en la que tiene previsto ejecutar la tarea.

Para una lista de puntos de conexión de Amazon S3, consulte la [Referencia general de AWS](#).

3. En el parámetro `--bucket-name`, especifique el nombre del bucket de S3.
4. Para el `--agent-arns` parámetro, especifique el DataSync agente que creó para esta transferencia.
5. Para el parámetro `--access-key`, especifique la clave de acceso para un [usuario de IAM](#) que pueda acceder al bucket.
6. Para el parámetro `--secret-key`, introduzca la clave secreta del mismo usuario de IAM.
7. (Opcional) Para el `--subdirectory` parámetro, especifique un prefijo en el depósito de S3 que DataSync lea o escriba en él (en función de si el depósito es una ubicación de origen o de destino).

Warning

DataSync no puede transferir objetos con un prefijo que comience con una barra (/) o que incluya `///.`, o patrones `/. ./` Por ejemplo:

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

8. (Opcional) Para el parámetro `--tags`, especifique pares clave-valor que representen las etiquetas del recurso de ubicación.

Las etiquetas le ayudan a administrar, filtrar y buscar sus recursos. Le recomendamos crear una etiqueta de nombre para su ubicación.

9. Ejecute el comando `create-location-object-storage`.

Recibirá una respuesta que le mostrará el ARN de ubicación que acaba de crear.

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

Puede utilizar esta ubicación como origen o destino de la tarea. DataSync Para el otro bucket de S3 de esta transferencia, [cree una ubicación de Amazon S3](#).

Pasos a seguir a continuación

Algunos posibles pasos a seguir incluyen:

1. Si es necesario, cree su otra ubicación. Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)
2. [Configure los ajustes de la DataSync tarea](#), como los archivos que desea transferir y cómo gestionar los metadatos, entre otras opciones.
3. [Establezca un cronograma](#) para su DataSync tarea.
4. [Configure la supervisión](#) de su DataSync tarea.
5. [Inicie](#) su tarea.

Configuración de AWS DataSync transferencias con Amazon EFS

Para transferir datos a o desde su sistema de archivos Amazon EFS, debe crear una ubicación de AWS DataSync transferencia. DataSync puede usar esta ubicación como origen o destino para transferir datos.

Proporcionar DataSync acceso a los sistemas de archivos Amazon EFS

[La creación de una ubicación](#) implica entender cómo DataSync puede acceder a su almacenamiento. En el caso de Amazon EFS, DataSync monta el sistema de archivos como usuario raíz desde la nube privada virtual (VPC) [mediante](#) interfaces de red.

Contenido

- [Determinar la subred y los grupos de seguridad para su destino de montaje](#)
- [Acceso a sistemas de archivos restringidos](#)
 - [Crear un rol de DataSync IAM para el acceso al sistema de archivos](#)
 - [Ejemplo de política del sistema de archivos que permite DataSync el acceso](#)

Determinar la subred y los grupos de seguridad para su destino de montaje

Al crear la ubicación, debe especificar la subred y los grupos de seguridad que permiten conectarse DataSync a uno de los [destinos de montaje](#) del sistema de archivos Amazon EFS.

La subred que especifique debe estar ubicada:

- En la misma VPC que el sistema de archivos.
- En la misma zona de disponibilidad que al menos un destino de montaje del sistema de archivos.

Note

No es necesario especificar una subred que incluya un destino de montaje del sistema de archivos.

Los grupos de seguridad que especifique deben permitir el tráfico entrante en el puerto 2049 de NFS. Para obtener información sobre la creación y actualización de grupos de seguridad para sus objetivos de montaje, consulte la [Guía del usuario de Amazon EFS](#).

Especificación de grupos de seguridad asociados a un destino de montaje

Puede especificar un grupo de seguridad asociado a uno de los destinos de montaje del sistema de archivos. Recomendamos este enfoque desde el punto de vista de la administración de la red.

Especificación de grupos de seguridad que no estén asociados a un destino de montaje

También puede especificar un grupo de seguridad que no esté asociado a uno de los destinos de montaje del sistema de archivos. Sin embargo, este grupo de seguridad debe poder comunicarse con el grupo de seguridad de un destino de montaje.

Por ejemplo, así es como puede crear una relación entre el grupo de seguridad D (para DataSync) y el grupo de seguridad M (para el destino de montaje):

- El grupo de seguridad D, que se especifica al crear la ubicación, debe tener una regla que permita las conexiones salientes del puerto NFS 2049 al grupo de seguridad M.
- El grupo de seguridad M, que se asocia al objetivo de montaje, debe permitir el acceso entrante al puerto NFS 2049 desde el grupo de seguridad D.

Cómo encontrar el grupo de seguridad de un objetivo de montaje

Las siguientes instrucciones pueden ayudarle a identificar el grupo de seguridad de un destino de montaje del sistema de archivos Amazon EFS que desea utilizar DataSync para la transferencia.

1. En el AWS CLI, ejecute el siguiente `describe-mount-targets` comando.

```
aws efs describe-mount-targets \  
  --region file-system-region \  
  --file-system-id file-system-id
```

Este comando devuelve información sobre los objetivos de montaje del sistema de archivos (similar al resultado del siguiente ejemplo).

```
{  
  "MountTargets": [  
    {  
      "OwnerId": "111222333444",  
      "MountTargetId": "fsmt-22334a10",  
      "FileSystemId": "fs-123456ab",  
      "SubnetId": "subnet-f12a0e34",  
      "LifecycleState": "available",  
      "IpAddress": "11.222.0.123",  
      "NetworkInterfaceId": "eni-1234a044"  
    }  
  ]  
}
```

2. Anote el valor `MountTargetId` que desea usar.
3. Ejecute el siguiente comando `describe-mount-target-security-groups` usando el `MountTargetId` para averiguar el grupo de seguridad del destino de montaje.

```
aws efs describe-mount-target-security-groups \  
  --region file-system-region \  
  --mount-target-id mount-target-id
```

```
--mount-target-id mount-target-id
```

Debe especificar este grupo de seguridad al [crear su ubicación](#).

Acceso a sistemas de archivos restringidos

DataSync pueden transferirse a o desde los sistemas de archivos de Amazon EFS que restringen el acceso a través de [puntos de acceso](#) y [políticas de IAM](#).

Note

Si DataSync accede a un sistema de archivos de destino a través de un punto de acceso que impone la identidad del usuario, el usuario y el grupo POSIX de los datos de origen no se conservan si configura la DataSync tarea IDs para copiar la propiedad. En su lugar, los archivos y carpetas transferidos se configuran para el usuario y el grupo del punto de acceso. IDs Cuando esto ocurre, se produce un error en la verificación de la tarea porque DataSync detecta una discrepancia entre los metadatos de las ubicaciones de origen y destino.

Contenido

- [Crear un rol de DataSync IAM para el acceso al sistema de archivos](#)
- [Ejemplo de política del sistema de archivos que permite DataSync el acceso](#)

Crear un rol de DataSync IAM para el acceso al sistema de archivos

Si tiene un sistema de archivos Amazon EFS que restringe el acceso mediante una política de IAM, puede crear un rol de IAM que otorgue DataSync permiso para leer o escribir datos en el sistema de archivos. En ese caso, puede que necesite especificar esa función en la [política de su sistema de archivos](#).

Para crear el rol de IAM DataSync

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación situado a la izquierda, en Administración de acceso, elija Roles y luego Crear rol.
3. En la página Seleccionar entidad de confianza, en Tipo de entidad de confianza, elija Política de confianza personalizada.

4. Pegue el siguiente JSON en el editor de políticas:

JSON

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

5. Elija Siguiente. En la página Agregar permisos, elija Siguiente.
6. Introduzca un nombre de rol y elija Crear rol.

Especifique este rol al [crear su ubicación](#).

Ejemplo de política del sistema de archivos que permite DataSync el acceso

El siguiente ejemplo de política del sistema de archivos muestra cómo el acceso a un sistema de archivos de Amazon EFS (identificado en la política como `fs-1234567890abcdef0`) está restringido, pero aún permite el acceso a DataSync través de un rol de IAM denominado `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 un [rol de IAM](#) que da DataSync permiso para acceder al sistema de archivos.
- **Action**— Otorga acceso DataSync root y le permite leer y escribir en el sistema de archivos.
- **aws:SecureTransport**: requiere que los clientes de NFS utilicen TLS al conectarse al sistema de archivos.
- **elasticfilesystem:AccessPointArn**: permite el acceso al sistema de archivos solo a través de un punto de acceso específico.

Consideraciones de red con las transferencias de Amazon EFS

VPCs con los que utilices DataSync debe tener el arrendamiento predeterminado. VPCs con un arrendamiento dedicado no son compatibles.

Consideraciones de rendimiento con las transferencias de Amazon EFS

El modo de rendimiento del sistema de archivos de Amazon EFS puede afectar a la duración de la transferencia y al rendimiento del sistema de archivos durante la transferencia. Considere lo siguiente:

- Para obtener los mejores resultados, se recomienda usar el modo de rendimiento de Elastic. Si no utilizas el modo de rendimiento elástico, es posible que la transferencia tarde más.

- Si utiliza el modo de rendimiento por ráfagas, es posible que el rendimiento de las aplicaciones del sistema de archivos se vea afectado, ya que DataSync consume los créditos de ráfaga del sistema de archivos.
- La forma en que se [configura DataSync para comprobar los datos transferidos](#) puede afectar al rendimiento del sistema de archivos y a los costes de acceso a los datos.

Para obtener más información, consulte [Rendimiento de Amazon EFS](#) en la Guía del usuario de Amazon Elastic File System y en la página [Precios de Amazon EFS](#).

Creación de la ubicación de transferencia de Amazon EFS

Para crear la ubicación de transferencia, necesita un sistema de archivos de Amazon EFS existente. Si no tiene uno, consulte [Introducción a Amazon EFS](#) en la Guía del usuario de Amazon Elastic File System.

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. En Tipo de ubicación, elija el sistema de archivos de Amazon EFS.

Puede configurar esta ubicación como origen o destino posteriormente.

4. En Sistema de archivos, elija el sistema de archivos de Amazon EFS que desea utilizar como ubicación.
5. En Ruta de montaje, escriba la ruta de montaje de su sistema de archivos de Amazon EFS.

Especifica dónde se DataSync leen o escriben los datos (dependiendo de si se trata de una ubicación de origen o de destino) en el sistema de archivos.

De forma predeterminada, DataSync utiliza el directorio raíz (o el [punto de acceso](#) si proporciona uno para la configuración del punto de acceso EFS). También puede especificar subdirectorios usando barras diagonales (por ejemplo, /path/to/directory).

6. En Subred, elija una subred en la que desee DataSync crear las [interfaces de red](#) para administrar el tráfico de transferencia de datos.

La subred debe estar ubicada:

- En la misma VPC que el sistema de archivos.
- En la misma zona de disponibilidad que al menos un destino de montaje del sistema de archivos.

 Note

No es necesario especificar una subred que incluya un destino de montaje del sistema de archivos.

7. En el caso de los grupos de seguridad, elija el grupo de seguridad asociado al destino de montaje de un sistema de archivos de Amazon EFS. Puede elegir varios grupos de seguridad.

 Note

Los grupos de seguridad que especifique deben permitir el tráfico entrante en el puerto 2049 de NFS. Para obtener más información, consulte [Determinar la subred y los grupos de seguridad para su destino de montaje](#).

8. Para el cifrado en tránsito, elija si DataSync desea utilizar el cifrado Transport Layer Security (TLS) cuando transfiera datos hacia o desde su sistema de archivos.

 Note

Debe habilitar esta configuración para configurar un punto de acceso, un rol de IAM o ambos con su ubicación de Amazon EFS.

9. (Opcional) Para el punto de acceso EFS, elija un punto de acceso que DataSync pueda utilizar para montar el sistema de archivos.

Para obtener más información, consulte [Acceso a sistemas de archivos restringidos](#).

10. (Opcional) Para el rol de IAM, especifique un rol que permita acceder DataSync al sistema de archivos.

Para obtener información sobre la creación de este rol, consulte [Crear un rol de DataSync IAM para el acceso al sistema de archivos](#).

11. (Opcional) Seleccione Añadir etiqueta para etiquetar su sistema de archivos.

Una etiqueta es un par clave-valor que le ayuda a administrar, filtrar y buscar sus ubicaciones.

12. Seleccione Crear ubicación.

Usando el AWS CLI

1. Copie el siguiente 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. Para `--efs-filesystem-arn`, especifique el nombre de recurso de Amazon (ARN) del sistema de archivos de Amazon EFS desde o hacia el que está realizando la transferencia.
3. Para `--subdirectory`, especifique una ruta de montaje para el sistema de archivos.

Aquí es donde DataSync lee o escribe los datos (dependiendo de si se trata de una ubicación de origen o de destino) en su sistema de archivos.

De forma predeterminada, DataSync utiliza el directorio raíz (o el [punto de acceso](#) si lo proporciona `--access-point-arn`). También puede especificar subdirectorios usando barras diagonales (por ejemplo, `/path/to/directory`).

4. En `--ec2-config`, haga lo siguiente:

- Para `SecurityGroupArns`, especifique el ARN del grupo de seguridad asociado al destino de montaje del sistema de archivos. Puede especificar varios grupos de seguridad.

 Note

Los grupos de seguridad que especifique deben permitir el tráfico entrante en el puerto 2049 de NFS. Para obtener más información, consulte [Determinar la subred y los grupos de seguridad para su destino de montaje](#).

- Para `SubnetArn`, especifique el ARN de la subred en la que desea DataSync crear las [interfaces de red](#) para administrar el tráfico de transferencia de datos.

La subred debe estar ubicada:

- En la misma VPC que el sistema de archivos.
- En la misma zona de disponibilidad que al menos un destino de montaje del sistema de archivos.

 Note

No es necesario especificar una subred que incluya un destino de montaje del sistema de archivos.

5. Para `el-tls-in-transit-encryption`, especifique si DataSync desea utilizar el cifrado Transport Layer Security (TLS) cuando transfiera datos hacia o desde su sistema de archivos.

 Note

Debe configurar este parámetro como `TLS1_2` para configurar un punto de acceso, un rol de IAM o ambos con su ubicación de Amazon EFS.

6. (Opcional) Para `access-point-arn`, especifique el ARN de un punto de acceso que DataSync pueda utilizar para montar el sistema de archivos.

Para obtener más información, consulte [Acceso a sistemas de archivos restringidos](#).

7. (Opcional) Para `file-system-access-role-arn`, especifique el ARN de un rol de IAM que permita acceder DataSync al sistema de archivos.

Para obtener información sobre la creación de este rol, consulte [Crear un rol de DataSync IAM para el acceso al sistema de archivos](#).

8. Ejecute el comando `create-location-efs`.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la ubicación que creó. Por ejemplo:

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

Configurar las transferencias con el servidor FSx de archivos de Windows

Para transferir datos a o desde su sistema de archivos Amazon FSx for Windows File Server, debe crear una ubicación de AWS DataSync transferencia. DataSync puede usar esta ubicación como origen o destino para transferir datos.

Proporcionar DataSync acceso a los sistemas FSx de archivos del servidor de archivos de Windows

DataSync [se conecta al sistema FSx de archivos del servidor de archivos de Windows con el protocolo Server Message Block \(SMB\) y lo monta desde la nube privada virtual \(VPC\) mediante interfaces de red.](#)

Note

VPCs con el que utilices DataSync debe tener una tenencia predeterminada. VPCs con un arrendamiento dedicado no son compatibles.

Temas

- [Permisos necesarios](#)
- [Protocolos de autenticación necesarios](#)
- [Espacios de nombres de DFS](#)

Permisos necesarios

Debe proporcionar DataSync al usuario los derechos necesarios para montar y acceder a los archivos, carpetas y metadatos de archivos del servidor de archivos de Windows. FSx

Se recomienda que este usuario pertenezca a un grupo de Microsoft Active Directory para administrar el sistema de archivos. Las características específicas de este grupo dependen de la configuración de Active Directory:

- Si lo utiliza AWS Directory Service for Microsoft Active Directory con FSx Windows File Server, el usuario debe ser miembro del grupo de FSx administradores AWS delegados.
- Si utiliza Active Directory autoadministrado con FSx Windows File Server, el usuario debe ser miembro de uno de los siguientes grupos:
 - El grupo de administradores de dominio, que es el grupo de administradores delegados predeterminado.
 - Un grupo de administradores delegados personalizado con derechos de usuario que permiten DataSync copiar los permisos de propiedad de los objetos y las listas de control de acceso de Windows (ACLs).

 Important

No puede cambiar el grupo de administradores delegados después de haber implementado el sistema de archivos. Debe volver a implementar el sistema de archivos o restaurarlo desde una copia de seguridad para utilizar el grupo de administradores delegados personalizado con los siguientes derechos de usuario que DataSync necesita copiar los metadatos.

Derecho de usuario	Descripción
Restaurar archivos y directorios (SE_RESTORE_NAME)	Permite DataSync copiar la propiedad de los objetos, los permisos, los metadatos de los archivos y las listas de acceso discrecional de NTFS (DACLs). Este derecho de usuario se suele conceder a los miembros de los grupos Domain Admins y Backup Operators (ambos grupos predeterminados de Active Directory).
Administre el registro de auditoría y seguridad (SE_SECURITY_NAME)	Permite copiar DataSync las listas de control de acceso al sistema NTFS (SACLs).

Derecho de usuario	Descripción
	Este derecho de usuario se suele conceder a los miembros del grupo de administradores de dominio.

- Si desea copiar Windows ACLs y realiza la transferencia entre un servidor de archivos SMB y FSx un sistema de archivos del Servidor de Archivos de Windows o entre FSx los sistemas de archivos del Servidor de Archivos de Windows, los usuarios que proporcione DataSync deben pertenecer al mismo dominio de Active Directory o tener una relación de confianza de Active Directory entre sus dominios.

Warning

El usuario del sistema del servidor de archivos del servidor de archivos de Windows debe tener permisos de control total en todas las carpetas del sistema de archivos. FSx No cambie los permisos de las ACL de NTFS de este usuario en sus carpetas. Si los tiene, DataSync puede cambiar los permisos del sistema de archivos de forma que el recurso compartido de archivos sea inaccesible e impida que se puedan utilizar las copias de seguridad del sistema de archivos. Para obtener más información sobre el acceso a nivel de archivos y carpetas, consulte la Guía [del usuario de Amazon FSx for Windows File Server](#).

Protocolos de autenticación necesarios

Su servidor de archivos FSx para Windows debe utilizar la autenticación NTLM para DataSync poder acceder a él. DataSync no puede acceder a un servidor de archivos que utilice la autenticación Kerberos.

Espacios de nombres de DFS

DataSync no admite los espacios de nombres del Sistema de archivos distribuido (DFS) de Microsoft. En su lugar, se recomienda especificar un servidor de archivos subyacente o un recurso compartido al crear la ubicación. DataSync

Para obtener más información, consulte [Agrupación de varios sistemas de archivos con espacios de nombres DFS en la Guía](#) del usuario de Amazon FSx para Windows File Server.

Cómo crear su ubicación de transferencia FSx para el servidor de archivos de Windows

Antes de empezar, asegúrese de tener un servidor de archivos existente FSx para Windows en su Región de AWS. Para obtener más información, consulte [Introducción a Amazon FSx](#) en la Guía del usuario de Amazon FSx para Windows File Server.

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. Para el tipo de ubicación, selecciona Amazon FSx.
4. Para el sistema de FSx archivos, elija el FSx sistema de archivos del servidor de archivos de Windows que desee usar como ubicación.
5. En el campo Nombre compartido, introduzca una ruta de montaje para el servidor de archivos de Windows mediante barras diagonales. FSx

Especifica la ruta en la que se DataSync leen o escriben los datos (dependiendo de si se trata de una ubicación de origen o de destino).

También puede incluir subdirectorios (por ejemplo, /path/to/directory).

6. Para los grupos de seguridad, elija hasta cinco grupos de EC2 seguridad de Amazon que proporcionen acceso a la subred preferida de su sistema de archivos.

Los grupos de seguridad que elija deben poder comunicarse con los grupos de seguridad del sistema de archivos. Para obtener información sobre la configuración de grupos de seguridad para el acceso al sistema de archivos, consulte la [Guía del usuario de Amazon FSx for Windows File Server](#).

Note

Si elige un grupo de seguridad que no permite conexiones desde dentro de sí mismo, haga una de estas cosas:

- Configure el grupo de seguridad para permitir que se comunique dentro de sí mismo.

- Elija un grupo de seguridad diferente que pueda comunicarse con el grupo de seguridad del destino de montaje.

7. En Usuario, introduzca el nombre de un usuario que pueda acceder al servidor FSx de archivos de Windows.

Para obtener más información, consulte [Permisos necesarios](#).

8. En Contraseña, introduzca la contraseña del nombre de usuario.
9. (Opcional) En Dominio, introduzca el nombre del dominio de Windows al que pertenece el sistema FSx de archivos del servidor de archivos de Windows.

Si tiene varios dominios de Active Directory en su entorno, al configurar esta configuración se asegura de que DataSync se conecten al sistema de archivos correcto.

10. (Opcional) Introduzca los valores de los campos Clave y Valor para etiquetarlos FSx para el servidor de archivos de Windows.

Las etiquetas le ayudan a administrar, filtrar y buscar sus AWS recursos. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

11. Seleccione Crear ubicación.

Uso del AWS CLI

Para crear una ubicación FSx para el servidor de archivos de Windows mediante el AWS CLI

- Usa el siguiente comando para crear una FSx ubicación de 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
```

En el comando `create-location-fsx-windows`, haga lo siguiente:

- `fsx-filesystem-arn`: especifique el nombre de recurso de Amazon (ARN) del sistema de archivos hacia o desde el que desea transferir.
- `security-group-arns`— Especifique un máximo ARNs de cinco grupos de EC2 seguridad de Amazon que proporcionan acceso a la subred preferida de su sistema de archivos.

Los grupos de seguridad que especifique deben poder comunicarse con los grupos de seguridad del sistema de archivos. Para obtener información sobre la configuración de grupos de seguridad para el acceso al sistema de archivos, consulte la [Guía del usuario de Amazon FSx for Windows File Server](#).

 Note

Si elige un grupo de seguridad que no permite conexiones desde dentro de sí mismo, haga una de estas cosas:

- Configure el grupo de seguridad para permitir que se comunique dentro de sí mismo.
 - Elija un grupo de seguridad diferente que pueda comunicarse con el grupo de seguridad del destino de montaje.
- La Región de AWS — La región que especificas es aquella en la que se encuentra tu sistema de FSx archivos de Amazon de destino.

El comando anterior devuelve un ARN de ubicación similar al que se muestra a continuación.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07db7abfc326c50fb"
}
```

Configurar DataSync las transferencias con FSx for Lustre

Para transferir datos a o desde su sistema de archivos Amazon FSx for Lustre, debe crear una ubicación de AWS DataSync transferencia. DataSync puede usar esta ubicación como fuente o destino para transferir datos.

Proporcionar DataSync acceso a cuatro FSx sistemas de archivos Lustre

DataSync accede al sistema de archivos FSx de Lustre mediante el cliente de Lustre.

DataSync requiere acceso a todos los datos de su sistema de archivos de FSx for Lustre. Para tener este nivel de acceso, DataSync monta su sistema de archivos como usuario root utilizando un ID de usuario (UID) y un ID de grupo (GID) de. 0

DataSync monta el sistema de archivos desde la nube privada virtual (VPC) [mediante](#) interfaces de red. DataSync gestiona por completo la creación, el uso y la eliminación de estas interfaces de red en su nombre.

 Note

VPCs con las que utilices DataSync debe tener un arrendamiento predeterminado. VPCs con un arrendamiento dedicado no son compatibles.

Crear su ubicación FSx de transferencia para Lustre

Para crear la ubicación de transferencia, necesita un sistema de archivos existente FSx para Lustre. Para obtener más información, consulte [Introducción a Amazon FSx for Lustre](#) en la Guía del usuario de Amazon FSx for Lustre.

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en. <https://console.aws.amazon.com/datasync/>
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. Para el tipo de ubicación, selecciona Amazon FSx.

Puede configurar esta ubicación como origen o destino posteriormente.

4. Para FSx el sistema de archivos, elija el FSx sistema de archivos de Lustre que desee usar como ubicación.
5. En Ruta de montaje, introduzca la ruta de montaje de su sistema de archivos FSx para Lustre.

La ruta puede incluir un subdirectorio. Cuando la ubicación se utiliza como fuente, DataSync lee los datos de la ruta de montaje. Cuando la ubicación se utiliza como destino, DataSync escribe todos los datos en la ruta de montaje. Si no se proporciona un subdirectorio, DataSync usa el directorio raíz (/).

6. Para los grupos de seguridad, elija hasta cinco grupos de seguridad que proporcionen acceso a su sistema de archivos de FSx for Lustre.

Los grupos de seguridad deben poder acceder a los puertos del sistema de archivos. El sistema de archivos también debe permitir el acceso desde los grupos de seguridad.

Para obtener más información sobre los grupos de seguridad, consulte [Control de acceso al sistema de archivos con Amazon VPC](#) en la Guía del usuario de Amazon FSx for Lustre.

7. (Opcional) Introduzca los valores de los campos clave y valor para etiquetar el FSx sistema de archivos de Lustre.

Las etiquetas le ayudan a administrar, filtrar y buscar sus AWS recursos. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

8. Seleccione Crear ubicación.

Uso del AWS CLI

Para crear una ubicación FSx para Lustre mediante el AWS CLI

- Utilice el siguiente comando para crear una ubicación FSx para 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
```

Los parámetros son obligatorios en el comando `create-location-fsx-lustre`.

- `fsx-filesystem-arn`: el nombre de recurso de Amazon (ARN) completo del sistema de archivos en el que desea leer o escribir.
- `security-group-arns`— El ARN de un grupo de EC2 seguridad de Amazon para aplicarlo a las [interfaces de red](#) de la subred preferida del sistema de archivos.

El comando anterior devuelve un ARN de ubicación similar al que se muestra a continuación.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:111222333444:location/
loc-07sb7abfc326c50fb"
}
```

Configuración de DataSync transferencias con Amazon FSx para OpenZFS

Para transferir datos a o desde tu sistema de archivos Amazon FSx for OpenZFS, debes crear una ubicación de AWS DataSync transferencia. DataSync puede usar esta ubicación como fuente o destino para transferir datos.

Proporcionar DataSync acceso a los FSx sistemas de archivos OpenZFS

DataSync [monta su sistema FSx de archivos OpenZFS desde su nube privada virtual \(VPC\) mediante interfaces de red](#). DataSync gestiona completamente la creación, el uso y la eliminación de estas interfaces de red en su nombre.

Note

VPCs con las que utilices DataSync debe tener un arrendamiento predeterminado. VPCs con un arrendamiento dedicado no son compatibles.

Configuración FSx para la autorización del sistema de archivos OpenZFS

DataSync accede al sistema de archivos FSx de OpenZFS como cliente NFS y monta el sistema de archivos como usuario root con un ID de usuario (UID) y un ID de grupo (GID) de 0.

DataSync Para copiar todos los metadatos de los archivos, debe configurar los ajustes de exportación a NFS en los volúmenes del sistema de archivos mediante `no_root_squash`. Sin embargo, puede limitar este nivel de acceso solo a una DataSync tarea específica.

Para obtener más información, consulte [Propiedades de volumen](#) en la Guía del usuario de Amazon FSx for OpenZFS.

Configurar las exportaciones de NFS específicas para DataSync (recomendado)

Puede configurar una exportación de NFS específica para cada volumen al que solo acceda su DataSync tarea. Haga esto para el volumen anterior más reciente de la ruta de montaje que especificó al crear su ubicación FSx para OpenZFS.

Para configurar una exportación de NFS específica para DataSync

1. Cree su [DataSync tarea](#).

Esto crea las interfaces de red de la tarea que especifique en la configuración de exportación de NFS.

2. Localice las direcciones IP privadas de las interfaces de red de la tarea mediante la EC2 consola de Amazon o AWS CLI.
3. FSx Para el volumen del sistema de archivos OpenZFS, configure los siguientes ajustes de exportación a NFS para cada una de las interfaces de red de la tarea:
 - Dirección del cliente: introduzca la dirección IP privada de la interfaz de red (por ejemplo, **10.24.34.0**).
 - Opciones de NFS: introduzca `rw,no_root_squash`.

Configuración de las exportaciones de NFS para todos los clientes

Puede especificar una exportación de NFS que permita el acceso raíz a todos los clientes.

Cómo configurar una exportación de NFS para todos los clientes

- Para el volumen del sistema de archivos OpenZFS, configure los siguientes ajustes de exportación a NFS: FSx
 - Dirección del cliente: introduzca `*`.
 - Opciones de NFS: introduzca `rw,no_root_squash`.

Crear su ubicación de transferencia FSx para OpenZFS

Para crear la ubicación, necesita un sistema de archivos existente FSx para OpenZFS. Si no tiene uno, consulte [Introducción a Amazon FSx para OpenZFS](#) en la Guía del usuario de Amazon FSx for OpenZFS.

Mediante la consola de DataSync

1. Abra la consola en. AWS DataSync <https://console.aws.amazon.com/datasync/>
2. En el panel de navegación situado a la izquierda, seleccione Ubicaciones y luego elija Crear ubicación.
3. Para el tipo de ubicación, selecciona Amazon FSx.

Puede configurar esta ubicación como origen o destino posteriormente.

4. Para FSx el sistema de archivos, elige el FSx sistema de archivos de OpenZFS que quieras usar como ubicación.
5. En Ruta de montaje, introduzca la ruta de montaje de su sistema de archivos FSx OpenZFS.

La ruta debe empezar por `/fsx` y puede ser cualquier ruta de directorio existente en el sistema de archivos. Cuando la ubicación se utiliza como fuente, DataSync lee los datos de la ruta de montaje. Cuando la ubicación se utiliza como destino, DataSync escribe todos los datos en la ruta de montaje. Si no se proporciona un subdirectorio, DataSync usa el directorio del volumen raíz (por ejemplo, `/fsx`).

6. Para los grupos de seguridad, elija hasta cinco grupos de seguridad que proporcionen acceso de red a su sistema FSx de archivos OpenZFS.

Los grupos de seguridad deben proporcionar acceso a los puertos de red que utiliza el FSx sistema de archivos OpenZFS. El sistema de archivos debe permitir el acceso a la red desde los grupos de seguridad.

Para obtener más información sobre los grupos de seguridad, consulte [Control de acceso al sistema de archivos con Amazon VPC](#) en la Guía del usuario de Amazon FSx for OpenZFS.

7. (Opcional) Amplíe la configuración adicional y, para la versión NFS, elija la versión NFS que DataSync utiliza para acceder al sistema de archivos.

De forma predeterminada, DataSync usa la versión 4.1 de NFS.

8. (Opcional) Introduzca los valores de los campos clave y valor para etiquetarlos en el sistema FSx de archivos OpenZFS.

Las etiquetas le ayudan a administrar, filtrar y buscar su ubicación. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

9. Seleccione Crear ubicación.

Usando el AWS CLI

Para crear una ubicación FSx para OpenZFS mediante el AWS CLI

1. Copie el siguiente comando `create-location-fsx-open-zfs`:

```
aws datasync create-location-fsx-open-zfs \
  --fsx-file-system-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 las opciones en el comando de la siguiente manera:

- Para `fsx-filesystem-arn`, especifique el nombre de recurso de Amazon (ARN) del sistema de archivos de ubicación completo. Esto incluye el Región de AWS lugar donde reside el sistema de archivos Cuenta de AWS, su ID y el identificador del sistema de archivos.
- Para `security-group-arns`, especifique el ARN del grupo de EC2 seguridad de Amazon que proporciona acceso a las [interfaces de red de la subred](#) preferida de su sistema FSx de archivos OpenZFS. Esto incluye el Región de AWS lugar donde reside su EC2 instancia de Amazon Cuenta de AWS, su ID y el ID del grupo de seguridad.

Para obtener más información sobre los grupos de seguridad, consulte [Control de acceso al sistema de archivos con Amazon VPC](#) en la Guía del usuario de Amazon FSx for OpenZFS.

- Para `protocol`, especifique el protocolo que se DataSync utiliza para acceder a su sistema de archivos. (DataSync actualmente solo admite NFS).

3. Ejecute el comando . Obtendrá una respuesta en la que se muestra la ubicación que acaba de crear.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
  abcdef01234567890"
}
```

Configuración de transferencias con Amazon FSx para NetApp ONTAP

Para transferir datos a o desde tu sistema de archivos Amazon FSx for NetApp ONTAP, debes crear una ubicación de AWS DataSync transferencia. DataSync puede usar esta ubicación como fuente o destino para transferir datos.

Proporcionar DataSync acceso a los sistemas FSx de archivos de ONTAP

FSx Para acceder a un sistema de archivos de ONTAP, DataSync monta una máquina virtual de almacenamiento (SVM) en el sistema de archivos mediante [las interfaces de red](#) de la nube privada virtual (VPC). DataSync crea estas interfaces de red en la subred preferida de su sistema de archivos solo cuando crea una tarea que incluya su ubicación de ONTAP. FSx

 Note

VPCs con las que utilices DataSync debe tener un arrendamiento predeterminado. VPCs con un arrendamiento dedicado no son compatibles.

DataSync pueden conectarse a un FSx SVM del sistema de archivos ONTAP y copiar datos mediante el protocolo Network File System (NFS) o Server Message Block (SMB).

Temas

- [Uso del protocolo NFS](#)
- [Uso del protocolo SMB](#)
- [Protocolos no admitidos](#)
- [Elección del protocolo correcto](#)
- [Acceder a los volúmenes SnapLock](#)

Uso del protocolo NFS

Con el protocolo NFS, DataSync utiliza el mecanismo de AUTH_SYS seguridad con un ID de usuario (UID) y un ID de grupo (GID) para autenticarse con el SVM. 0

 Note

DataSync actualmente solo es compatible con la versión 3 de NFS para las ubicaciones de ONTAP. FSx

Uso del protocolo SMB

Con el protocolo SMB, DataSync utiliza las credenciales que usted proporciona para autenticarse con su SVM.

Versiones compatibles de SMB

De forma predeterminada, elige DataSync automáticamente una versión del protocolo SMB en función de la negociación con el servidor de archivos SMB. También puede configurarlo DataSync para usar una versión específica, pero le recomendamos que lo haga solo si DataSync tiene

problemas para negociar automáticamente con el servidor de archivos SMB. Por motivos de seguridad, recomendamos utilizar la versión 3.0.2 o posterior de SMB.

Consulte la siguiente tabla para ver una lista de las opciones de la DataSync consola y la API para configurar una versión SMB con su FSx ubicación de ONTAP:

Opción de la consola	Opción de la API	Descripción
Automático	AUTOMATIC	DataSync y el servidor de archivos SMB negocian la versión más alta de SMB que admiten mutuamente, entre la 2.1 y la 3.1.1. Esta es la opción predeterminada y recomendada. Si, por el contrario, elige una versión específica que el servidor de archivos no admite, es posible que aparezca un error <code>Operation Not Supported</code> .
SMB 3.0.2	SMB3	Restringe la negociación del protocolo solo a la versión 3.0.2 de SMB.
SMB 2.1	SMB2	Restringe la negociación del protocolo solo a la versión 2.1 de SMB.
SMB 2.0	SMB2_0	Restringe la negociación del protocolo solo a la versión 2.0 de SMB.

Permisos necesarios

Debe proporcionar a DataSync un usuario local en su SVM o a un usuario de dominio en su Microsoft Active Directory los derechos necesarios para montar sus archivos, carpetas y metadatos de archivos y acceder a ellos.

Si proporciona un usuario en Active Directory, tenga en cuenta lo siguiente:

- Si lo utiliza AWS Directory Service for Microsoft Active Directory, el usuario debe ser miembro del grupo de FSxadministradores AWS delegados.
- Si utiliza una instancia de Active Directory autoadministrada, el usuario debe ser miembro de uno de dos grupos:

- El grupo de administradores de dominio, que es el grupo de administradores delegados predeterminado.
- Un grupo de administradores delegados personalizado con derechos de usuario que permite DataSync copiar los permisos de propiedad de los objetos y las listas de control de acceso de Windows (ACLs).

Important

No puede cambiar el grupo de administradores delegados después de haber implementado el sistema de archivos. Debe volver a implementar el sistema de archivos o restaurarlo desde una copia de seguridad para utilizar el grupo de administradores delegados personalizado con los siguientes derechos de usuario que DataSync necesita copiar los metadatos.

Derecho de usuario	Descripción
Actuar como parte del sistema operativo (SE_TCB_NAME)	Permite DataSync copiar la propiedad de los objetos, los permisos, los metadatos de los archivos y las listas de acceso discrecional de NTFS (ACLs). Este derecho de usuario se suele conceder a los miembros de los grupos Domain Admins y Backup Operators (ambos grupos predeterminados de Active Directory).
Administre el registro de auditoría y seguridad (SE_SECURITY_NAME)	Permite copiar DataSync las listas de control de acceso al sistema NTFS (SACLs). Este derecho de usuario se suele conceder a los miembros del grupo de administradores de dominio.

- Si desea copiar Windows ACLs y realizar transferencias entre FSx sistemas de archivos ONTAP mediante SMB (u otros tipos de sistemas de archivos que utilicen SMB), los usuarios

que proporcione DataSync deben pertenecer al mismo dominio de Active Directory o tener una relación de confianza de Active Directory entre sus dominios.

Protocolos de autenticación necesarios

Para acceder DataSync al recurso compartido SMB, el sistema de archivos de ONTAP FSx debe utilizar la autenticación NTLM. DataSync no puede acceder a los sistemas de archivos FSx de ONTAP que utilizan la autenticación Kerberos.

Espacios de nombres de DFS

DataSync no admite los espacios de nombres del Sistema de archivos distribuido (DFS) de Microsoft. En su lugar, se recomienda especificar un servidor de archivos subyacente o un recurso compartido al crear la ubicación. DataSync

Protocolos no admitidos

DataSync no puede acceder a FSx los sistemas de archivos ONTAP mediante el protocolo iSCSI (Interfaz de sistemas informáticos pequeños de Internet).

Elección del protocolo correcto

Para conservar los metadatos de los archivos FSx para las migraciones a ONTAP, configure las ubicaciones de DataSync origen y destino para que utilicen el mismo protocolo. Entre los protocolos compatibles, SMB conserva los metadatos con la máxima fidelidad (consulte [Comprenda cómo DataSync gestiona los metadatos de archivos y objetos](#) para ver más información).

Al migrar desde un servidor Unix (Linux) o un recurso compartido de almacenamiento conectado a la red (NAS) que sirve a los usuarios a través de NFS, haga lo siguiente:

1. [Cree una ubicación NFS](#) para el servidor Unix (Linux) o el recurso compartido NAS. (Esta será su ubicación de origen).
2. Configure el volumen FSx de ONTAP al que va a transferir los datos con el estilo de seguridad de [Unix](#).
3. Cree una ubicación FSx para su sistema de archivos ONTAP que esté configurado para NFS. (Esta será su ubicación de destino).

Al migrar desde un servidor Windows o un recurso compartido NAS que sirve a los usuarios a través de SMB, haga lo siguiente:

1. [Cree una ubicación SMB](#) para el servidor Windows o el recurso compartido NAS. (Esta será su ubicación de origen).
2. Configure el volumen FSx de ONTAP al que va a transferir los datos con el estilo de seguridad [NTFS](#).
3. Cree una ubicación FSx para su sistema de archivos ONTAP que esté configurado para SMB. (Esta será su ubicación de destino).

Si su entorno FSx para ONTAP utiliza varios protocolos, le recomendamos que consulte a un AWS especialista en almacenamiento. Para obtener información sobre las prácticas recomendadas para el acceso multiprotocolo, consulte [Habilitar cargas de trabajo multiprotocolo con Amazon FSx for ONTAP](#). NetApp

Acceder a los volúmenes SnapLock

Si va a transferir datos a un [SnapLock volumen](#) de un sistema de archivos FSx compatible con ONTAP, asegúrese de que los SnapLock ajustes de confirmación automática y modo de adición de volumen estén desactivados en el volumen durante la transferencia. Podrá volver a habilitar esta configuración cuando haya terminado de transferir los datos.

Crear tu ubicación de transferencia FSx para ONTAP

Para crear la ubicación, necesita un sistema de archivos existente FSx para ONTAP. Si no tienes uno, consulta [Cómo empezar a usar Amazon FSx for NetApp ONTAP](#) en la Guía del usuario de Amazon FSx for NetApp ONTAP.

Mediante la consola de DataSync

1. Abre la AWS DataSync consola en. <https://console.aws.amazon.com/datasync/>
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. Para el tipo de ubicación, selecciona Amazon FSx.

Puede configurar esta ubicación como origen o destino posteriormente.

4. Para FSx el sistema de archivos, elija el FSx sistema de archivos de ONTAP que desee usar como ubicación.
5. En Máquina virtual de almacenamiento, elija una máquina virtual de almacenamiento (SVM) en el sistema de archivos desde o hacia donde desea copiar datos.

6. En Ruta de montaje, especifique una ruta al archivo compartido en la SVM donde copiará los datos.

Puede especificar una ruta de unión (también conocida como punto de montaje), una ruta de qtree (para recursos compartidos de archivos NFS) o un nombre de recurso compartido (para recursos compartidos de archivos SMB). Por ejemplo, la ruta de montaje podría ser /vol1, /vol1/tree1 o /share1.

 Tip

No especifique una ruta en el volumen raíz de la SVM. Para obtener más información, consulte [Administración FSx de máquinas virtuales de almacenamiento de ONTAP](#) en la Guía del usuario de Amazon FSx for NetApp ONTAP.

7. Para los grupos de seguridad, elija hasta cinco grupos de EC2 seguridad de Amazon que proporcionen acceso a la subred preferida de su sistema de archivos.

Los grupos de seguridad deben permitir el tráfico saliente en los siguientes puertos (según el protocolo que utilice):

- NFS: puertos TCP 111, 635 y 2049
- SMB: puerto TCP 445

Los grupos de seguridad del sistema de archivos también deben permitir el tráfico entrante en los mismos puertos.

8. En Protocolo, elija el protocolo de transferencia de datos que se DataSync utiliza para acceder al SVM de su sistema de archivos.

Para obtener más información, consulte [Elección del protocolo correcto](#).

NFS

DataSync usa la versión 3 de NFS.

SMB

Configure una versión de SMB, un usuario, una contraseña y un nombre de dominio de Active Directory (si es necesario) para acceder a la SVM.

- (Opcional) Amplíe la configuración adicional y elija una versión SMB para usarla DataSync al acceder a su SVM.

De forma predeterminada, elige DataSync automáticamente una versión en función de la negociación con el servidor de archivos SMB. Para obtener más información, consulte [Uso del protocolo SMB](#).

- En Usuario, introduzca un nombre de usuario que puede montar y acceder a los archivos, carpetas y metadatos que quiera transferir en la SVM.

Para obtener más información, consulte [Uso del protocolo SMB](#).

- En Contraseña, introduzca la contraseña del usuario que especificó y que puede acceder a la SVM.
- (Opcional) En el nombre de dominio de Active Directory, introduzca el nombre completo del dominio (FQDN) del Active Directory al que pertenece la SVM.

Si tiene varios dominios en su entorno, al configurar esta configuración se asegura de que DataSync se conecten al SVM correcto.

9. (Opcional) Introduzca los valores de los campos Clave y Valor para etiquetar el sistema FSx de archivos ONTAP.

Las etiquetas le ayudan a gestionar, filtrar y buscar sus AWS recursos. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

10. Seleccione Crear ubicación.

Uso del AWS CLI

Para crear una ubicación FSx para ONTAP mediante el AWS CLI

1. Copie el siguiente 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 las opciones en el comando de la siguiente manera:

- Para `storage-virtual-machine-arn`, especifique el nombre de recurso de Amazon (ARN) completo de una máquina virtual de almacenamiento (SVM) del sistema de archivos en el que quiere copiar datos o desde el que quiere copiar datos.

Este ARN incluye el Región de AWS lugar donde reside el sistema de archivos, el suyo Cuenta de AWS, el sistema de archivos y el SVM. IDs

- Para `security-group-arns`, especifique los grupos ARNs de EC2 seguridad de Amazon que proporcionan acceso a las [interfaces de red](#) de la subred preferida de su sistema de archivos.

Esto incluye el Región de AWS lugar donde reside su EC2 instancia de Amazon Cuenta de AWS, su grupo de seguridad y el suyo IDs. Puede especificar hasta cinco grupos de seguridad ARNs.

Para obtener más información sobre los grupos de seguridad, consulte [Control de acceso al sistema de archivos con Amazon VPC](#) en la Guía del usuario de Amazon FSx for NetApp ONTAP.

- Para `protocol`, configure el protocolo que se DataSync utiliza para acceder al SVM de su sistema de archivos.
 - Para NFS, puede usar la configuración predeterminada:

```
--protocol NFS={}
```

- Para SMB, debe especificar un nombre de usuario y una contraseña que puedan acceder al SVM:

```
--protocol SMB={User=smb-user, Password=smb-password}
```

3. Ejecute el comando .

Recibirá una respuesta que le mostrará la ubicación que acaba de crear.

```
{
  "LocationArn": "arn:aws:datasync:us-west-2:123456789012:location/loc-
  abcdef01234567890"
}
```


Transferir hacia o desde otro almacenamiento en la nube con AWS DataSync

Con AWS DataSync, puede transferir datos entre otros proveedores de nube y servicios AWS de almacenamiento. Para obtener más información, consulta [¿Dónde puedo transferir mis datos DataSync?](#)

Temas

- [Planificación de transferencias hacia o desde sistemas de almacenamiento en la nube de terceros](#)
- [Configuración de AWS DataSync transferencias con Google Cloud Storage](#)
- [Configuración de transferencias con Microsoft Azure Blob Storage](#)
- [Configuración de AWS DataSync transferencias con Microsoft Azure Files Acciones para pequeñas y medianas empresas](#)
- [Configuración de transferencias de con otro almacenamiento de objetos en la nube](#)

Planificación de transferencias hacia o desde sistemas de almacenamiento en la nube de terceros

Al planificar las transferencias de datos entre nubes, tenga en cuenta lo siguiente:

- Uso de un agente: solo se necesita un agente para acceder al almacenamiento en otras nubes cuando se utilizan tareas en modo básico. [Las tareas del modo mejorado](#) no requieren un agente. Si decides usar un agente, puedes implementarlo como una [EC2 instancia de Amazon](#) al transferirlo desde un almacenamiento de objetos compatible con S3 de un proveedor de nube, o como una máquina virtual de Google Compute Engine o Azure para las transferencias desde esos servicios de almacenamiento específicos, respectivamente. Al realizar transferencias desde sistemas de archivos de Google y Azure, recomendamos implementar el agente como una máquina virtual de Google o Azure para que el agente esté lo más cerca posible del sistema de archivos. Además, DataSync comprime los datos del agente a, lo que puede ayudar a reducir los costes de AWS salida. DataSync proporciona una lista de [ubicaciones en la nube validadas](#) que proporcionan la [compatibilidad requerida con la API de Amazon S3](#).
- El punto final de almacenamiento de objetos de la otra nube: el punto final de almacenamiento de un proveedor de nube externo suele ser específico de una región o cuenta. El punto final regional se utiliza como servidor en la ubicación de almacenamiento de DataSync objetos, junto con un nombre de depósito específico.

- Clases de almacenamiento de los objetos de origen: al igual que Amazon S3, algunos proveedores de nube admiten un nivel de archivo que requiere una restauración antes de poder acceder a los objetos archivados. Por ejemplo, los objetos del nivel de archivo Blob de Azure deben recuperarse para un acceso estándar antes de la transferencia de datos. Se puede acceder inmediatamente a los objetos del nivel de archivo de Google Cloud Storage y no es necesario restaurarlos, pero el acceso directo al nivel de archivo conlleva costes de recuperación. Revisa la documentación de tu clase de almacenamiento entre nubes para determinar los requisitos de acceso y las tarifas de recuperación antes de comenzar la transferencia de datos. Para obtener más información sobre la restauración de objetos archivados en Amazon S3, consulte [Restauración de un objeto archivado](#) en la Guía del usuario de Amazon Simple Storage Service.
- Acceso al almacenamiento de objetos: la transferencia de datos entre proveedores de nube externos requiere el acceso al almacenamiento de objetos de la otra nube en forma de claves de autenticación. Por ejemplo, para proporcionar acceso a Google Cloud Storage, debes configurar una ubicación de almacenamiento de DataSync objetos que se conecte a la [API XML de Google Cloud Storage](#) y se autentique mediante una [clave de código de autenticación de mensajes \(HMAC\) basada en hash](#) para tu cuenta de servicio. [Para el almacenamiento de blobs de Azure, configuras una DataSync ubicación de blobs de Azure dedicada que se autentica mediante tokens SAS](#). DataSync se utiliza AWS Secrets Manager para almacenar de forma segura las credenciales de almacenamiento de objetos. Para obtener más información, consulte [Proteger las credenciales de las ubicaciones de almacenamiento](#).
- Compatibilidad con etiquetas de objetos:
 - A diferencia de Amazon S3, no todos los proveedores de nube admiten [etiquetas de objetos](#). DataSync las tareas pueden fallar al intentar leer las etiquetas de la ubicación de origen si el proveedor de la nube no admite etiquetas de objetos a través de la API de Amazon S3 o si las credenciales que proporciona no son suficientes para recuperar las etiquetas. DataSync ofrece una opción de tarea para desactivar la [lectura y la copia de etiquetas](#) de objetos durante una transferencia si no se admiten las etiquetas de objetos o si no se desea conservarlas. Revise la documentación de su proveedor de servicios en la nube para determinar si las etiquetas de objeto son compatibles y compruebe la configuración de las etiquetas de objeto de la tarea de transferencia antes de iniciar la transferencia.
 - Puede usar la API de Amazon S3 para comprobar si un proveedor de nube devolverá una get-object-tagging solicitud. Para obtener más información, consulte [get-object-tagging](#) en la Referencia de los comandos de AWS CLI .

Un proveedor de servicios en la nube que admita etiquetas de objetos devolverá una respuesta similar a la del siguiente ejemplo:

```
aws s3api get-object-tagging --bucket BUCKET_NAME --endpoint- url=https://  
BUCKET_ENDPOINT --key prefix/file1  
  
{  
  
    "TagSet": []  
  
}
```

Un proveedor de servicios en la nube que no lo `get-object-tagging` admita devolverá el siguiente mensaje:

```
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
```

- Costes asociados a las solicitudes y a la salida de datos: la transferencia de datos desde un almacenamiento de objetos en la nube conlleva [costes de solicitud y salida](#) relacionados con la lectura y la transferencia de datos. Los cargos por solicitud varían entre los proveedores de servicios en la nube y entre las clases de almacenamiento, cuando corresponda. Consulte la documentación de su proveedor de servicios en la nube sobre los costos específicos de las solicitudes relacionadas con la clase de almacenamiento de la que planea leer. Para obtener una descripción general de los cargos por solicitud que DataSync implican las transferencias de datos, consulte Cómo [evaluar los costos de las solicitudes de S3 cuando se utiliza DataSync](#) y los [AWS DataSync precios](#). La transferencia de datos desde proveedores de nube específicos genera cargos por salida. Los costos de transferencia de datos varían entre los proveedores de la nube y también dependen de la región en la que se almacenan los datos.
- Tasas de solicitud de almacenamiento de objetos: los proveedores de servicios en la nube tienen diferentes características de rendimiento y tasa de solicitud para sus plataformas de almacenamiento de objetos. Revise las tasas de solicitud de su otro proveedor de servicios en la nube y determine dónde se aplican los límites de solicitud. Planifique con antelación las transferencias altamente paralelizadas compuestas por varios agentes, en las que podría ser necesario crear particiones específicas o aumentar el rendimiento.

Amazon S3 ha documentado las tasas de solicitud en función de las cuales puede crear su solución. Las tasas de solicitud de Amazon S3 son por prefijo particionado y se pueden escalar

a varios prefijos. Para obtener más información, consulte [Patrones de diseño de prácticas recomendadas: optimización del rendimiento de Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

Configuración de AWS DataSync transferencias con Google Cloud Storage

El siguiente tutorial muestra cómo AWS DataSync migrar objetos de un depósito de Google Cloud Storage (GCS) a un depósito de Amazon S3.

Descripción general

DataSync usa la [API XML de Google Cloud Storage](#) para las transferencias de datos. Esta API proporciona una interfaz compatible con Amazon S3 para leer y escribir datos con buckets de GCS.

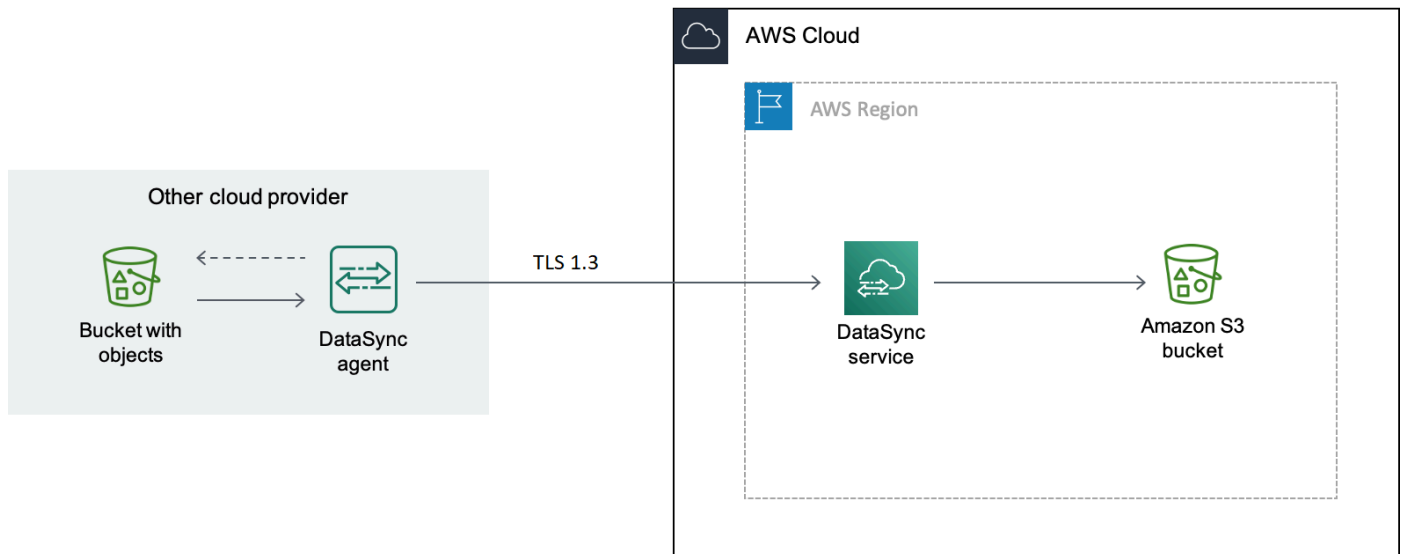
DataSync admite transferencias entre GCS y los servicios de almacenamiento. AWS Al copiar entre GCS y Amazon EFS o Amazon FSx, se requiere un agente y la tarea debe utilizar el modo Básico. Al copiar entre GCS y Amazon S3, solo se necesita un agente cuando se utiliza el modo Básico.

Si utilizas un agente para la transferencia, puedes implementar el agente en Google Cloud o en tu Amazon VPC.

Agent in Google Cloud

1. Despliegas un DataSync agente en tu entorno de Google Cloud.
2. El agente lee el bucket de Google Cloud Storage con una clave de código de autenticación de mensajes basado en hash (HMAC).
3. Los objetos de tu depósito de Google Cloud Storage se transfieren de forma segura a través de TLS 1.3 a través de Nube de AWS un dispositivo de punto final público.
4. El DataSync servicio escribe los datos en tu depósito de S3.

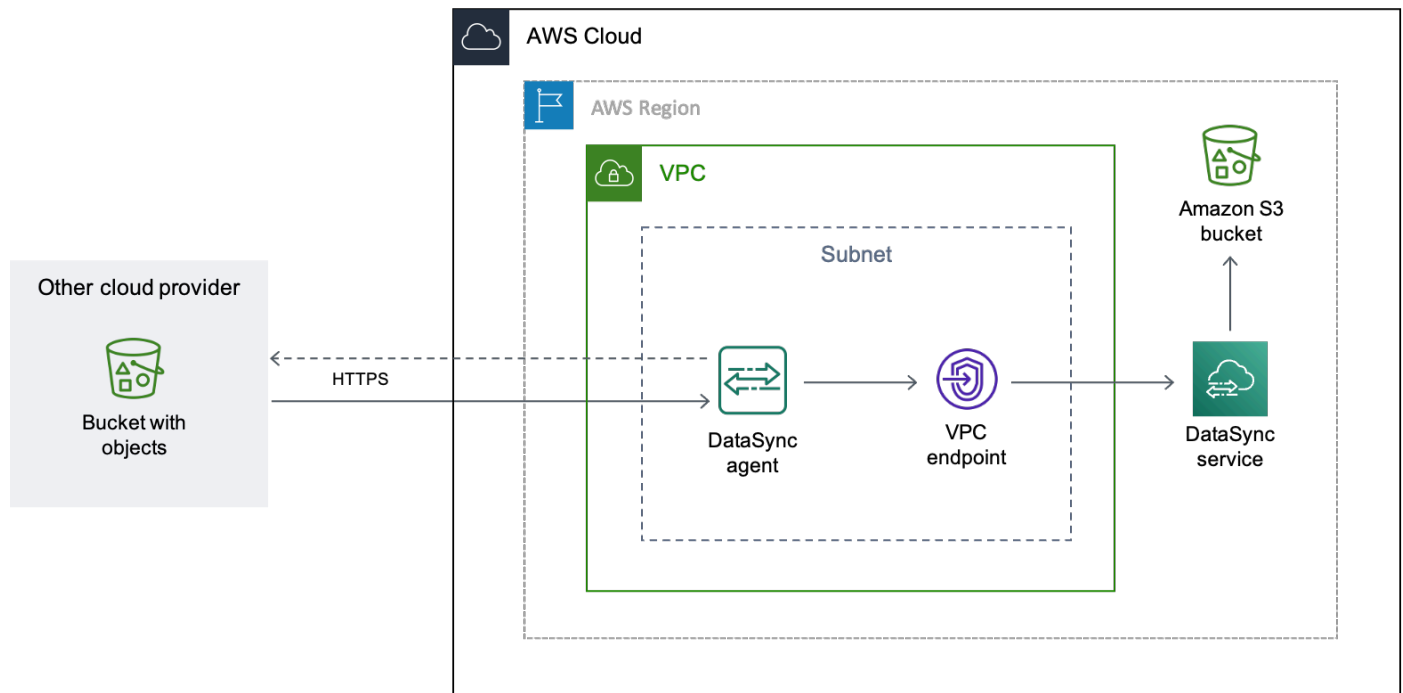
En el siguiente diagrama se ilustra la transferencia.



Agent in your VPC

1. Despliega un DataSync agente en una nube privada virtual (VPC) de su AWS entorno.
2. El agente lee el bucket de Google Cloud Storage con una clave de código de autenticación de mensajes basado en hash (HMAC).
3. Los objetos de tu depósito de Google Cloud Storage se transfieren de forma segura a través de TLS 1.3 a través de Nube de AWS un punto final de VPC privado.
4. El DataSync servicio escribe los datos en tu depósito de S3.

En el siguiente diagrama se ilustra la transferencia.



Costos

Las tarifas asociadas a esta migración pueden incluir:

- Ejecutar una instancia de máquina virtual (VM) de Google [Compute Engine](#) (si implementas tu DataSync agente en Google Cloud)
- Ejecutar una EC2 instancia de [Amazon](#) (si despliega su DataSync agente en una VPC interna) AWS
- Transferir los datos mediante el uso [DataSync](#), incluidos los cargos de solicitud relacionados con [Google Cloud Storage](#) y [Amazon S3](#) (si S3 es una de tus ubicaciones de transferencia)
- Transferencia de datos desde [Google Cloud Storage](#)
- Almacenamiento de datos en [Amazon S3](#)

Requisitos previos

Antes de comenzar, haga lo siguiente si aún no lo ha hecho:

- [Cree un bucket de Google Cloud Storage](#) con los objetos a los que quiera transferir a AWS.
- [Regístrese para una Cuenta de AWS](#).
- [Cree un bucket de Amazon S3](#) para almacenar los objetos después de que estén en AWS.

Creación de una clave HMAC para su bucket de Google Cloud Storage

DataSync utiliza una clave HMAC asociada a tu cuenta de servicio de Google para autenticarse y leer el depósito desde el que estás transfiriendo datos. (Para ver instrucciones detalladas sobre cómo crear claves HMAC, consulte la [Documentación de Google Cloud Storage](#)).

Cómo crear una clave HMAC

1. Cree una clave HMAC para su cuenta de servicio de Google.
2. Asegúrese de que su cuenta de servicio de Google tenga al menos permisos `Storage Object Viewer`.
3. Guarde el ID y el secreto de acceso de la clave HMAC en un lugar seguro.

Necesitarás estos elementos más adelante para configurar la ubicación de DataSync origen.

Paso 2: configurar su red

La configuración de la red solo es necesaria cuando se utiliza un DataSync agente con la transferencia. Los requisitos de red para esta migración dependen del lugar en el que se despliegue el agente.

Para un DataSync agente en Google Cloud

Si quieres alojar a tu DataSync agente en Google Cloud, configura tu red para [permitir las DataSync transferencias a través de un punto final público](#).

Para un DataSync agente en su VPC

Si desea alojar a su agente AWS, necesita una VPC con un punto final de interfaz. DataSync utiliza el punto final de la VPC para facilitar la transferencia.

Cómo configurar la red para un punto de conexión de VPC

1. Si no tiene una, [cree una VPC](#) en el mismo lugar que su bucket Región de AWS de S3.
2. [Cree una subred privada para su VPC](#).
3. [Cree un punto final de servicio de VPC para](#) DataSync
4. Configure su red para [permitir las DataSync transferencias a través de un punto final de servicio de VPC](#).

Para ello, modifique el [grupo de seguridad](#) asociado a su punto de conexión de servicio de VPC.

Paso 3: Crear un DataSync agente (opcional)

Solo se necesita un DataSync agente cuando se utilizan las tareas del modo básico. Si utilizas el modo mejorado para realizar transferencias entre Google Cloud Storage (GCS) y Amazon S3, no necesitas ningún agente. Si quieres usar el modo básico, necesitas un DataSync agente que pueda acceder a tu depósito de GCS.

Para Google Cloud

En este escenario, el DataSync agente se ejecuta en tu entorno de Google Cloud.

Antes de empezar: [instala la CLI de Google Cloud](#).

Cómo crear el agente para Google Cloud

1. Abre la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, elija Agentes y luego, Crear agente.
3. Para Hypervisor, elija VMware ESXi y, a continuación, elija Descargar la imagen para descargar un .zip archivo que contenga el agente.
4. Abra un terminal. Ejecute el siguiente comando para descomprimir la imagen:

```
unzip AWS-DataSync-Agent-VMWare.zip
```

5. Extraiga el contenido del archivo .ova del agente, empezando por aws-datasync ejecutando el siguiente comando:

```
tar -xvf aws-datasync-2.0.1655755445.1-x86_64.xfs.gpt.ova
```

6. Importe el archivo .vmdk del agente a Google Cloud ejecutando el siguiente comando CLI de 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

La importación del archivo .vmdk puede tardar hasta dos horas.

7. Cree e inicie una instancia de máquina virtual para la imagen del agente que acaba de importar.

La instancia necesita las siguientes configuraciones para su agente. (Para ver instrucciones detalladas sobre cómo crear una instancia, consulte la [Documentación de Google Cloud Compute Engine](#)).

- En el tipo de máquina, seleccione una de las siguientes opciones:
 - e2-standard-8: para ejecutar DataSync tareas con hasta 20 millones de objetos.
 - e2-standard-16: para ejecutar DataSync tareas con más de 20 millones de objetos.
- Para ver la configuración del disco de arranque, vaya a la sección de imágenes personalizadas. A continuación, elija la imagen del DataSync agente que acaba de importar.
- Para configurar la cuenta de servicio, elija su cuenta de servicio de Google (la misma cuenta que utilizó en el [paso 1](#)).
- Para la configuración del firewall, elija la opción para permitir el tráfico HTTP (puerto 80).

Para activar el DataSync agente, el puerto 80 debe estar abierto en el agente. No se requiere que el puerto sea accesible públicamente. Una vez activado, DataSync cierra el puerto.

8. Una vez que la instancia de máquina virtual esté en ejecución, anote la dirección IP pública.

Necesitará esta dirección IP para activar el agente.

9. Vuelve a la DataSync consola. En la pantalla Crear agente, donde descargó la imagen del agente, haga lo siguiente para activar el agente:

- En el tipo de punto de conexión, elija la opción de puntos de conexión de servicio público (por ejemplo, puntos de conexión de servicio público en el Este de EE. UU. (Ohio)).
- En Clave de activación, elija Obtener automáticamente la clave de activación de su agente.
- En Dirección del agente, introduzca la dirección IP pública de la instancia de máquina virtual del agente que acaba de crear.
- Seleccione Obtener clave.

10. Asigne un nombre para el agente y, a continuación, elija Crear agente.

Su agente está en línea y listo para transferir datos.

Para su VPC

En este escenario, el agente se ejecuta como una EC2 instancia de Amazon en una VPC asociada a la suya. Cuenta de AWS

Antes de empezar: [configure AWS Command Line Interface \(AWS CLI\)](#).

Cómo crear el agente para su VPC

1. Abra un terminal. Asegúrese de configurar su AWS CLI perfil para usar la cuenta asociada a su bucket de S3.
2. Copie el siguiente comando. Sustituya *vpc-region* por la Región de AWS donde reside la VPC (por ejemplo, us-east-1).

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

3. Ejecute el comando. En la salida, anote la propiedad "Value".

Este valor es el ID de DataSync Amazon Machine Image (AMI) de la región que especificó. Por ejemplo, un ID de AMI podría ser ami-1234567890abcdef0.

4. Copie la siguiente URL. De nuevo, sustituya *vpc-region* por la Región de AWS donde reside la VPC. Luego, sustituya *ami-id* por el ID de AMI que anotó en el paso anterior.

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

5. Pegue la URL en un navegador.

Aparece la página de lanzamiento de la EC2 instancia de AWS Management Console Amazon.

6. Para el tipo de instancia, elige una de las [EC2 instancias de Amazon recomendadas para DataSync los agentes](#).
7. En Par de claves, seleccione un par de claves existente o cree uno nuevo.
8. En Configuración de red, elija la VPC y la subred donde quiera implementar el agente.
9. Seleccione Iniciar instancia.
10. Una vez que la EC2 instancia de Amazon esté en ejecución, [elige tu punto de enlace de VPC](#).
11. [Activación del agente](#).

Paso 4: Crea una ubicación de DataSync origen para tu depósito de Google Cloud Storage

Para configurar una DataSync ubicación para tu depósito de Google Cloud Storage, necesitas el identificador de acceso y el secreto de la clave HMAC que creaste en el [paso 1](#).

Para crear la ubicación de DataSync origen

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. En Tipo de ubicación, seleccione Almacenamiento de objetos.
4. En Servidor, introduzca **storage.googleapis.com**.
5. En Nombre del bucket, introduzca el nombre del bucket de Google Cloud Storage.
6. En Carpeta, introduzca un prefijo de objeto.

DataSync solo copia los objetos con este prefijo.

7. Si la transferencia requiere un agente, selecciona Usar agentes y, a continuación, elige el agente que creaste en el [paso 3](#).
8. Amplíe Configuración adicional. En Protocolo del servidor, seleccione HTTPS. En Puerto del servidor, seleccione 443.
9. Desplácese hasta la sección Autenticación. Asegúrese de que la casilla Requiere credenciales esté seleccionada y, a continuación, haga lo siguiente:
 - En Clave de acceso, introduzca el ID de acceso de la clave HMAC.
 - En Clave secreta, introduce directamente la clave secreta de tu clave HMAC o especifica un AWS Secrets Manager secreto que contenga la clave. Para obtener más información, consulte [Proporcionar credenciales para las ubicaciones de almacenamiento](#).
10. Seleccione Crear ubicación.

Paso 5: Cree una ubicación de DataSync destino para su depósito de S3

Necesita una DataSync ubicación en la que desee que terminen sus datos.

Para crear la ubicación de DataSync destino

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. [Cree una DataSync ubicación para el depósito de S3](#).

Si implementó el DataSync agente en la VPC, en este tutorial se supone que el bucket de S3 está en el mismo Región de AWS lugar que la VPC y el agente. DataSync

Paso 6: Crear e iniciar una tarea DataSync

Con las ubicaciones de origen y destino configuradas, puede empezar a mover los datos a ellas AWS.

Para crear e iniciar la DataSync tarea

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. En la página Configurar ubicación de origen, haga lo siguiente:
 - a. Elija Elegir una ubicación existente.
 - b. Elija la ubicación de origen que creó en el [paso 4](#) y, a continuación, elija Siguiente.
4. En la página Configurar ubicación de destino, haga lo siguiente:
 - a. Elija Elegir una ubicación existente.
 - b. Elija la ubicación de destino que creó en el [paso 5](#) y, a continuación, seleccione Siguiente.
5. En la página Configurar ajustes, haga lo siguiente:
 - a. En Configuración de transferencia de datos, expanda Ajustes adicionales y desactive la casilla Copiar etiquetas de objetos.

Important

Como la API XML de Google Cloud Storage no admite la lectura ni la escritura de etiquetas de objetos, es posible que se produzca un error en la DataSync tarea si intentas copiar etiquetas de objetos.

- b. Configure cualquier otro ajuste de tareas que desee y, a continuación, seleccione Siguiente.
6. En la página Revisar, revise los ajustes y luego seleccione Crear tarea.
 7. En la página de detalles de la tarea, elija Iniciar y, a continuación, elija una de las siguientes acciones:

- Para ejecutar la tarea sin modificarla, seleccione Comenzar con los valores predeterminados.
- Para modificar la tarea antes de ejecutarla, elija Comenzar con las opciones principales.

Cuando finalice la tarea, verá los objetos del bucket de Google Cloud Storage en el bucket de S3.

Configuración de transferencias con Microsoft Azure Blob Storage

Con él AWS DataSync, puede transferir datos entre Microsoft Azure Blob Storage (incluido el almacenamiento de Azure Data Lake Storage Gen2 blobs) y los siguientes AWS servicios de almacenamiento:

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

Para configurar este tipo de transferencia, cree una [ubicación](#) de transferencia para su Azure Blob Storage. Puede usar esta ubicación como origen o destino de la transferencia. Solo se necesita un DataSync agente para transferir datos entre Azure Blob y Amazon EFS o Amazon FSx, o cuando se utilizan tareas del modo Básico. No necesita un agente para transferir datos entre Azure Blob y Amazon S3 mediante el modo mejorado.

Proporcionar DataSync acceso a su Azure Blob Storage

La forma de DataSync acceder a tu cuenta Azure Blob Storage depende de varios factores, como si te estás transfiriendo hacia o desde el almacenamiento de bloques y el tipo de [token de firma de acceso compartido \(SAS\)](#) que utilices. Los objetos también deben estar en un [nivel de acceso](#) con el que DataSync puedan funcionar.

Temas

- [Tokens SAS](#)
- [Niveles de acceso](#)

Tokens SAS

Un token SAS especifica los permisos de acceso al almacenamiento de blobs. (Para obtener más información sobre SAS, consulte la [Documentación de Azure Blob Storage](#)).

Puede generar tokens SAS para proporcionar diferentes niveles de acceso. DataSync admite tokens con los siguientes niveles de acceso:

- Cuenta
- Contenedor

Los permisos de acceso DataSync necesarios dependen del alcance del token. Si no tiene los permisos correctos, es posible que la transferencia no se realice correctamente. Por ejemplo, la transferencia no se realizará correctamente si mueve objetos con etiquetas a Azure Blob Storage pero su token SAS no tiene permisos de etiquetado.

Temas

- [Permisos de token SAS para acceso a nivel de cuenta](#)
- [Permisos de token SAS para acceso a nivel de contenedor](#)
- [Políticas de caducidad de SAS](#)

Permisos de token SAS para acceso a nivel de cuenta

DataSync necesita un token de acceso a nivel de cuenta con los siguientes permisos (en función de si se transfiere hacia o desde Azure Blob Storage).

Transfers from blob storage

- Servicios permitidos:: blob
- Tipos de recursos permitidos: contenedor, objeto

Si no incluyes estos permisos, no DataSync podrás transferir los metadatos de tus objetos, incluidas las etiquetas de los [objetos](#).

- Permisos permitidos: lectura, enumeración
- Permisos de indexación de blobs permitidos: [lectura y escritura \(si quieres DataSync copiar etiquetas de objetos\)](#)

Transfers to blob storage

- Servicios permitidos:: blob
- Tipos de recursos permitidos: contenedor, objeto

Si no incluyes estos permisos, no DataSync podrás transferir los metadatos de tus objetos, incluidas las etiquetas de los objetos.

- Permisos permitidos: leer, escribir, enumerar y eliminar (si quieres DataSync eliminar archivos que no están en tu fuente de transferencia)
- Permisos de indexación de blobs permitidos: lectura/escritura (si quieres DataSync copiar etiquetas de objetos)

Permisos de token SAS para acceso a nivel de contenedor

DataSync necesita un token de acceso a nivel de contenedor con los siguientes permisos (dependiendo de si se está transfiriendo hacia o desde). Azure Blob Storage

Transfers from blob storage

- Lectura
- Enumeración
- Etiqueta (si quieres copiar etiquetas DataSync de objetos)

Note

No puede añadir el permiso para etiquetar al generar un token SAS en el portal de Azure. Para añadir el permiso para etiquetar, genere el token mediante la aplicación [Azure Storage Explorer](#) o genere un [token SAS que proporcione acceso a nivel de cuenta](#).

Transfers to blob storage

- Lectura
- Escritura
- Enumeración
- Eliminar (si quieres DataSync eliminar archivos que no están en tu fuente de transferencia)

- Etiqueta (si quieres DataSync copiar [etiquetas de objetos](#))

 Note

No puede añadir el permiso para etiquetar al generar un token SAS en el portal de Azure. Para añadir el permiso para etiquetar, genere el token mediante la aplicación [Azure Storage Explorer](#) o genere un [token SAS que proporcione acceso a nivel de cuenta](#).

Políticas de caducidad de SAS

Asegúrese de que su SAS no caduque antes de finalizar la transferencia. Para obtener información sobre la configuración de una política de caducidad de SAS, consulte la [Documentación de Azure Blob Storage](#).

Si el SAS caduca durante la transferencia, ya no DataSync podrá acceder a su Azure Blob Storage ubicación. (Es posible que aparezca un mensaje de Failed to open directory). Si esto ocurre, [actualice su ubicación](#) con un nuevo token SAS y reinicie la DataSync tarea.

Niveles de acceso

Al transferir desde Azure Blob Storage, DataSync puede copiar objetos en los niveles caliente y frío. En el caso de los objetos del nivel de acceso al archivo, debe rehidratar dichos objetos en el nivel caliente o frío antes de poder copiarlos.

Al transferirlos a Azure Blob Storage, DataSync puede copiar objetos a los niveles de acceso caliente, frío y archivado. Si está copiando objetos en el nivel de acceso al archivo, no DataSync podrá verificar la transferencia si está intentando [verificar todos los datos del destino](#).

DataSync no es compatible con el nivel de acceso en frío. Para obtener más información sobre los niveles de acceso, consulte la [Documentación de Azure Blob Storage](#).

Consideraciones sobre las transferencias de Azure Blob Storage

Cuando planee transferir datos hacia o desde Azure Blob Storage allí DataSync, hay algunas cosas que debe tener en cuenta.

Temas

- [Costos](#)

- [Tipos de blobs](#)
- [Disponibilidad de Región de AWS](#)
- [Copiado de etiquetas de objeto](#)
- [Transferencia a Amazon S3](#)
- [Eliminación de directorios en un destino de transferencia](#)
- [Limitaciones](#)

Costos

Las tarifas asociadas a mover datos hacia dentro o hacia afuera de Azure Blob Storage pueden incluir:

- Ejecutar una [máquina Azure virtual \(VM\)](#) (si despliega un DataSync agente Azure)
- Ejecutar una EC2 instancia de [Amazon](#) (si despliega un DataSync agente en una VPC interna) AWS
- Transferir los datos mediante el uso [DataSync](#), incluidos los cargos de solicitud relacionados [Azure Blob Storage](#) con [Amazon S3](#) (si S3 es una de sus ubicaciones de transferencia)
- Transferencia de datos hacia adentro o hacia afuera de [Azure Blob Storage](#)
- Almacenamiento de datos en un [servicio AWS de almacenamiento](#) compatible con DataSync

Tipos de blobs

El DataSync funcionamiento de los tipos de blobs depende de si los transfieres hacia o desde Azure Blob Storage. Cuando mueves datos al almacenamiento de bloques, los objetos o archivos que se DataSync transfieren solo pueden ser bloques de bloques. Cuando mueves datos del almacenamiento de bloques, DataSync puedes transferir bloques, páginas y anexar bloques.

Para obtener más información acerca de los tipos de blobs, consulte la [Documentación de Azure Blob Storage](#).

Disponibilidad de Región de AWS

Puedes crear una ubicación de Azure Blob Storage transferencia en cualquiera de las [Región de AWS que sea compatible](#) con. DataSync

Copiado de etiquetas de objeto

La posibilidad de DataSync conservar las etiquetas de los objetos al realizar transferencias de ida y Azure Blob Storage vuelta depende de los siguientes factores:

- El tamaño de las etiquetas de un objeto: no DataSync se puede transferir un objeto con etiquetas que superen los 2 KB.
- Si DataSync está configurado para copiar etiquetas de objetos: DataSync [copia las etiquetas de objetos](#) de forma predeterminada.
- El espacio de nombres que usa su cuenta de Azure almacenamiento: DataSync puede copiar etiquetas de objetos si su cuenta de Azure almacenamiento usa un espacio de nombres plano, pero no si su cuenta usa un espacio de nombres jerárquico (una función de). Azure Data Lake Storage Gen2 DataSync La tarea fallará si intenta copiar etiquetas de objetos y su cuenta de almacenamiento utiliza un espacio de nombres jerárquico.
- Si su token SAS autoriza el etiquetado: los permisos que necesita para copiar etiquetas de objetos varían según el nivel de acceso que proporcione su token. La tarea fallará si intenta copiar etiquetas de objetos y su token no tiene los permisos adecuados para etiquetar. Para obtener más información, consulte los requisitos de permiso para los [tokens de acceso a nivel de cuenta](#) o los [tokens de acceso a nivel de contenedor](#).

Transferencia a Amazon S3

Al realizar la transferencia a Amazon S3, DataSync no transferirá Azure Blob Storage objetos de más de 5 TB ni objetos con metadatos de más de 2 KB.

Eliminación de directorios en un destino de transferencia

Al realizar la transferencia a Azure Blob Storage, DataSync puede [eliminar objetos del almacenamiento de blobs que no estén presentes en la fuente de transferencia](#). (Para configurar esta opción, desactive la opción Conservar los archivos eliminados de la DataSync consola. Su [token SAS](#) también debe tener permisos de eliminación).

Si configuras la transferencia de esta manera, DataSync no se eliminarán los directorios de tu almacenamiento de blobs si tu cuenta de Azure almacenamiento utiliza un espacio de nombres jerárquico. En este caso, debe eliminar los directorios manualmente (por ejemplo, utilizando [Azure Storage Explorer](#)).

Limitaciones

Recuerde las siguientes limitaciones cuando transfiera datos a Azure Blob Storage o desde él:

- DataSync [crea algunos directorios](#) en una ubicación para facilitar la transferencia. Si Azure Blob Storage es una ubicación de destino y tu cuenta de almacenamiento usa un espacio de nombres jerárquico, es posible que veas subdirectorios específicos para cada tarea (por ejemplo) en la carpeta. `task-000011112222abcde /.aws-datasync` DataSync normalmente elimina estos subdirectorios después de una transferencia. Si eso no sucede, puede eliminar usted mismo estos directorios específicos de tareas mientras la tarea no esté en ejecución.
- DataSync no admite el uso de un token SAS para acceder únicamente a una carpeta específica del contenedor. Azure Blob Storage
- No puedes proporcionar DataSync un token SAS de delegación de usuarios para acceder a tu almacenamiento de blobs.

Crear tu DataSync agente (opcional)

Solo se necesita un DataSync agente para transferir datos entre Azure Blob y Amazon EFS o Amazon FSx, o cuando se utilizan tareas del modo Básico. No necesita un agente para transferir datos entre Azure Blob y Amazon S3 mediante el modo mejorado. En esta sección se describe cómo implementar y activar un agente.

Tip

Si bien puedes implementar tu agente en una EC2 instancia de Amazon, el uso de un Microsoft Hyper-V agente puede reducir la latencia de la red y aumentar la compresión de los datos.

Agentes de Microsoft Hyper-V

Puede implementar su DataSync agente directamente Azure con una Microsoft Hyper-V imagen.

Tip

Antes de continuar, considere la posibilidad de utilizar un script del intérprete de comandos que pueda ayudarle a implementar su agente de Hyper-V en Azure de forma más rápida. Puede obtener más información y descargar el código en [GitHub](#).

Si usa el script, puede pasar directamente a la sección sobre [Obtención de la clave de activación de su agente](#).

Temas

- [Requisitos previos](#)
- [Descarga y preparación de su agente](#)
- [Implementación de su agente en Azure](#)
- [Obtención de la clave de activación de su agente](#)
- [Activación de su agente](#)

Requisitos previos

Para preparar el DataSync agente e implementarlo en Azure, debe hacer lo siguiente:

- Habilite Hyper-V en su máquina local.
- Instale [PowerShell](#) (incluido el Hyper-V Module).
- Instale la [CLI de Azure](#).
- Instale [AzCopy](#).

Descarga y preparación de su agente

Descargue un agente de la DataSync consola. Antes de poder implementar el agente en Azure, debe convertirlo en un disco duro virtual (VHD) de tamaño fijo. Para obtener más información, consulte la [Documentación de Azure](#).

Cómo descargar y preparar su agente

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, elija Agentes y luego, Crear agente.
3. Para Hipervisor, elija Microsoft Hyper-V y, a continuación, elija Descargar la imagen.

El agente se descarga en un archivo .zip que contiene un archivo .vhdx.

4. Extraiga el archivo .vhdx en su máquina local.
5. Abra PowerShell y haga lo siguiente:

- a. Copie el siguiente cmdlet de Convert-VHD:

```
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. Sustituya cada instancia de *local-path-to-vhdx-file* por la ubicación del archivo .vhdx en su máquina local.
- c. Ejecute el comando .

Su agente ahora es un VHD de tamaño fijo (con un formato de archivo .vhd) y está listo para su implementación en Azure.

Implementación de su agente en Azure

El despliegue de su DataSync agente Azure implica:

- Creación de un disco administrado en Azure
- Carga de su agente en ese disco administrado
- Conexión del disco administrado a una máquina virtual Linux

Cómo implementar su agente en Azure

1. En PowerShell, vaya al directorio que contiene el archivo .vhd de su agente.
2. Ejecute el comando `ls` y guarde el valor `Length` (por ejemplo, 85899346432).

Este es el tamaño de la imagen del agente en bytes, que necesitará al crear un disco administrado que pueda contener la imagen.

3. Haga lo siguiente para crear un disco administrado:

- a. Copie el siguiente comando Azure de la CLI:

```
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. Sustituya *your-managed-disk* por un nombre para su disco administrado.
- c. Sustituya *your-resource-group* por el nombre del grupo de recursos de Azure al que pertenece su cuenta de almacenamiento.
- d. Sustituya *your-azure-region* por la región de Azure en la que se encuentra su grupo de recursos.
- e. Sustituya *agent-size-bytes* por el tamaño de su imagen de agente.
- f. Ejecute el comando .

Este comando crea un disco gestionado vacío con un [SKU estándar](#) en el que puede cargar su DataSync agente.

4. Para generar una firma de acceso compartido (SAS) que permita el acceso de escritura al disco administrado, haga lo siguiente:
 - a. Copie el siguiente comando Azure de la CLI:

```
az disk grant-access -n your-managed-disk `
-g your-resource-group `
--access-level Write `
--duration-in-seconds 86400
```

- b. Sustituya *your-managed-disk* por el nombre del disco administrado que creó.
- c. Sustituya *your-resource-group* por el nombre del grupo de recursos de Azure al que pertenece su cuenta de almacenamiento.
- d. Ejecute el comando .

En la salida, busque y anote el URI del SAS. Necesitará este URI cuando cargue el agente en Azure.

El SAS le permite escribir en el disco durante un máximo de una hora. Esto significa que dispone de una hora para cargar su agente en el disco administrado.

5. Para cargar el agente en su disco administrado en Azure, haga lo siguiente:
 - a. Copie el siguiente comando AzCopy:

```
.\azcopy copy local-path-to-vhd-file sas-uri --blob-type PageBlob
```

- b. Sustituya *local-path-to-vhd-file* por la ubicación del archivo del agente .vhd en su máquina local.
 - c. Sustituya *sas-uri* por el URI de SAS que obtuvo cuando ejecutó el comando `az disk grant-access`.
 - d. Ejecute el comando .
6. Cuando finalice la carga del agente, revoque el acceso al disco administrado. Para hacerlo, copie el siguiente comando Azure de la CLI:

```
az disk revoke-access -n your-managed-disk -g your-resource-group
```

- a. Sustituya *your-resource-group* por el nombre del grupo de recursos de Azure al que pertenece su cuenta de almacenamiento.
 - b. Sustituya *your-managed-disk* por el nombre del disco administrado que creó.
 - c. Ejecute el comando .
7. Haga lo siguiente para conectar el disco administrado a una nueva máquina virtual Linux:
- a. Copie el siguiente comando Azure de la CLI:

```
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. Sustituya *your-resource-group* por el nombre del grupo de recursos de Azure al que pertenece su cuenta de almacenamiento.
- c. Sustituya *your-agent-vm* por un nombre para la máquina virtual que pueda recordar.
- d. Sustituya *your-managed-disk* por el nombre del disco administrado que está conectando a la máquina virtual.
- e. Ejecute el comando .

Ha implementado su agente. Antes de empezar a configurar la transferencia de datos, debe activar el agente.

Obtención de la clave de activación de su agente

Para obtener manualmente la clave de activación de su DataSync agente, siga estos pasos.

Como alternativa, [DataSync puede obtener automáticamente la clave de activación](#), pero este enfoque requiere cierta configuración de red.

Cómo obtener la clave de activación de su agente

1. En el portal de Azure, [habilite el diagnóstico de arranque de la máquina virtual para su agente](#); para ello, seleccione la configuración Habilitar con una cuenta de almacenamiento personalizada y especifique su cuenta de almacenamiento de Azure.

Una vez que haya activado los diagnósticos de arranque de la máquina virtual de su agente, podrá acceder a la consola local del agente para obtener la clave de activación.

2. Mientras está en el portal de Azure, vaya a su máquina virtual y elija Consola serie.
3. En la consola local del agente, inicie sesión con las siguientes credenciales predeterminadas:
 - Nombre de usuario: **admin**
 - Contraseña: **password**

Recomendamos cambiar al menos la contraseña del agente en algún momento. En la consola local del agente, introduzca **5** en el menú principal y, a continuación, utilice el comando `passwd` para cambiar la contraseña.

4. Introduzca **0** para obtener la clave de activación del agente.
5. Introduzca la Región de AWS ubicación que está utilizando DataSync (por ejemplo, **us-east-1**).
6. Elija el [punto de conexión del servicio](#) con el que se conectará el agente AWS.
7. Guarde el valor del resultado de la `Activation key`.

Activación de su agente

Una vez que tenga la clave de activación, podrá terminar de crear su DataSync agente.

Cómo activar el agente

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, elija Agentes y luego, Crear agente.
3. Como Hipervisor, elija Microsoft Hyper-V.
4. Para el tipo de punto final, elija el mismo tipo de punto final de servicio que especificó al obtener la clave de activación de su agente (por ejemplo, seleccione puntos finales de servicio público en **Region name**).
5. Configure su red para que funcione con el tipo de punto de conexión de servicio que utilice su agente. Para conocer los requisitos de la red de punto de conexión del servicio, consulte los siguientes temas:
 - [Puntos de conexión de VPC](#)
 - [Puntos de conexión públicos](#)
 - [Puntos de conexión del estándar federal de procesamiento de información \(FIPS\)](#)
6. Para la clave de activación, haga lo siguiente:
 - a. Elija Introducir manualmente la clave de activación de su agente.
 - b. Introduzca la clave de activación que obtuvo de la consola local del agente.
7. Elija Crear agente.

Su agente está listo para conectarse con su Azure Blob Storage. Para obtener más información, consulte [Creación de su ubicación de transferencia de Azure Blob Storage](#).

EC2 Agentes de Amazon

Puede implementar su DataSync agente en una EC2 instancia de Amazon.

Para crear un EC2 agente de Amazon

1. [Despliega un EC2 agente de Amazon](#).
2. [Elija un punto de conexión de servicio](#) que el agente use para comunicarse con AWS.

En esta situación, se recomienda utilizar un punto de conexión de servicio de nube privada virtual (VPC).

3. Configure su red para que funcione con los [puntos de conexión del servicio de VPC](#).
4. [Active el agente](#).

Creación de su ubicación de transferencia de Azure Blob Storage

Puedes configurarlo DataSync para que Azure Blob Storage lo utilices como fuente o destino de la transferencia.

Antes de empezar

Asegúrese de saber [cómo se DataSync accede a los niveles de acceso Azure Blob Storage y los tipos de blob](#) y cómo funciona con ellos. También necesita un [DataSync agente](#) que pueda conectarse a su Azure Blob Storage contenedor.

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. En Tipo de ubicación, elija Microsoft Azure Blob Storage.
4. En URL del contenedor, escriba la URL del contenedor implicado en la transferencia.
5. (Opcional) Para Acceder al nivel de acceso cuando se usa como destino, elija el [nivel de acceso](#) al que quiere que se transfieran sus objetos o archivos.
6. En Carpeta, introduzca los segmentos de ruta si desea limitar la transferencia a un directorio virtual del contenedor (por ejemplo, /my/images).
7. Si su transferencia requiere un agente, elija Usar agentes y, a continuación, elija el DataSync agente que pueda conectarse con su Azure Blob Storage contenedor.
8. En el caso del token SAS, proporciona las credenciales necesarias para acceder DataSync a tu almacenamiento de blobs. Algunos conjuntos de datos públicos de Azure Blob Storage no requieren credenciales. Puede introducir un token SAS directamente o especificar un AWS Secrets Manager secreto que contenga el token. Para obtener más información, consulte [Proporcionar credenciales para las ubicaciones de almacenamiento](#).

El token SAS forma parte de la cadena URI de SAS que aparece después del URI del recurso de almacenamiento y de un signo de interrogación (?). Un token tiene un aspecto similar a este:

```
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) Proporcione valores para los campos Clave y Valor para etiquetar la ubicación.

Las etiquetas le ayudan a administrar, filtrar y buscar sus AWS recursos. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

10. Seleccione Crear ubicación.

Uso del AWS CLI

1. Copie el siguiente 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 el parámetro `--container-url`, especifique la URL del contenedor Azure Blob Storage implicado en la transferencia.
3. En el parámetro `--authentication-type`, especifique SAS. Si está accediendo a un conjunto de datos público que no requiere autenticación, especifique `NONE`.
4. Para la Token opción del `--sas-configuration` parámetro, especifique el token SAS que permite acceder DataSync a su almacenamiento de blobs.

También puedes proporcionar parámetros adicionales para proteger tus claves mediante AWS Secrets Manager. Para obtener más información, consulte [Proporcionar credenciales para las ubicaciones de almacenamiento](#).

El token SAS forma parte de la cadena URI de SAS que aparece después del URI del recurso de almacenamiento y de un signo de interrogación (?). Un token tiene un aspecto similar a este:

```
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 el `--agent-arns` parámetro, especifique el nombre de recurso de Amazon (ARN) del DataSync agente que se puede conectar al contenedor.

El siguiente es un ejemplo de agente de ARN: `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

Puede especificar más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

6. Para el parámetro `--subdirectory`, especifique los segmentos de ruta si quiere limitar la transferencia a un directorio virtual del contenedor (por ejemplo, `/my/images`).
7. (Opcional) Para el parámetro `--access-tier`, especifique el [nivel de acceso](#) (HOT, COOL o ARCHIVE) al que quiere que se transfieran sus objetos o archivos.

Este parámetro solo es aplicable cuando se utiliza esta ubicación como destino de transferencia.

8. (Opcional) Para el parámetro `--tags`, especifique pares clave-valor que le ayuden a administrar, filtrar y buscar su ubicación.

Le recomendamos crear una etiqueta de nombre para su ubicación.

9. Ejecute el comando `create-location-azure-blob`.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la ubicación que creó. Por ejemplo:

```
{
  "LocationArn": "arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh"
}
```

Visualización de su ubicación de transferencia de Azure Blob Storage

Puedes obtener detalles sobre la ubicación de DataSync transferencia existente para tu Azure Blob Storage.

Mediante la consola de DataSync

1. Abre la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones.
3. Elija su ubicación de Azure Blob Storage.

Puedes ver los detalles de tu ubicación, incluidas las tareas de DataSync transferencia que la estén utilizando.

Usando el AWS CLI

1. Copie el siguiente comando `describe-location-azure-blob`:

```
aws datasync describe-location-azure-blob \  
  --location-arn "your-azure-blob-location-arn"
```

2. Para el parámetro `--location-arn`, especifique el ARN de la ubicación Azure Blob Storage que creó (por ejemplo, `arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. Ejecute el comando `describe-location-azure-blob`.

Recibirá una respuesta que le mostrará detalles sobre su ubicación. Por ejemplo:

```
{  
  "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"],  
}
```

Actualización de su ubicación de transferencia de Azure Blob Storage

Si es necesario, puede modificar la configuración de su ubicación en la consola o mediante la AWS CLI.

Usando el AWS CLI

1. Copie el siguiente comando `update-location-azure-blob`:

```
aws datasync update-location-azure-blob \  
  --location-arn "your-azure-blob-location-arn" \  
  --authentication-type "SAS" \  
  --subdirectory "/my/images"
```

```
--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 el parámetro `--location-arn`, especifique el ARN de la ubicación Azure Blob Storage que va a actualizar (por ejemplo, `arn:aws:datasync:us-east-1:123456789012:location/loc-12345678abcdefgh`).
3. En el parámetro `--authentication-type`, especifique SAS.
4. Para la Token opción del `--sas-configuration` parámetro, especifique el token SAS que permite acceder DataSync a su almacenamiento de blobs.

El token forma parte de la cadena URI de SAS que aparece después del URI del recurso de almacenamiento y de un signo de interrogación (?). Un token tiene un aspecto similar a este:

```
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 el `--agent-arns` parámetro, especifique el nombre de recurso de Amazon (ARN) del DataSync agente que quiere conectar al contenedor.

El siguiente es un ejemplo de agente de ARN: `arn:aws:datasync:us-east-1:123456789012:agent/agent-01234567890aaabfb`

Puede especificar más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

6. Para el parámetro `--subdirectory`, especifique los segmentos de ruta si quiere limitar la transferencia a un directorio virtual del contenedor (por ejemplo, `/my/images`).
7. (Opcional) Para el parámetro `--access-tier`, especifique el [nivel de acceso](#) (HOT, COOL o ARCHIVE) al que desea que se transfieran sus objetos.

Este parámetro solo es aplicable cuando se utiliza esta ubicación como destino de transferencia.

Pasos a seguir a continuación

Cuando termines de crear una DataSync ubicación para tu transferencia Azure Blob Storage, puedes seguir configurando tu transferencia. Aquí se indican algunos pasos siguientes que se deben tener en cuenta:

1. Si aún no lo ha hecho, [cree otra ubicación](#) desde o hacia la que planea transferir los datos a su Azure Blob Storage o desde este.
2. Obtén información sobre cómo DataSync [gestiona los metadatos y los archivos especiales](#), especialmente si tus ubicaciones de transferencia no tienen una estructura de metadatos similar.
3. Configure la forma en que se transfieren sus datos. Por ejemplo, puede [transferir solo un subconjunto de sus datos](#) o eliminar archivos de su almacenamiento de blobs que no estén en su ubicación de origen (siempre y cuando su [token SAS](#) tenga permisos de eliminación).
4. [Inicie la transferencia](#).

Configuración de AWS DataSync transferencias con Microsoft Azure Files Acciones para pequeñas y medianas empresas

Puede configurarlo AWS DataSync para transferir datos a o desde un Microsoft Azure Files Recurso compartido del bloque de mensajes del servidor (SMB).

Tip

[Para ver un tutorial completo sobre cómo transferir datos de archivos compartidos de Azure Files a archivos compartidos por pequeñas y medianas empresas AWS, consulte el AWS blog sobre almacenamiento.](#)

Proporcionar DataSync acceso a recursos compartidos para pequeñas y medianas empresas

DataSync se conecta a su recurso compartido SMB mediante el protocolo SMB y se autentica con las credenciales que usted le proporciona.

Temas

- [Versiones del protocolo SMB compatibles](#)

- [Permisos necesarios](#)

Versiones del protocolo SMB compatibles

De forma predeterminada, elige DataSync automáticamente una versión del protocolo SMB en función de la negociación con el servidor de archivos SMB.

También puede configurarlo DataSync para usar una versión SMB específica, pero le recomendamos que lo haga solo si DataSync tiene problemas para negociar automáticamente con el servidor de archivos SMB. DataSync es compatible con las versiones 1.0 y posteriores para SMB. Por motivos de seguridad, recomendamos utilizar la versión 3.0.2 o posterior para SMB. Las versiones anteriores, como SMB 1.0, contienen vulnerabilidades de seguridad conocidas que los atacantes pueden aprovechar para comprometer sus datos.

Consulta la siguiente tabla para ver una lista de las opciones de la DataSync consola y la API:

Opción de la consola	Opción de la API	Descripción
Automático	AUTOMATIC	DataSync y el servidor de archivos SMB negocian la versión más alta de SMB que admiten mutuamente, entre la 2.1 y la 3.1.1. Esta es la opción predeterminada y recomendada. Si, por el contrario, elige una versión específica que el servidor de archivos no admite, es posible que aparezca un error <code>Operation Not Supported</code> .
SMB 3.0.2	SMB3	Restringe la negociación del protocolo solo a la versión 3.0.2 de SMB.
SMB 2.1	SMB2	Restringe la negociación del protocolo solo a la versión 2.1 de SMB.
SMB 2.0	SMB2_0	Restringe la negociación del protocolo solo a la versión 2.0 de SMB.
SMB 1.0	SMB1	Restringe la negociación del protocolo solo a la versión 1.0 de SMB.

Permisos necesarios

DataSync necesita un usuario que tenga permiso para montar y acceder a su ubicación SMB. Este usuario puede ser un usuario local de su instancia de Windows File Server o puede ser un usuario del dominio definido en Microsoft Active Directory.

Para establecer la propiedad del objeto, se DataSync requiere el SE_RESTORE_NAME privilegio, que normalmente se otorga a los miembros de los grupos integrados de Active Directory, Backup Operators y Domain Admins. Proporcionar este privilegio a DataSync un usuario también ayuda a garantizar permisos suficientes para acceder a los archivos, las carpetas y los metadatos de los archivos, excepto en el caso de las listas de control de acceso al sistema NTFS (SACLs).

Se requieren privilegios adicionales para poder copiar SACLs. Esta operación requiere específicamente el privilegio de Windows SE_SECURITY_NAME, que se concede a los miembros del grupo de Administradores de dominio. Si configura la tarea para que se copie SACLs, asegúrese de que el usuario tenga los privilegios necesarios. Para obtener más información sobre cómo configurar una tarea para SACLs copiarla, consulte [Configuración de la forma en que gestionan los archivos, los objetos y los metadatos](#).

Al copiar datos entre un servidor de archivos SMB y el sistema de archivos Amazon FSx for Windows File Server, las ubicaciones de origen y destino deben pertenecer al mismo dominio de Microsoft Active Directory o tener una relación de confianza de Active Directory entre sus dominios.

Crear la ubicación de transferencia de Azure Files mediante la consola

1. Abra la AWS DataSync consola en. <https://console.aws.amazon.com/datasync/>
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. En Location type (Tipo de ubicación), elija Server Message Block (SMB).

Puede configurar esta ubicación como origen o destino posteriormente.

4. En el caso de los agentes, elija uno o varios DataSync agentes que desee conectar a su recurso compartido SMB.

Si elige más de un agente, asegúrese de entender el uso de [varios agentes para una ubicación](#).

5. En el caso del servidor SMB, introduzca el nombre del sistema de nombres de dominio (DNS) o la dirección IP del recurso compartido SMB que montará el DataSync agente.

 Note

No puede especificar una dirección IP de versión 6 (IPv6).

6. En Nombre del recurso compartido, introduzca el nombre del recurso compartido exportado por el recurso compartido SMB en el que DataSync se leerán o escribirán los datos.

Puede incluir un subdirectorio en la ruta del recurso compartido (por ejemplo, `/path/to/subdirectory`). Asegúrese de que otros clientes de SMB de la red también puedan montar esta ruta.

Para copiar todos los datos del subdirectorio, DataSync debe poder montar el recurso compartido SMB y acceder a todos sus datos. Para obtener más información, consulte [Permisos necesarios](#).

7. (Opcional) Amplíe la configuración adicional y elija una versión SMB para usarla DataSync al acceder a su recurso compartido SMB.

De forma predeterminada, elige DataSync automáticamente una versión en función de la negociación con el recurso compartido para pequeñas y medianas empresas. Para obtener más información, consulte [Versiones compatibles de SMB](#).

8. En Usuario, introduzca el nombre de usuario que puede montar el recurso compartido SMB y que tiene permiso para acceder a los archivos y carpetas que intervienen en la transferencia.

Para obtener más información, consulte [Permisos necesarios](#).

9. En Contraseña, introduzca la contraseña del usuario que puede montar el recurso compartido SMB y que tiene los permisos para obtener acceso a los archivos y carpetas que intervienen en la transferencia..

10. (Opcional) Para Dominio, introduzca el nombre de dominio de Windows al que pertenece su recurso compartido de SMB.

Si tiene varios dominios en su entorno, al configurar esta configuración se asegura de que DataSync se conecte al recurso compartido correcto.

11. (Opcional) Elija Añadir etiqueta para etiquetar su ubicación.

Las etiquetas son pares de clave-valor que le ayudan a administrar, filtrar y buscar sus recursos de DataSync. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

12. Seleccione Crear ubicación.

Configuración de transferencias de con otro almacenamiento de objetos en la nube

Con AWS DataSync, puede transferir datos entre los [servicios AWS de almacenamiento y los](#) siguientes proveedores de almacenamiento de objetos en la nube:

- [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](#)

Solo se necesita un DataSync agente cuando se transfieren datos entre sistemas de almacenamiento de otras nubes y Amazon EFS o Amazon FSx, o cuando se utilizan tareas en modo básico. No necesita un agente para transferir datos entre sistemas de almacenamiento de otras nubes y Amazon S3 mediante el modo mejorado.

Independientemente de si utiliza un agente, también debe crear una [ubicación](#) de transferencia para su almacenamiento de objetos en la nube (específicamente, una ubicación de almacenamiento de objetos). DataSync puede usar esta ubicación como origen o destino para su transferencia.

Proporcionar DataSync acceso a su otro almacenamiento de objetos en la nube

La forma en que DataSync accede a su almacenamiento de objetos en la nube depende de varios factores, como si su almacenamiento es compatible con la API de Amazon S3 y los permisos y credenciales que se DataSync necesitan para acceder a su almacenamiento.

Temas

- [Compatibilidad con la API de Amazon S3](#)
- [Permisos de almacenamiento y puntos de conexión](#)
- [Credenciales de almacenamiento](#)

Compatibilidad con la API de Amazon S3

Su almacenamiento de objetos en la nube debe ser compatible con las siguientes [operaciones de la API de Amazon S3](#) DataSync para poder conectarse a él:

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

Permisos de almacenamiento y puntos de conexión

Debe configurar los permisos que le permiten acceder DataSync a su almacenamiento de objetos en la nube. Si su almacenamiento de objetos es una ubicación de origen, DataSync necesita permisos de lectura y lista para el depósito desde el que está transfiriendo los datos. Si tu almacenamiento de objetos es una ubicación de destino, DataSync necesitas permisos de lectura, lista, escritura y eliminación para el depósito.

DataSync también necesita un punto final (o servidor) para conectarse a su almacenamiento. En la siguiente tabla se describen los puntos finales que DataSync se pueden utilizar para acceder a otro almacenamiento de objetos en la nube:

Otro proveedor de nube	Punto de conexión
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 (en la mayoría de las regiones)
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 obtener detalles sobre cómo configurar los permisos de buckets e información actualizada sobre los puntos de conexión de almacenamiento, consulte la documentación de su proveedor de nube.

Credenciales de almacenamiento

DataSync también necesita las credenciales para acceder al depósito de almacenamiento de objetos implicado en la transferencia. Puede tratarse de una clave de acceso y una clave secreta o algo similar, según la nomenclatura que utilice su proveedor de almacenamiento en la nube para referirse a estas credenciales.

Para obtener más información, consulte la documentación de su proveedor de nube.

Consideraciones a la hora de realizar una transferencia desde otro almacenamiento de objetos en la nube

Cuando planee transferir objetos hacia o desde otro proveedor de almacenamiento en la nube mediante el uso DataSync, hay algunas cosas que debe tener en cuenta.

Temas

- [Costos](#)
- [Clases de almacenamiento](#)
- [Etiquetas de objetos](#)
- [Transferencia a Amazon S3](#)

Costos

Las tarifas asociadas a la entrada y salida de datos de otro proveedor de almacenamiento en la nube pueden incluir:

- Ejecutar una EC2 instancia de [Amazon](#) para su DataSync agente
- Transferir los datos mediante el uso [DataSync](#), incluidos los cargos de solicitud relacionados con su almacenamiento de objetos en la nube y [Amazon S3](#) (si S3 es su destino de transferencia)
- Transferencia de datos desde o hacia su almacenamiento en la nube (consulte los precios de su proveedor de nube)
- Almacenar datos en un [servicio de AWS almacenamiento](#) compatible con DataSync
- Almacenamiento de datos en otro proveedor de nube (consulte los precios de su proveedor de nube)

Clases de almacenamiento

Algunos proveedores de almacenamiento en la nube tienen clases de almacenamiento (similares a [Amazon S3](#)) que no se DataSync pueden leer sin antes restaurarlas. Por ejemplo, Oracle Cloud Infrastructure Object Storage tiene una clase de almacenamiento de archivos. Debe restaurar los objetos de esa clase de almacenamiento antes de DataSync poder transferirlos. Para obtener más información, consulte la documentación de su proveedor de nube.

Etiquetas de objetos

No todos los proveedores de nube admiten etiquetas de objetos. Es posible que los que sí lo hagan no permitan consultar etiquetas a través de la API de Amazon S3. En cualquier situación, la tarea de DataSync transferencia podría fallar si intenta copiar las etiquetas de los objetos.

Para evitarlo, desactive la casilla de verificación Copiar etiquetas de objetos de la DataSync consola al crear, iniciar o actualizar la tarea.

Transferencia a Amazon S3

Al transferir a Amazon S3, no DataSync se pueden transferir objetos de más de 5 TB. DataSync además, solo puede copiar metadatos de objetos de hasta 2 KB.

Creando tu DataSync agente

Solo se necesita un DataSync agente cuando se transfieren datos entre sistemas de almacenamiento de otras nubes y Amazon EFS o Amazon FSx, o cuando se utilizan tareas en modo básico. No necesita un agente para transferir datos entre sistemas de almacenamiento de otras nubes y Amazon S3 mediante el modo mejorado. En esta sección se describe cómo implementar y activar un agente en una EC2 instancia de Amazon de su nube privada virtual (VPC) en AWS.

Para crear un EC2 agente de Amazon

1. [Despliega un EC2 agente de Amazon.](#)
2. [Elija un punto final de servicio](#) con el que el agente se comunique AWS.

En este caso, le recomendamos que utilice un punto de conexión de servicio de VPC.

3. Configure su red para que funcione con los [puntos de conexión del servicio de VPC](#).
4. [Active el agente.](#)

Creación de una ubicación de transferencia para su otro almacenamiento de objetos en la nube

Puede configurarlo DataSync para usar su almacenamiento de objetos en la nube como ubicación de origen o destino.

Antes de empezar

Asegúrese de saber [cómo DataSync accede a su almacenamiento de objetos en la nube](#). También necesitas un [DataSync agente](#) que pueda conectarse a tu almacenamiento de objetos en la nube.

1. Abre la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones y Crear ubicación.
3. En Tipo de ubicación, seleccione Almacenamiento de objetos.
4. En Servidor, introduce el [punto final](#) que DataSync puedes usar para acceder a tu almacenamiento de objetos en la nube:
 - 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 (en la mayoría de las regiones)
 - 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. En el campo Nombre del bucket, introduzca el nombre del bucket de almacenamiento de objetos desde o hacia el que va a transferir los datos.
6. En Carpeta, introduzca un prefijo de objeto. DataSync solo transfiere objetos con este prefijo.
7. Si su transferencia requiere un agente, elija Usar agentes y, a continuación, elija el DataSync agente que se pueda conectar con su almacenamiento de objetos en la nube.
8. Amplíe Configuración adicional. En Protocolo del servidor, seleccione HTTPS. En Puerto del servidor, seleccione 443.
9. Desplácese hasta la sección Autenticación. Asegúrese de que la casilla Requiere credenciales esté seleccionada y, a continuación, proporcione DataSync sus [credenciales de almacenamiento](#).
 - En Clave de acceso, introduzca el ID para acceder a su almacenamiento de objetos en la nube.

- En el caso de la clave secreta, proporciona la clave secreta para acceder a tu almacenamiento de objetos en la nube. Puedes introducir la clave directamente o especificar un AWS Secrets Manager secreto que contenga la clave. Para obtener más información, consulte [Proporcionar credenciales para las ubicaciones de almacenamiento](#).

10. (Opcional) Proporcione valores para los campos Clave y Valor para etiquetar la ubicación.

Las etiquetas le ayudan a administrar, filtrar y buscar sus AWS recursos. Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

11. Seleccione Crear ubicación.

Pasos a seguir a continuación

Cuando termines de crear una DataSync ubicación para tu almacenamiento de objetos en la nube, puedes seguir configurando la transferencia. Aquí se indican algunos pasos siguientes que se deben tener en cuenta:

1. Si aún no lo ha hecho, [cree otra ubicación](#) desde o hacia la que planea transferir sus datos en AWS.
2. Obtén información sobre cómo DataSync [se gestionan los metadatos y los archivos especiales](#) para las ubicaciones de almacenamiento de objetos.
3. Configure la forma en que se transfieren sus datos. Por ejemplo, tal vez solo desee [transferir un subconjunto de sus datos](#).

Important

Asegúrese de configurar correctamente la forma en que se DataSync copian las etiquetas de los objetos. Para obtener más información, consulte las consideraciones acerca de las [Etiquetas de objetos](#).

4. [Inicie la transferencia](#).

Transferencia a o desde un almacenamiento compatible con S3 en Snowball Edge

Con AWS DataSync, puede transferir objetos entre el [almacenamiento compatible con Amazon S3 en un AWS Snowball Edge](#) dispositivo o clúster y cualquiera de los siguientes servicios de AWS almacenamiento:

- [Amazon S3](#)
- [Amazon Elastic File System \(Amazon EFS\)](#)
- [Servidor FSx de archivos Amazon para Windows](#)
- [Amazon FSx para Lustre](#)
- [Amazon FSx para OpenZFS](#)
- [Amazon FSx para NetApp ONTAP](#)

Requisitos previos

Antes de comenzar, asegúrese de que ha hecho lo siguiente:

- Creó un recurso de AWS almacenamiento en el Región de AWS lugar desde o hacia el que planea transferir los datos. Por ejemplo, podría ser un bucket S3 o un sistema de archivos de Amazon EFS en el este de EE. UU. (Norte de Virginia).
- Ha establecido una conexión de red de área extendida (WAN) para el tráfico que entra y sale de su entorno de almacenamiento en las instalaciones. Por ejemplo, puede establecer este tipo de conexión con [AWS Direct Connect](#).

Cuando [cree su DataSync agente](#), configurará esta conexión WAN para que DataSync pueda transferir datos entre su almacenamiento local compatible con Amazon S3 y su recurso de almacenamiento interno. AWS

- Ha descargado e instalado el [cliente de Snowball Edge](#).

Proporcionar DataSync acceso al almacenamiento compatible con S3

Para acceder a su depósito de almacenamiento compatible con Amazon S3, DataSync necesita lo siguiente:

- Credenciales de usuario en su dispositivo o clúster de Snowball Edge que pueden acceder al bucket desde o hacia el que está transfiriendo los datos.
- Un certificado HTTPS que permita DataSync verificar la autenticidad de la conexión entre el DataSync agente y el s3api punto final de su dispositivo o clúster.

Temas

- [Obtención de las credenciales de usuario para acceder a su bucket de S3](#)
- [Obtención de un certificado para conectar el punto de conexión s3api](#)

Obtención de las credenciales de usuario para acceder a su bucket de S3

DataSync necesita la clave de acceso y la clave secreta para un usuario que pueda acceder al depósito con el que está trabajando en su dispositivo o clúster de Snowball Edge.

Cómo obtener las credenciales de usuario para acceder a su bucket

1. Abra una terminal y ejecute el cliente de Snowball Edge.

Para obtener más información acerca de ejecutar el cliente de Snowball Edge, consulte [Uso del cliente Snowball](#) en la Guía para desarrolladores de AWS Snowball Edge .

2. Para obtener las claves de acceso asociadas a su dispositivo o clúster, ejecute el siguiente comando de snowballEdge:

```
snowballEdge list-access-keys
```

3. En el resultado, busque la clave de acceso del bucket con el que DataSync funcionará (por ejemplo, AKIAIOSFODNN7EXAMPLE).
4. Para obtener la clave de acceso secreta, ejecute el siguiente comando snowballEdge. Sustituya *access-key-for-datasync* por la clave de acceso que encontró en el paso anterior.

```
snowballEdge get-secret-access-key --access-key-id access-key-for-datasync
```

El resultado incluye la clave secreta correspondiente a la clave de acceso (p. ej., wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY).

5. Guarde la clave de acceso y la clave secreta en un lugar que pueda recordar.

Necesitarás estas claves cuando [configures la ubicación de DataSync origen](#) de tu transferencia.

Obtención de un certificado para conectar el punto de conexión **s3api**

Necesita un certificado HTTPS que pueda comprobar la autenticidad de la conexión entre el DataSync agente y un dispositivo de s3api punto final del clúster o dispositivo Snowball Edge.

Cómo obtener un certificado para conectar el punto de conexión **s3api**

1. En el cliente de Snowball Edge, ejecute el siguiente comando `list-certificates`:

```
snowballEdge list-certificates
```

En la salida, tome nota del valor de `CertificateArn`. Este es el nombre de recurso de Amazon (ARN) del certificado. Necesitará el ARN para obtener el contenido del certificado.

2. Ejecute el siguiente comando `get-certificate` que especifica el ARN del certificado que acaba de recuperar:

```
snowballEdge get-certificate --certificate-arn arn:aws:snowball-  
device:::certificate/78EXAMPLE516EXAMPLEf538EXAMPLEa7
```

3. Copie el resultado, incluidas las líneas `BEGIN CERTIFICATE` y `END CERTIFICATE`, y guárdelo como un archivo `.pem`.

Ejemplo de salida de **get-certificate**:

```
-----BEGIN CERTIFICATE-----  
Certificate  
-----END CERTIFICATE-----
```

Debe especificar este `.pem` archivo al [crear la ubicación DataSync de origen](#) de la transferencia.

Crear un DataSync agente en su entorno de almacenamiento local

Durante una transferencia, DataSync utiliza un [agente](#) para leer o escribir en el almacenamiento compatible con Amazon S3 de su dispositivo o clúster Snowball Edge.

Este agente debe implementarse en su entorno de almacenamiento en las instalaciones, donde pueda conectarse a su dispositivo o clúster a través de la red. Por ejemplo, puede ejecutar el agente en un VMware ESXi hipervisor que tenga acceso a la red local a su clúster.

Para crear un DataSync agente en su entorno de almacenamiento local

1. Asegúrese de que el [DataSync agente se pueda ejecutar en su hipervisor](#) y de que le [asigne suficientes recursos de máquina virtual \(VM\)](#).
2. Implemente el agente en el entorno en las instalaciones.

A fin de obtener instrucciones, consulte uno de los siguientes temas, en función del tipo de hipervisor en el que vaya a implementar el agente:

- [Implemente su agente en VMware](#)
- [Implementación del agente en una máquina basada en el kernel de Linux \(KVM\)](#)
- [Implementación del agente en Microsoft Hyper-V](#)
- [Despliega a tu agente en Amazon EC2](#)

 Warning

No recomendamos implementar un agente en Amazon EC2 Agent para acceder al almacenamiento local debido al aumento de la latencia de la red.

3. Configure su red para permitir el siguiente tráfico entre el agente y su almacenamiento compatible con Amazon S3:

De	Para	Puerto y protocolo
DataSync agente	Una interfaz de red virtual (VNI) para un punto de conexión s3api de su dispositivo o clúster. Si tiene un clúster, puede ser cualquier VNI del punto de conexión s3api.	TCP 443 (HTTPS)

Si necesita encontrar un VNI en su dispositivo o clúster, consulte [Describing your virtual network interfaces](#) en Snowball Edge.

4. [Elija un punto final de servicio](#) que el agente utilice para comunicarse con el DataSync servicio.
5. [Activación del agente](#).

Configuración de la ubicación de origen de la transferencia

Tras crear el agente, puede configurar la ubicación de origen de la DataSync transferencia.

Note

En las siguientes instrucciones se da por hecho que realiza la transferencia desde un almacenamiento compatible con Amazon S3, pero también puede utilizar esta ubicación como destino de la transferencia.

Para configurar la ubicación de origen mediante la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos. Elija Tareas y luego Crear tarea.
3. En la página Configure source location (Configurar ubicación de origen), seleccione Create a new location (Crear una nueva ubicación).
4. En Tipo de ubicación, seleccione Almacenamiento de objetos.
5. En el caso de los agentes, elija el DataSync agente que creó en su entorno de almacenamiento local.
6. En Servidor, introduzca el VNI del punto de conexión s3api que utiliza su almacenamiento compatible con Amazon S3.

Si tiene un clúster de Snowball Edge en lugar de un único dispositivo, puede especificar cualquiera de los puntos finales del s3api clúster. VNIs

7. En Nombre del bucket, introduzca el nombre del bucket de almacenamiento compatible con Amazon S3 desde el que está transfiriendo los objetos.
8. En Carpeta, introduzca un prefijo de objeto.

DataSync solo transfiere objetos con este prefijo.

9. Para configurar la DataSync conexión al dispositivo o clúster de Snowball Edge, expanda Configuración adicional y haga lo siguiente:
 - a. En Protocolo del servidor, seleccione HTTPS.
 - b. En Puerto del servidor, introduzca **443**.
 - c. En Certificado, elija el archivo de certificado para la [conexión del punto de conexión s3api](#).
10. Seleccione Requiere credenciales e introduzca la Clave de acceso y la Clave secreta para [acceder al bucket de almacenamiento compatible con Amazon S3](#) de su dispositivo o clúster de Snowball Edge.
11. Elija Next.

Configuración de la ubicación de destino de la transferencia

La ubicación de destino de su transferencia debe estar en la misma ubicación Región de AWS y Cuenta de AWS en la que creó su agente.

Antes de empezar: compruebe que ha [configurado la ubicación de origen](#) de la transferencia.

Para configurar la ubicación de destino de la transferencia mediante la DataSync consola

1. En la página Configurar la ubicación de destino, selecciona Crear una nueva ubicación o Elegir una ubicación existente para el recurso AWS de almacenamiento al que vas a transferir los objetos.

Si va a crear una nueva ubicación, consulte uno de los siguientes temas:

- [Amazon S3](#)
- [Amazon EFS](#)
- [FSx para Windows File Server](#)
- [FSx para Lustre](#)
- [FSx para OpenZFS](#)
- [FSx para ONTAP](#)

2. Cuando haya terminado de configurar la ubicación de destino, seleccione Siguiente.

Configuración de los ajustes de su transferencia

Con DataSync, puede especificar un programa de transferencia, personalizar la forma en que se verifica la integridad de los datos y especificar si desea transferir solo un subconjunto de objetos, entre otras opciones.

Antes de empezar: compruebe que ha [configurado la ubicación de destino](#) de la transferencia.

Para configurar los ajustes de transferencia mediante la consola DataSync

1. En la página Configurar ajustes, cambie los ajustes de la transferencia o utilice los valores predeterminados.

Para obtener más información sobre estas opciones, consulte [Elegir qué AWS DataSync se transfiere](#).

2. Elija Next.
3. Revise los detalles de su transferencia y, a continuación, elija Crear tarea.

Inicio de la transferencia

Después de crear la tarea de transferencia, ya puede comenzar a mover los datos. Para obtener instrucciones sobre cómo iniciar una tarea mediante la DataSync consola o AWS CLI, consulte [Cómo iniciar la tarea](#).

Limitaciones

- Si el sistema de almacenamiento de origen utiliza el protocolo NFS (como Amazon EFS), no DataSync podrá transferir archivos con vínculos físicos a un dispositivo Snowball Edge.
- DataSync no puede transferir objetos de más de 1024 bytes de un dispositivo Snowball Edge a un bucket de S3. Para obtener más información, consulte la [Guía del usuario de Amazon S3](#).

Crear una tarea para transferir sus datos

Una tarea describe dónde y cómo se AWS DataSync transfieren los datos. Una tarea consta de lo siguiente:

- [Ubicación de origen](#): el sistema o servicio de almacenamiento desde el que se DataSync transfieren los datos.

- [Ubicación de destino](#): el sistema o servicio de almacenamiento al que se DataSync transfieren los datos.
- [Opciones de tareas](#): ajustes como los archivos que se van a transferir, cómo se verifican los datos, cuándo se ejecuta la tarea, etc.
- [Ejecuciones de tareas](#): cuando ejecuta una tarea, esto se llama ejecución de tareas.

Creación de su tarea de

Al crear una DataSync tarea, se especifican las ubicaciones de origen y destino. También puede personalizar la tarea eligiendo qué archivos desea transferir, cómo se gestionan los metadatos, estableciendo un cronograma y mucho más.

Antes de crear la tarea, asegúrate de entender [cómo funcionan DataSync las transferencias](#) y revisa las [cuotas de tareas](#).

Important

Si planea transferir datos a o desde una ubicación de Amazon S3, consulte [cómo DataSync pueden afectar los cargos por solicitud de S3](#) y la [página de DataSync precios](#) antes de empezar.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. Asegúrese de estar en uno de los Regiones de AWS lugares donde planea transferir datos.
3. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
4. En la página Configure source location (Configurar ubicación de origen) elija [crear](#) o elija una ubicación de origen y después elija Next (Siguiendo).
5. En la página Configurar ubicación de destino, [crea](#) o elige una ubicación de destino y, a continuación, selecciona Siguiendo.
6. (Recomendado) En la página de configuración, asigne a la tarea un nombre que pueda recordar.
7. Mientras se encuentre en la página de configuración, elija las opciones de la tarea o utilice la configuración predeterminada.

Puede que te interesen algunas de las siguientes opciones:

- Especifica el [modo de tarea](#) que deseas usar.
- Especifique qué datos desea transferir mediante un [manifiesto](#) o [filtros](#).
- Configure cómo [gestionar los metadatos de los archivos](#) y [verificar la integridad de los datos](#).
- Supervisa tu transferencia con [informes de tareas](#) o [Amazon CloudWatch](#). Le recomendamos configurar algún tipo de supervisión para su tarea.

Cuando haya terminado, elija Siguiente.

8. Revise la configuración de la tarea y después elija Crear tarea.

Ya está listo para [comenzar su tarea](#).

Usando el AWS CLI

Una vez que [haya creado las ubicaciones de DataSync origen y destino](#), podrá crear su tarea.

1. En AWS CLI la configuración, asegúrate de usar una de las ubicaciones en las Regiones de AWS que planeas transferir los datos.
2. Copie el siguiente 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. Para --source-location-arn, especifique el nombre de recurso de Amazon (ARN) de la ubicación de origen.
4. Para --destination-location-arn, especifique el ARN de la ubicación de destino.

Si realizas una transferencia entre Regiones de AWS nuestras cuentas, asegúrate de que el ARN incluya la otra región o ID de cuenta.

5. (Recomendado) Para --name, especifique un nombre para la tarea que pueda recordar.
6. Especifique otras opciones de tareas según sea necesario. Puede que te interesen algunas de las siguientes opciones:

- Especifique qué datos desea transferir mediante un [manifiesto](#) o [filtros](#).
- Configure cómo [gestionar los metadatos de los archivos](#) y [verificar la integridad de los datos](#).
- Supervisa tu transferencia con [informes de tareas](#) o [Amazon CloudWatch](#). Le recomendamos configurar algún tipo de supervisión para su tarea.

Para ver más opciones, consulta [create-task](#). A continuación, se muestra un create-task comando de ejemplo que especifica varias opciones:

```
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. Ejecute el comando create-task.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la tarea que creó. Por ejemplo:

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/task-08de6e6697796f026"
}
```

Ya está listo para [comenzar su tarea](#).

Estados de las tareas

Cuando creas una DataSync tarea, puedes comprobar su estado para ver si está lista para ejecutarse.

Estado de la consola	Estado de la API	Descripción
Disponible	AVAILABLE	La tarea está lista para empezar a transferir datos.
Running	RUNNING	La ejecución de una tarea está en curso. Para obtener más información, consulte Estados de ejecución de las tareas .
No disponible	UNAVAILABLE	Un DataSync agente utilizado por la tarea está desconectado. Para obtener más información, consulte ¿Qué hago si mi agente está desconectado?
En cola	QUEUED	Se está ejecutando otra tarea en la que se utiliza el mismo DataSync agente. Para obtener más información, consulte Saber cuándo la tarea está en cola .

Particionar grandes conjuntos de datos con múltiples tareas

Si va a transferir un conjunto de datos grande, como [migrar](#) millones de archivos u objetos, le recomendamos particionar el conjunto de datos con varias tareas. DataSync Dividir los datos de origen en varias tareas (y, posiblemente, en [agentes](#), según las ubicaciones) ayuda a reducir el tiempo que se tarda en DataSync preparar y transferir los datos.

Considere algunas de las formas en que puede particionar un conjunto de datos grande en varias DataSync tareas:

- Crea tareas que transfieran carpetas independientes. Por ejemplo, puede crear dos tareas que tengan como destino `/FolderA` y `/FolderB`, respectivamente, en el almacenamiento de origen.
- Cree tareas que transfieran subconjuntos de archivos, objetos y carpetas mediante un [manifiesto](#) o [filtros](#).

Tenga en cuenta que este enfoque puede aumentar las I/O operaciones de almacenamiento y afectar al ancho de banda de la red. Para obtener más información, consulte el blog sobre [Cómo acelerar las transferencias de datos con arquitecturas DataSync escalables](#).

Segmentación de los datos transferidos con múltiples tareas

Si va a transferir diferentes conjuntos de datos al mismo destino, puede crear varias tareas para ayudar a segmentar los datos que transfiere.

Por ejemplo, si va a realizar la transferencia al mismo bucket de S3 denominado MyBucket, puede crear distintos prefijos en el bucket que correspondan a cada tarea. Este enfoque evita que el nombre del archivo entre en conflicto con los conjuntos de datos y te permite establecer diferentes permisos para cada prefijo. A continuación le explicamos cómo puede configurar esto:

1. Cree tres prefijos en el destino MyBucket denominado task1, task2 y task3:
 - s3://MyBucket/task1
 - s3://MyBucket/task2
 - s3://MyBucket/task3
2. Cree tres DataSync tareas denominadas task1task2, y task3 que se transfieran al prefijo correspondiente en. MyBucket

Elegir un modo de tarea para la transferencia de datos

AWS DataSync La tarea se puede ejecutar en uno de los siguientes modos:

- Modo mejorado: transfiere un número prácticamente ilimitado de objetos con un rendimiento superior al del modo básico. Las tareas del modo mejorado optimizan el proceso de transferencia de datos al enumerar, preparar, transferir y verificar los datos en paralelo. El modo mejorado está disponible actualmente para transferencias entre ubicaciones de Amazon S3, transferencias entre Amazon S3 Azure Blob y Amazon S3 sin agente y transferencias entre otras nubes y Amazon S3 sin agente.
- Modo básico: transfiere archivos u objetos entre el AWS almacenamiento y todas las demás DataSync ubicaciones compatibles. Las tareas del modo básico están sujetas a [cuotas](#) en cuanto al número de archivos, objetos y directorios de un conjunto de datos. El modo básico prepara, transfiere y verifica los datos de forma secuencial, lo que lo hace más lento que el modo mejorado para la mayoría de las cargas de trabajo.

Comprender las diferencias entre los modos de tarea

La siguiente información puede ayudarle a determinar qué modo de tarea debe utilizar.

Funcionalidad	Comportamiento de modo mejorado	Comportamiento del modo básico
Rendimiento	DataSync enumera, prepara, transfiere y verifica sus datos en paralelo. Ofrece un rendimiento superior al del modo básico para la mayoría de las cargas de trabajo (como la transferencia de objetos grandes)	DataSync prepara, transfiere y verifica los datos de forma secuencial. El rendimiento es más lento que en el modo mejorado para la mayoría de las cargas de trabajo
Número de elementos de un conjunto de datos con los que DataSync se puede trabajar por ejecución de tarea	Un número prácticamente ilimitado de objetos	Se aplican cuotas
Contadores y métricas de transferencia de datos	Más contadores y métricas que en el modo Básico, como el número de objetos que DataSync se encuentran en la ubicación de origen y el número de objetos que se preparan durante la ejecución de cada tarea	Menos contadores y métricas que en el modo mejorado
Registro	Registros estructurados (formato JSON)	Registros no estructurados
Ubicaciones compatibles	Actualmente, para transferencias entre ubicaciones de Amazon S3, transferencias entre Amazon S3 Azure Blob y Amazon S3 sin agente y transferencias entre otras nubes y Amazon S3 sin agente.	Para transferencias entre todas las ubicaciones DataSync compatibles

Funcionalidad	Comportamiento de modo mejorado	Comportamiento del modo básico
Opciones de verificación de datos	DataSync verifica solo los datos transferidos	DataSync verifica todos los datos de forma predeterminada
límites de ancho de banda	No aplicable	Compatible
Costo	Para obtener más información, consulta la página DataSync de precios	Para obtener más información, consulta la página DataSync de precios
Gestión de errores en el caso de etiquetas de objetos no compatibles	En el caso de las transferencias de almacenamiento en la nube hacia o desde ubicaciones que no admiten el etiquetado de objetos, la ejecución de la tarea fallará inmediatamente si la <code>ObjectTags</code> opción no está especificada o está configurada en. <code>PRESERVE</code>	En el caso de las transferencias de almacenamiento en la nube hacia o desde ubicaciones que no admiten el etiquetado de objetos, la ejecución de las tareas se ejecutará con normalidad, pero notificará los errores por objeto de los objetos etiquetados si la <code>ObjectTags</code> opción no está especificada o está configurada en. <code>PRESERVE</code>

Elegir un modo de tarea

Puede elegir el modo mejorado solo para las transferencias entre ubicaciones de Amazon S3, las transferencias entre Amazon S3 Azure Blob y Amazon S3 sin un agente y las transferencias entre otras nubes y Amazon S3 sin un agente. De lo contrario, debe utilizar el modo básico. Por ejemplo, una transferencia desde una ubicación [NFS local a una ubicación](#) S3 requiere el modo básico.

Las opciones y el rendimiento de las tareas pueden variar en función del modo de tarea que elija. Una vez creada la tarea, no podrá cambiar el modo de la tarea.

Permisos necesarios

Para crear una tarea en modo mejorado, el rol de IAM que utilices DataSync debe tener el `iam:CreateServiceLinkedRole` permiso.

Para tus permisos DataSync de usuario, considera [AWSDataSyncFullAccess](#) utilizarlos. Se trata de una política AWS gestionada que proporciona al usuario un acceso total DataSync y mínimo a sus dependencias.

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en. <https://console.aws.amazon.com/datasync/>
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. Para el modo Tarea, elija una de las siguientes opciones:
 - Mejorado
 - Básica

Para obtener más información, consulte [Comprender las diferencias entre los modos de tarea](#).

5. Mientras se encuentre en la página de configuración, elija otras opciones de tareas o utilice la configuración predeterminada.

Puede que te interesen algunas de las siguientes opciones:

- Especifique qué datos desea transferir mediante un [manifiesto](#) o [filtros](#).
- Configure cómo [gestionar los metadatos de los archivos](#) y [verificar la integridad de los datos](#).
- Supervisa tu transferencia con [informes de tareas](#) o [Amazon CloudWatch Logs](#).

Cuando haya terminado, elija Siguiente.

6. Revise la configuración de la tarea y después elija Crear tarea.

Usando el AWS CLI

1. En tu AWS CLI configuración, asegúrate de usar uno de los Regiones de AWS lugares donde planeas transferir datos.
2. Copie el siguiente 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. Para `--source-location-arn`, especifique el nombre de recurso de Amazon (ARN) de la ubicación de origen.
4. Para `--destination-location-arn`, especifique el ARN de la ubicación de destino.

Si realizas una transferencia entre Regiones de AWS nuestras cuentas, asegúrate de que el ARN incluya la otra región o ID de cuenta.

5. Para `--task-mode`, especifique `ENHANCED` o `BASIC`

Para obtener más información, consulte [Comprender las diferencias entre los modos de tarea](#).

6. Especifique otras opciones de tareas según sea necesario. Puede que te interesen algunas de las siguientes opciones:

- Especifique qué datos desea transferir mediante un [manifiesto](#) o [filtros](#).
- Configure cómo [gestionar los metadatos de los archivos](#) y [verificar la integridad de los datos](#).
- Supervisa tu transferencia con [informes de tareas](#) o [Amazon CloudWatch Logs](#).

Para ver más opciones, consulta [create-task](#). Este es un ejemplo de `create-task` comando que especifica el modo mejorado y varias opciones más:

```
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. Ejecute el comando `create-task`.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la tarea que creó. Por ejemplo:

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Uso de la DataSync API

Puede especificar el modo de DataSync tarea configurando el `TaskMode` parámetro en la [CreateTask](#) operación.

Elegir qué AWS DataSync se transfiere

AWS DataSync le permite elegir qué desea transferir y cómo quiere que se traten sus datos. Algunas opciones son:

- Transferir una lista exacta de archivos u objetos mediante un manifiesto.
- Incluir o excluir ciertos tipos de datos en su transferencia mediante un filtro.
- En el caso de las transferencias periódicas, se mueven solo los datos que han cambiado desde la última transferencia
- Sobrescribir los datos de la ubicación de destino para que coincidan con los de la ubicación de origen.
- Elegir qué metadatos de archivo u objeto se van a conservar en las distintas ubicaciones de almacenamiento.

Temas

- [Transferir archivos u objetos específicos mediante un manifiesto](#)
- [Transferencia de archivos, objetos y carpetas específicos mediante filtros](#)
- [Comprenda cómo DataSync gestiona los metadatos de archivos y objetos](#)

- [Enlaces y directorios copiados por AWS DataSync](#)
- [Configuración de la forma en que gestionan los archivos, los objetos y los metadatos](#)

Transferir archivos u objetos específicos mediante un manifiesto

Un manifiesto es una lista de archivos u objetos que AWS DataSync deseas transferir. Por ejemplo, en lugar de tener que transferir todo lo que hay en un bucket de S3 con potencialmente millones de objetos, DataSync transfiere solo los objetos que incluyes en tu manifiesto.

Los manifiestos son similares a los [filtros](#), pero permiten identificar exactamente qué archivos u objetos se van a transferir en lugar de datos que coincidan con un patrón de filtro.

Creación de un manifiesto

Un manifiesto es un archivo con formato de valores separados por comas (CSV) en el que se enumeran los archivos u objetos de la ubicación de origen que deseas transferir. DataSync Si el origen es un bucket de S3, también puede incluir la versión de un objeto que desea transferir.

Temas

- [Directrices](#)
- [Ejemplos de manifiestos](#)

Directrices

Usa estas pautas para ayudarte a crear un manifiesto que funcione con. DataSync

Do

- Especifique la ruta completa de cada archivo u objeto que desea transferir.

No puede especificar solo un directorio o una carpeta con la intención de transferir todo su contenido. En estas situaciones, considere usar un [filtro de inclusión](#) en lugar de un manifiesto.

- Asegúrese de que la ruta de cada archivo u objeto es relativa a la ruta de montaje, carpeta, directorio o prefijo que especificó al configurar la ubicación de DataSync origen.

Por ejemplo, supongamos que [configura una ubicación de S3](#) con un prefijo denominado photos. Ese prefijo incluye un objeto my-picture.png que desea transferir. En el manifiesto, solo necesita especificar el objeto (my-picture.png) en lugar del prefijo y el objeto (photos/my-picture.png).

- Para especificar la versión del objeto de Amazon S3 IDs, separe la ruta del objeto y el ID de versión mediante una coma.

En el siguiente ejemplo, se muestra una entrada de manifiesto con dos campos. El primer campo incluye un objeto denominado `picture1.png`. El segundo campo está separado por una coma e incluye un identificador de versión de `111111`:

```
picture1.png,111111
```

- Utilice comillas en las siguientes situaciones:
 - Cuando una ruta contiene caracteres especiales (comas, comillas y finales de línea):

```
"filename,with,commas.txt"
```

- Cuando una ruta abarca varias líneas:

```
"this  
is  
a  
filename.txt"
```

- Cuando una ruta incluye comillas:

```
filename""with""quotes.txt
```

Esto representa una ruta denominada `filename"with"quotes.txt`.

Estas reglas de citación también se aplican a los campos de ID de versión. En general, si el campo de un manifiesto tiene una comilla, debes incluir otra comilla de cierre.

- Separe cada entrada de archivo u objeto con una línea nueva.

Puede separar las líneas mediante saltos de línea al estilo Linux (avance de línea o corte de línea) o Windows (corte de línea seguido de un corte de línea).

- Guarda el manifiesto (por ejemplo, `my-manifest.csv` o `my-manifest.txt`).
- Cargue el manifiesto en un bucket de S3 al que [DataSync pueda acceder](#).

Este depósito no tiene que estar en la misma cuenta Región de AWS o en la misma cuenta en la que lo estás usando DataSync.

Don't

- Especifique solo un directorio o una carpeta con la intención de transferir todo su contenido.

Un manifiesto solo puede incluir las rutas completas de los archivos y los objetos que desea transferir. Si configura la ubicación de origen para usar una ruta de montaje, carpeta, directorio o prefijo específicos, no tiene que incluirlos en el manifiesto.

- Especifique una ruta de archivo u objeto que supere los 4096 caracteres.
- Especifique una ruta de archivo, una ruta de objeto o un ID de versión del objeto de Amazon S3 que supere los 1024 bytes.
- Especifique rutas de archivos u objetos duplicadas.
- Incluye un identificador de versión del objeto si la ubicación de origen no es un bucket de S3.
- Incluye más de dos campos en una entrada de manifiesto.

Una entrada solo puede incluir una ruta de archivo u objeto y (si corresponde) un ID de versión del objeto de Amazon S3.

- Incluya caracteres que no se ajusten a la codificación UTF-8.
- Incluya espacios no intencionados en sus campos de entrada fuera de las comillas.

Ejemplos de manifiestos

Usa estos ejemplos para ayudarte a crear un manifiesto que funcione con DataSync.

Manifiesto con rutas completas de archivos u objetos

En el siguiente ejemplo se muestra un manifiesto con las rutas completas de los archivos u objetos que desea transferir.

```
photos/picture1.png  
photos/picture2.png  
photos/picture3.png
```

Manifiesto solo con claves de objetos

El siguiente ejemplo muestra un manifiesto con objetos para transferir desde una ubicación de origen de Amazon S3. Como la [ubicación está configurada](#) con el prefijo photos, solo se especifican las claves de los objetos.

```
picture1.png  
picture2.png  
picture3.png
```

Manifiesto con las rutas y la versión de los objetos IDs

Las dos primeras entradas del siguiente ejemplo de manifiesto incluyen versiones específicas de objetos de Amazon S3 que se van a transferir.

```
photos/picture1.png,111111  
photos/picture2.png,121212  
photos/picture3.png
```

Manifiesto con caracteres UTF-8

En el siguiente ejemplo se muestra un manifiesto con archivos que incluyen caracteres UTF-8.

```
documents/résumé1.pdf  
documents/résumé2.pdf  
documents/résumé3.pdf
```

Proporcionar DataSync acceso a tu manifiesto

Necesitas un rol AWS Identity and Access Management (de IAM) que dé DataSync acceso a tu manifiesto en su bucket de S3. Este rol debe incluir los permisos siguientes:

- `s3:GetObject`
- `s3:GetObjectVersion`

Puede generar este rol automáticamente en la DataSync consola o crearlo usted mismo.

Note

Si tu manifiesto está en otro lugar Cuenta de AWS, debes crear este rol manualmente.

Creación automática del rol de IAM

Al crear o iniciar una tarea de transferencia en la consola, DataSync puedes crearte un rol de IAM con los `s3:GetObjectVersion` permisos `s3:GetObject` y los que necesitas para acceder a tu manifiesto.

Permisos necesarios para crear el rol automáticamente

Para crear el rol automáticamente, asegúrate de que el rol que estás usando para acceder a la DataSync consola tenga los siguientes permisos:

- `iam:CreateRole`
- `iam:CreatePolicy`
- `iam:AttachRolePolicy`

Crear el rol de IAM (misma cuenta)

Puedes crear manualmente el rol de IAM que DataSync necesita acceder a tu manifiesto. En las siguientes instrucciones se da por sentado que estás en el mismo Cuenta de AWS lugar en el que lo usas DataSync y que se encuentra el bucket de S3 del manifiesto.

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación situado a la izquierda, en Administración de acceso, elija Roles y luego Crear rol.
3. En la página Seleccionar entidad de confianza, en Tipo de entidad de confianza, elija Servicio de AWS.
4. En Caso de uso, elige una opción DataSync en la lista desplegable y selecciona DataSync. Elija Siguiente.
5. En la página Agregar permisos, elija Siguiente. Introduzca un nombre de rol y elija Crear rol.
6. En la página Roles, busque el rol que acaba de crear y seleccione el nombre.
7. En la página de detalles del rol, elija la pestaña Permisos. Elija Agregar permisos y luego Crear política insertada.
8. Elija la pestaña JSON y pegue la siguiente política de ejemplo en el 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. En la política de ejemplo que acaba de pegar, sustituya los siguientes valores por los suyos:
 - a. Reemplace *amzn-s3-demo-bucket* por el nombre del bucket de S3 que aloja el manifiesto.
 - b. Reemplace *my-manifest.csv* por el nombre del archivo de su manifiesto.
10. Elija Siguiente. Escriba un nombre para la política y elija Crear política.
11. (Recomendado) Para evitar el [problema del suplente confuso entre servicios](#), haga lo siguiente:
 - a. En la página de detalles del rol, elija la pestaña Relaciones de confianza. Elija Editar la política de confianza.
 - b. Actualice la política de confianza mediante el siguiente ejemplo, que incluye las claves de contexto de condición global de `aws:SourceArn` y `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:"  
  }  
}  
}]  
}
```

- Sustituya cada instancia *account-id* por el Cuenta de AWS ID en el que la esté utilizando DataSync.
 - *region* Sustitúyala por la ubicación Región de AWS que estás utilizando DataSync.
- c. Elija Actualizar política.

Has creado un rol de IAM que te permite acceder DataSync a tu manifiesto. Especifique este rol al [crear](#) o [iniciar](#) la tarea.

Crear el rol de IAM (cuenta diferente)

Si tu manifiesto está en un bucket de S3 que pertenece a otro Cuenta de AWS, debes crear manualmente el rol de IAM que se DataSync utiliza para acceder al manifiesto. Luego, Cuenta de AWS en la ubicación del manifiesto, debes incluir el rol en la política del bucket de S3.

Creación del rol

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación situado a la izquierda, en Administración de acceso, elija Roles y luego Crear rol.
3. En la página Seleccionar entidad de confianza, en Tipo de entidad de confianza, elija Servicio de AWS.
4. En Caso de uso, elige una opción DataSync en la lista desplegable y selecciona DataSync. Elija Siguiente.
5. En la página Agregar permisos, elija Siguiente. Introduzca un nombre de rol y elija Crear rol.
6. En la página Roles, busque el rol que acaba de crear y seleccione el nombre.
7. En la página de detalles del rol, elija la pestaña Permisos. Elija Agregar permisos y luego Crear política insertada.
8. Elija la pestaña JSON y pegue la siguiente política de ejemplo en el 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. En la política de ejemplo que acaba de pegar, sustituya los siguientes valores por los suyos:
 - a. Reemplace *amzn-s3-demo-bucket* por el nombre del bucket de S3 que aloja el manifiesto.
 - b. Reemplace *my-manifest.csv* por el nombre del archivo de su manifiesto.
10. Elija Siguiente. Escriba un nombre para la política y elija Crear política.
11. (Recomendado) Para evitar el [problema del suplente confuso entre servicios](#), haga lo siguiente:
 - a. En la página de detalles del rol, elija la pestaña Relaciones de confianza. Elija Editar la política de confianza.
 - b. Actualice la política de confianza mediante el siguiente ejemplo, que incluye las claves de contexto de condición global de `aws:SourceArn` y `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:*"
            }
        }
    }
}

```

- Sustituya cada instancia *account-id* de por el Cuenta de AWS ID que esté utilizando DataSync.
 - *region* Reemplázala por la Región de AWS que estás usando DataSync.
- c. Elija Actualizar política.

Ha creado el rol de IAM que puede incluir en su política de bucket de S3.

Actualización de la política del bucket de S3 con el rol

Una vez que hayas creado el rol de IAM, debes añadirlo a la política de bucket de S3 en el otro Cuenta de AWS lugar en el que se encuentra tu manifiesto.

1. En el AWS Management Console, cambia a la cuenta con el bucket de S3 de tu manifiesto.
2. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
3. En la página de detalles del bucket, elija la pestaña Permisos.
4. En Política de buckets, seleccione Editar y haga lo siguiente para modificar su política de bucket de S3:
 - a. Actualice lo que hay en el editor para incluir las siguientes declaraciones 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* Sustitúyelo por el Cuenta de AWS ID de la cuenta con la que lo estás utilizando DataSync .
 - c. *datasync-role* Sustitúyalo por el rol de IAM que acabas de crear y que permite acceder DataSync a tu manifiesto.
 - d. Reemplace *amzn-s3-demo-bucket* por el nombre del bucket de S3 que aloja el manifiesto en el otro Cuenta de AWS.
5. Seleccione Save changes (Guardar cambios).

Has creado un rol de IAM que te permite acceder DataSync a tu manifiesto en la otra cuenta. Especifique este rol al [crear](#) o [iniciar](#) la tarea.

Especificar el manifiesto al crear una tarea

Puedes especificar el manifiesto que quieres usar DataSync al crear una tarea.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación de la izquierda, seleccione Tasks (Tareas) y, a continuación, seleccione Create task (Crear tarea).
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. Para Contenido a digitalizar, seleccione Archivos, objetos y carpetas específicos y, a continuación, seleccione Uso de un manifiesto.
5. Para el URI de S3, elija el manifiesto que esté alojado en un bucket de S3.

De forma alternativa, puede introducir el URI (por ejemplo, `s3://bucket/prefix/my-manifest.csv`).

6. En la versión Object, elige la versión del manifiesto que DataSync quieres usar.

De forma predeterminada, DataSync usa la última versión del objeto.

7. Para rol de acceso al manifiesto, realice una de las operaciones siguientes:
 - Seleccione Generar automáticamente DataSync para crear automáticamente un rol de IAM con los permisos necesarios para acceder al manifiesto en su bucket de S3.
 - Elija un rol de IAM existente que pueda acceder a su manifiesto.

Para obtener más información, consulte [Proporcionar DataSync acceso a tu manifiesto](#).

8. Configure cualquier otro ajuste que desee para las tareas y, a continuación, seleccione Siguiente.
9. Seleccione Crear tarea.

Usando el AWS CLI

1. Copie el siguiente 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. Para el parámetro --source-location-arn, especifique el nombre de recurso de Amazon (ARN) de la ubicación desde la que transfiere los datos.
3. Para el parámetro --destination-location-arn, especifique el ARN de la ubicación a la que transfiere los datos.

4. Para el parámetro `--manifest-config`, haga lo siguiente:

- `ManifestObjectPath`: especifique la clave de objeto S3 de su manifiesto.
- `BucketAccessRoleArn`— Especifique la función de IAM que permite acceder DataSync al manifiesto en su bucket de S3.

Para obtener más información, consulte [Proporcionar DataSync acceso a tu manifiesto](#).

- `S3BucketArn`: especifique el ARN del bucket de S3 que aloja el manifiesto.
- `ManifestObjectVersionId`— Especifica la versión del manifiesto que quieres DataSync usar.

De forma predeterminada, DataSync utiliza la última versión del objeto.

5. Ejecute el comando `create-task` para crear la tarea.

Cuando lo tenga todo listo, puede [iniciar la tarea de transferencia](#).

Especificar el manifiesto al iniciar una tarea

Puede especificar el manifiesto que desea usar DataSync al ejecutar una tarea.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación de la izquierda, elija Tasks (Tareas) y, a continuación, elija la tarea que desea iniciar.
3. En la página de descripción general de la tarea, elija Iniciar y, a continuación, elija Comenzar con las opciones de anulación.
4. Para Contenido a digitalizar, seleccione Archivos, objetos y carpetas específicos y, a continuación, seleccione Uso de un manifiesto.
5. Para el URI de S3, elija el manifiesto que esté alojado en un bucket de S3.

De forma alternativa, puede introducir el URI (por ejemplo, `s3://bucket/prefix/my-manifest.csv`).

6. En la versión Object, elige la versión del manifiesto que DataSync quieres usar.

De forma predeterminada, DataSync usa la última versión del objeto.

7. Para rol de acceso al manifiesto, realice una de las operaciones siguientes:
 - Seleccione Generar automáticamente DataSync para crear automáticamente un rol de IAM para acceder al manifiesto en su bucket de S3.
 - Elija un rol de IAM existente que pueda acceder a su manifiesto.

Para obtener más información, consulte [Proporcionar DataSync acceso a tu manifiesto](#).

8. Elija Iniciar para comenzar la transferencia.

Usando el AWS CLI

1. Copie el siguiente 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. Para el parámetro `--task-arn`, especifique el nombre de recurso de Amazon (ARN) de la tarea que está iniciando.
3. Para el parámetro `--manifest-config`, haga lo siguiente:
 - `ManifestObjectPath`: especifique la clave de objeto S3 de su manifiesto.
 - `BucketAccessRoleArn`— Especifique la función de IAM que permite acceder DataSync al manifiesto en su bucket de S3.

Para obtener más información, consulte [Proporcionar DataSync acceso a tu manifiesto](#).

- `S3BucketArn`: especifique el ARN del bucket de S3 que aloja el manifiesto.

- `ManifestObjectVersionId`— Especifica la versión del manifiesto que quieres DataSync usar.

De forma predeterminada, DataSync utiliza la última versión del objeto.

4. Ejecute el comando `start-task-execution` para iniciar la transferencia.

Limitaciones

- No puede usar un manifiesto junto con [filtros](#).
- No puede especificar solo un directorio o una carpeta con la intención de transferir todo su contenido. En estas situaciones, considere usar un [filtro de inclusión](#) en lugar de un manifiesto.
- No puedes usar la opción de tarea Conservar los archivos eliminados (`PreserveDeletedFiles` de la [API](#)) para [mantener archivos u objetos en el destino que no estén en el origen](#). DataSync solo transfiere lo que aparece en tu manifiesto y no borra nada del destino.

Solución de problemas

Si estás transfiriendo objetos con una versión específica IDs desde un bucket de S3, es posible que veas un error relacionado con `HeadObject` o `GetObjectTagging`. Por ejemplo, aquí hay un error relacionado con `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
```

Si ve alguno de estos errores, compruebe que la función de IAM que se DataSync utiliza para acceder a la ubicación de origen de S3 tenga los siguientes permisos:

- `s3:GetObjectVersion`
- `s3:GetObjectVersionTagging`

Si necesita actualizar su rol con estos permisos, consulte [Crear un rol de IAM para acceder DataSync a su ubicación de Amazon S3](#).

Pasos a seguir a continuación

Si aún no lo ha hecho, [inicie la tarea](#). De lo contrario, [supervise la actividad de la tarea](#).

Transferencia de archivos, objetos y carpetas específicos mediante filtros

AWS DataSync permite aplicar filtros para incluir o excluir datos de la ubicación de origen en una transferencia. Por ejemplo, si no quiere transferir archivos temporales con la extensión `.tmp`, puede crear un filtro de exclusión para impedir que estos archivos se transfieran a la ubicación de destino.

Puede utilizar una combinación de filtros de exclusión e inclusión en la misma tarea de transferencia. Si modifica los filtros de una tarea, esos cambios se aplicarán la próxima vez que ejecute la tarea.

Definiciones, sintaxis y términos relacionados con los filtros

Familiarícese con los conceptos relacionados con el DataSync filtrado:

Filtro

La cadena completa que constituye un filtro determinado (por ejemplo, `*.tmp | *.temp o /folderA|/folderB`).

Los filtros se componen de patrones que están delimitados por caracteres de barra vertical (`|`). No necesita un delimitador cuando agrega patrones en la DataSync consola porque agrega cada patrón por separado.

Note

Los filtros distinguen entre mayúsculas y minúsculas. Por ejemplo, el filtro `/folderA` no coincide con `/FolderA`.

Patrón

Un patrón de un filtro. Por ejemplo, `*.tmp` es un patrón que forma parte del filtro `*.tmp | *.temp`. Si el filtro tiene varios patrones, debe delimitar cada patrón mediante una barra vertical (`|`).

Carpetas

- Todos los filtros se expresan con relación a la ruta de la ubicación de origen. Por ejemplo, supongamos que especifica `/my_source/` como la ruta de origen cuando crea su ubicación de origen y tarea y que especifica el filtro de inclusión `/transfer_this/`. En este caso, DataSync transfiere solo el directorio `/my_source/transfer_this/` y su contenido.
- Para especificar una carpeta situada directamente en la ubicación de origen, incluya una barra inclinada (`/`) delante de del nombre de la carpeta. En el ejemplo anterior, el patrón utiliza `/transfer_this`, no `transfer_this`.
- DataSync interpreta los siguientes patrones de la misma manera y hace coincidir tanto la carpeta como su contenido.

`/dir`

`/dir/`

- Cuando transfiera datos desde o hacia un depósito de Amazon S3, DataSync trata el `/` carácter de la clave del objeto como el equivalente a una carpeta de un sistema de archivos.

Caracteres especiales

A continuación, se muestran los caracteres especiales que se utilizan en los filtros.

Carácter especial	Descripción
* (comodín)	Carácter que representa cero o más caracteres. Por ejemplo, <code>/movies_folder*</code> coincide con <code>/movies_folder</code> y con <code>/movies_folder1</code> .
(barra vertical)	Carácter que se utiliza como delimitador de patrones. Permite especificar varios patrones distintos que pueden coincidir con el filtro. Por ejemplo, <code>*.tmp *.temp</code> coincide con los archivos que tienen la extensión <code>tmp</code> o <code>temp</code> .

 **Note**
No es necesario utilizar este delimitador cuando se añaden patrones en la consola porque cada patrón se añade en su propia línea.

Carácter especial	Descripción
<code>\</code> (barra diagonal invertida)	Un carácter se utiliza como carácter de escape (*, , \) en un archivo o un objeto. Es necesario utilizar una barra diagonal invertida doble (\\) cuando un nombre de archivo contiene una barra diagonal invertida. Del mismo modo, \\\\ representa dos barras diagonales invertidas consecutivas en el nombre de un archivo. Es necesario utilizar una barra diagonal invertida seguida de una barra vertical (\\) cuando un nombre de archivo contiene una barra vertical. No se tiene en cuenta una (\\) seguida de cualquier otro carácter o situada al final de un patrón.

Ejemplos de filtros

En los siguientes ejemplos se muestran los filtros habituales con los que puede utilizar DataSync.

Note

Existen límites en cuanto al número de caracteres que puede utilizar en un filtro. Para obtener más información, consulte [DataSync cuotas](#).

Excluir algunas carpetas de la ubicación de origen

En algunos casos, es posible que tenga que excluir carpetas de la ubicación de origen para que no se copien en la de destino. Por ejemplo, si tienes work-in-progress carpetas temporales, puedes usar algo como el siguiente filtro:

```
*/*.temp
```

Para excluir carpetas con contenido similar (como `/reports2021` y `/reports2022`), puede usar un filtro de exclusión como el siguiente:

```
/reports*
```

Para excluir carpetas de cualquier nivel de la jerarquía de archivos, puede usar un filtro de exclusión similar al siguiente.

```
*/folder-to-exclude-1|*/folder-to-exclude-2
```

Para excluir carpetas en el nivel superior de la ubicación de origen, puede usar un filtro de exclusión similar al siguiente.

```
/top-level-folder-to-exclude-1|/top-level-folder-to-exclude-2
```

Inclusión de un subconjunto de las carpetas de la ubicación de origen

En algunos casos, la ubicación de origen podría ser un recurso compartido de archivos de gran tamaño y podría ser necesario transferir parte de las carpetas situadas bajo la carpeta raíz. Para incluir carpetas específicas, comience una ejecución de tarea con un filtro de inclusión similar al siguiente.

```
/folder-to-transfer/*
```

Excluir tipos de archivos específicos

Para excluir determinados tipos de archivos de la transferencia, puede crear una ejecución de tarea con un filtro de exclusión como por ejemplo *.temp.

Transferencia de determinados archivos que especifique

Para transferir una lista de archivos individuales, inicie una ejecución de tarea con un filtro de inclusión como el siguiente: “/folder/subfolder/file1.txt|/folder/subfolder/file2.txt|/folder/subfolder/file2.txt”

Creación de filtros de inclusión

Los filtros de inclusión definen los archivos, objetos y carpetas que DataSync desea transferir. Puede configurar estos filtros al crear, editar o comenzar una tarea.

DataSync escanea y transfiere solo los archivos y carpetas que coinciden con los filtros de inclusión. Por ejemplo, para incluir un subconjunto de las carpetas de origen, puede especificar /important_folder_1|important_folder_2.

Note

Los filtros de inclusión únicamente admiten el carácter (*) como último carácter de un patrón. Por ejemplo, se admite `/documents*/code*` pero no `*.txt`.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación de la izquierda, seleccione Tasks (Tareas) y, a continuación, seleccione Create task (Crear tarea).
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. Para Contenido a digitalizar, seleccione Archivos, objetos y carpetas específicos y, a continuación, seleccione Uso de filtros.
5. En Incluye, introduzca su filtro (por ejemplo, `/important_folders` para incluir un directorio importante) y, a continuación, seleccione Añadir patrón.
6. Agregue otros filtros de inclusión según sea necesario.

Usando el AWS CLI

Al usar el AWS CLI, debe usar comillas simples (') alrededor del filtro y un | (barra vertical) como delimitador si tiene más de un filtro.

En el siguiente ejemplo se especifican dos filtros de inclusión, `/important_folder1` y `/important_folder2`, cuándo se ejecuta el 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'
```

Creación de filtros de exclusión

Los filtros de exclusión definen los archivos, objetos y carpetas de la ubicación de origen que no desea DataSync transferir. Puede configurar estos filtros al crear, editar o empezar una tarea.

Temas

- [Datos excluidos de forma predeterminada](#)

Datos excluidos de forma predeterminada

DataSync excluye automáticamente algunos datos de la transferencia:

- `.snapshot`— DataSync ignora cualquier ruta que termine en `.snapshot`, lo que normalmente se utiliza para obtener point-in-time instantáneas de los archivos o directorios de un sistema de almacenamiento.
- `/.aws-datasync` / `/.awssync` — DataSync crea estas carpetas en su ubicación para facilitar la transferencia.
- `/.zfs`— Es posible que veas esta carpeta en Amazon FSx para ubicaciones de OpenZFS.

Uso de la consola DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación de la izquierda, seleccione Tasks (Tareas) y, a continuación, seleccione Create task (Crear tarea).
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. En Excluye, introduzca el filtro (por ejemplo, `*/temp` para excluir las carpetas temporales) y, a continuación, seleccione Añadir patrón.
5. Agregue otros filtros de exclusión según sea necesario.
6. Si es necesario, añada [filtros de inclusión](#).

Usando el AWS CLI

Al usar el AWS CLI, debe usar comillas simples (`'`) alrededor del filtro y un `|` (barra vertical) como delimitador si tiene más de un filtro.

En el siguiente ejemplo se especifican dos filtros de exclusión, `*/temp` y `*/tmp`, cuándo se ejecuta el 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'
```

Comprenda cómo DataSync gestiona los metadatos de archivos y objetos

AWS DataSync puede conservar los metadatos del archivo o del objeto durante una transferencia de datos. La forma en que se copian los metadatos depende de las ubicaciones de transferencia y de si esas ubicaciones utilizan tipos de metadatos similares.

Metadatos a nivel del sistema

En general, DataSync no copia los metadatos a nivel del sistema. Por ejemplo, al transferir desde un servidor de archivos SMB, los permisos que configuró a nivel del sistema de archivos no se copian en el sistema de almacenamiento de destino.

Hay algunas excepciones. Al realizar transferencias entre Amazon S3 y otro almacenamiento de objetos, copia DataSync algunos metadatos de [objetos definidos por el sistema](#).

Metadatos copiados en las transferencias de Amazon S3

En las siguientes tablas se describen los metadatos que se DataSync pueden copiar cuando una transferencia implica una ubicación de Amazon S3.

Temas

- [A Amazon S3](#)
- [Entre Amazon S3 y otro almacenamiento de objetos](#)
- [Entre Amazon S3 y HDFS](#)

A Amazon S3

Al copiar desde una de estas ubicaciones	A esta ubicación	DataSync puede copiar
• NFS • Amazon EFS • FSx para Lustre • FSx para OpenZFS	• Amazon S3	Lo siguiente como metadatos de usuario de Amazon S3:

Al copiar desde una de estas ubicaciones	A esta ubicación	DataSync puede copiar
FSx para ONTAP (mediante NFS)		- Marcas temporales de modificación de archivos y carpetas - Marcas horarias de acceso a archivos y carpetas (solo DataSync se puede hacer si se hace el mejor esfuerzo) - ID de usuario e ID de grupo - Permisos POSIX Los metadatos de archivo almacenados en metadatos del usuario de Amazon S3 son interoperables con los recursos compartidos en puertas de enlace de archivos utilizando AWS Storage Gateway. Una puerta de enlace de archivos permite el acceso de baja latencia desde las redes locales a los datos que ha copiado en Amazon S3. DataSync Estos metadatos también son interoperables con FSx Lustre. Al DataSync copiar los objetos que contienen estos metadatos a un servidor NFS, se restauran los metadatos del archivo. La restauración de los metadatos requiere conceder permisos elevados

Al copiar desde una de estas ubicaciones	A esta ubicación	DataSync puede copiar
		al servidor NFS. Para obtener más información, consulte Configuración de AWS DataSync transferencias con un servidor de archivos NFS .

Entre Amazon S3 y otro almacenamiento de objetos

Al copiar entre estas ubicaciones	DataSync puede copiar
- Almacenamiento de objetos - Amazon S3	- Metadatos de objetos definidos por el usuario - Etiquetas de objetos - Los siguientes metadatos de objetos definidos por el sistema: - Content-Disposition - Content-Encoding - Content-Language - Contenido-Tipo Nota: DataSync copia los metadatos del sistema de todos los objetos durante una transferencia inicial. Si configura su tarea para transferir solo los datos que hayan cambiado, DataSync no copiará los metadatos del sistema en transferencias posteriores a menos que el contenido del objeto o los metadatos del usuario también se hayan modificado. DataSync no copia los metadatos de otros objetos, como las listas de control de acceso a
- Microsoft Azure Blob Storage - Amazon S3	

Al copiar entre estas ubicaciones	DataSync puede copiar
	los objetos (ACLs), las versiones anteriores de los objetos o la clave de última modificación.

Entre Amazon S3 y HDFS

Al copiar entre estas ubicaciones	DataSync puede copiar
- Sistema de archivos distribuido de Hadoop (HDFS) - Amazon S3	Lo siguiente como metadatos de usuario de Amazon S3: - Marcas temporales de modificación de archivos y carpetas - Marcas de tiempo de acceso a archivos y carpetas (solo DataSync se puede hacer si se hace el mejor esfuerzo) - ID de usuario e ID de grupo - Permisos POSIX HDFS utiliza cadenas para almacenar la propiedad de los usuarios y grupos de archivos y carpetas, en lugar de identificadores numéricos, como y. UIDs GIDs

Los metadatos se copian en las transferencias NFS

En la siguiente tabla se describe qué metadatos DataSync se pueden copiar entre ubicaciones que utilizan el Sistema de archivos de red (NFS).

Al copiar entre estas ubicaciones	DataSync puede copiar
- NFS - Amazon EFS - Amazon FSx para Lustre	Marcas temporales de modificación de archivos y carpetas

Al copiar entre estas ubicaciones	DataSync puede copiar
• Amazon FSx para OpenZFS • Amazon FSx para NetApp ONTAP (mediante NFS)	• Marcas horarias de acceso a archivos y carpetas (solo DataSync se puede hacer si se hace el mejor esfuerzo) • ID de usuario (UID) e ID de grupo (GID) • Permisos POSIX

Metadatos copiados en transferencias SMB

En la siguiente tabla se describe qué metadatos DataSync se pueden copiar entre las ubicaciones que utilizan el bloque de mensajes del servidor (SMB).

Al copiar entre estas ubicaciones	DataSync puede copiar
• SMB • Servidor FSx de archivos Amazon para Windows • FSx para ONTAP (mediante SMB)	• Marcas temporales del archivo: hora de acceso, hora de modificación y hora de creación • Identificador de seguridad (SID) del propietario del archivo • Atributos de archivo estándar: solo lectura (R), archivo (A), sistema (S), oculto (H), comprimido (C), contenido no indexado (I), cifrado (E), temporal (T), desconectado (O) y disperso (P) DataSync intenta copiar los atributos archivados (A) comprimidos (C), no indexados por contexto (I), dispersos (P) y temporales (T) haciendo todo lo posible. Si estos atributos no se aplican en el destino, se ignoran durante la verificación de la tarea. • Listas de acceso discrecional de NTFS (DACLS), que determinan si se concede o no el acceso a un objeto.

Al copiar entre estas ubicaciones	DataSync puede copiar
	Listas de control de acceso al sistema NTFS (SACLs), que utilizan los administradores para registrar los intentos de acceso a un objeto protegido. Nota: no SACLs se copian si utiliza la versión 1.0 de SMB. Se copian DACLS y SACLs requieren la concesión de permisos específicos al usuario de Windows que DataSync utilice SMB para acceder a su ubicación. Para obtener más información, consulte Crear una ubicación para SMB, FSx Windows File Server o FSx ONTAP (según el tipo de ubicación de la transferencia).

Metadatos copiados en otros escenarios de transferencia

DataSync gestiona los metadatos de las siguientes maneras al copiarlos entre estos sistemas de almacenamiento (la mayoría de los cuales tienen estructuras de metadatos diferentes).

Al copiar desde una de estas ubicaciones	A una de estas ubicaciones	DataSync puede copiar
- SMB - FSx para Windows File Server - FSx para ONTAP (mediante SMB)	- Amazon EFS - FSx para Lustre - FSx para OpenZFS - FSx para ONTAP (mediante NFS) - Amazon S3 - Almacenamiento de objetos - Azure Blob Storage - NFS	Metadatos POSIX predeterminados para todos los archivos y carpetas del sistema de archivos de destino o los objetos del bucket S3 de destino. Este enfoque incluye el uso del ID de usuario de POSIX predeterminado y los valores de ID de grupo.

Al copiar desde una de estas ubicaciones	A una de estas ubicaciones	DataSync puede copiar
		Los metadatos basados en Windows (por ejemplo ACLs) no se conservan.
- Almacenamiento de objetos - Amazon S3 - Azure Blob Storage	- Amazon EFS - FSx para Lustre - FSx para OpenZFS - FSx para ONTAP (mediante NFS)	Metadatos POSIX predeterminados en los archivos y carpetas de destino. Este enfoque incluye el uso del ID de usuario de POSIX predeterminado y los valores de ID de grupo.
- Amazon EFS - FSx para Lustre - FSx para OpenZFS - FSx para ONTAP (mediante NFS)	Azure Blob Storage	Los siguientes metadatos definidos por el usuario: - Marcas temporales de modificación de archivos y carpetas - Marcas horarias de acceso a archivos y carpetas (solo DataSync se puede hacer si se hace el mejor esfuerzo) - ID de usuario e ID de grupo - Permisos POSIX

Al copiar desde una de estas ubicaciones	A una de estas ubicaciones	DataSync puede copiar
• HDFS	• Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP (mediante NFS)	• Marcas temporales de modificación de archivos y carpetas • Marcas horarias de acceso a archivos y carpetas (solo DataSync se puede hacer si se hace el mejor esfuerzo) • Permisos POSIX HDFS almacena la propiedad de los usuarios y grupos de archivos y carpetas como cadenas en lugar de identificadores numéricos (como y). UIDs GIDs Los valores predeterminados para el sistema UIDs de archivos de destino se GIDs aplican al sistema de archivos de destino. Para obtener más información, consulte Comprenda cuándo y cómo se DataSync aplican los metadatos POSIX predeterminados.

Al copiar desde una de estas ubicaciones	A una de estas ubicaciones	DataSync puede copiar
• Amazon S3 • Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para Windows File Server • FSx para ONTAP	• HDFS	Marcas de tiempo de archivos y carpetas desde la ubicación de origen. El propietario del archivo o la carpeta se establece en función del usuario de HDFS o de la entidad principal de Kerberos que se especificó al crear la ubicación de transferencia de HDFS. La configuración de mapeo de grupos del clúster de Hadoop determina el grupo.
• Amazon S3 • Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP (mediante NFS) • Almacenamiento de objetos • NFS • HDFS	• SMB • FSx para Windows File Server • FSx para ONTAP (mediante SMB)	Marcas de tiempo de archivos y carpetas desde la ubicación de origen. La propiedad se establece en función del usuario de Windows que se especificó DataSync para acceder al recurso compartido o de Amazon FSx o SMB. Los permisos se heredan del directorio principal.
• Azure Blob Storage	• FSx para Windows File Server • FSx para ONTAP (mediante SMB)	

Comprenda cuándo y cómo se DataSync aplican los metadatos POSIX predeterminados

DataSync aplica los metadatos POSIX predeterminados en las siguientes situaciones:

- Cuando las ubicaciones de origen y destino de la transferencia no tienen estructuras de metadatos similares
- Cuando faltan metadatos en la ubicación de origen

En la siguiente tabla se describe cómo DataSync se aplican los metadatos POSIX predeterminados durante estos tipos de transferencias:

Origen	Destino	Permisos de archivos	Permiso de carpetas	UID	GID
• Amazon S3¹ • Almacenamiento de objetos¹ • Microsoft Azure Blob Storage¹	• Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP (mediante NFS) • NFS	0755	0755	65534	65534
• SMB	• Amazon S3 • Almacenamiento de objetos • Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP (mediante NFS)	0644	0755	65534	65534

Origen	Destino	Permisos de archivos	Permiso de carpetas	UID	GID
	• NFS				
• HDFS	• Amazon EFS • FSx para Lustre • FSx para OpenZFS • FSx para ONTAP (mediante NFS) • NFS	0644	0755	65534	65534

¹ En los casos en que los objetos no tengan metadatos que hayan sido aplicados previamente por DataSync

Enlaces y directorios copiados por AWS DataSync

AWS DataSync gestiona los enlaces físicos, los enlaces simbólicos y los directorios de forma diferente en función de las ubicaciones de almacenamiento implicadas en la transferencia.

Enlaces duros

A continuación, te DataSync explicamos cómo gestiona los enlaces físicos en algunos escenarios de transferencia comunes:

- Al realizar transferencias entre un servidor de archivos NFS, FSx para Lustre, FSx para OpenZFS, FSx para ONTAP (mediante NFS) y Amazon EFS, se conservan los enlaces físicos.
- Al transferir a Amazon S3, cada archivo subyacente al que hace referencia un enlace duro se transfiere solo una vez. Durante las transferencias incrementales, se crean objetos separados en el bucket de S3. Si un enlace duro no ha cambiado en Amazon S3, se restaura correctamente cuando se transfiere a un servidor de archivos NFS, FSx para Lustre, para OpenZFS, FSx FSx para ONTAP (mediante NFS) o al sistema de archivos Amazon EFS.

- Al transferir a Microsoft Azure Blob Storage, cada archivo subyacente al que hace referencia un enlace duro se transfiere solo una vez. Durante las transferencias incrementales, se crean objetos independientes en el almacenamiento de blob si hay nuevas referencias en el origen. Al realizar la transferencia desde Azure Blob Storage, DataSync transfiere los enlaces físicos como si fueran archivos individuales.
- Al realizar transferencias entre un servidor de archivos SMB, FSx para Windows File Server y FSx ONTAP (mediante SMB), no se admiten los enlaces físicos. Si DataSync encuentra vínculos físicos en estas situaciones, la tarea de transferencia finaliza con un error. Para obtener más información, consulta tus CloudWatch registros.
- Al transferir a HDFS, no se admiten los enlaces físicos. CloudWatch los registros muestran estos enlaces como omitidos.

Enlaces simbólicos

Así es como DataSync maneja los enlaces simbólicos en algunos escenarios de transferencia comunes:

- Al realizar transferencias entre un servidor de archivos NFS, FSx para Lustre, para OpenZFS, FSx FSx para ONTAP (mediante NFS) y Amazon EFS, se conservan los enlaces simbólicos.
- Al transferir datos a Amazon S3, la ruta de destino del enlace se almacena en el objeto de Amazon S3. El enlace se restaura correctamente cuando se transfiere a un servidor de archivos NFS, FSx para el sistema de archivos Lustre, FSx OpenZFS, FSx ONTAP o Amazon EFS.
- Al realizar la transferencia a Azure Blob Storage, no se admiten enlaces simbólicos. CloudWatch los registros muestran estos enlaces como omitidos.
- Al realizar transferencias entre un servidor de archivos SMB, FSx para Windows File Server y FSx ONTAP (mediante SMB), no se admiten los enlaces simbólicos. DataSync no transfiere un enlace simbólico en sí mismo, sino un archivo al que hace referencia el enlace simbólico. Para reconocer los archivos duplicados y deduplicarlos con enlaces simbólicos, debe configurar la deduplicación en el sistema de archivos de destino.
- Al transferir a HDFS, no se admiten los enlaces simbólicos. CloudWatch los registros muestran estos enlaces como omitidos.

Directorios

En general, DataSync conserva los directorios cuando se transfieren entre sistemas de almacenamiento. Este no es el caso en las siguientes situaciones:

- Al transferir a Amazon S3, los directorios se representan como objetos vacíos que tienen prefijos y terminan con una barra inclinada (/).
- Al transferir en Azure Blob Storage sin un espacio de nombres jerárquico, los directorios no existen. Lo que parece un directorio es solo una parte del nombre de un objeto.

Configuración de la forma en que gestionan los archivos, los objetos y los metadatos

Puede configurar la forma en que AWS DataSync gestiona sus archivos, objetos y sus metadatos asociados al transferirlos de una ubicación a otra.

Por ejemplo, en el caso de las transferencias periódicas, es posible que desee sobrescribir los archivos del destino que hayan cambiado en la ubicación de origen a fin de mantener la sincronización entre las ubicaciones. Puede copiar propiedades como los permisos POSIX para archivos y carpetas, las etiquetas asociadas a los objetos y las listas de control de acceso (ACLs).

Opciones del modo de transferencia

Puede configurar si DataSync transfiere solo los datos (incluidos los metadatos) que se modifican tras una copia inicial o todos los datos cada vez que ejecute la tarea. Si planeas realizar transferencias recurrentes, es posible que solo desees transferir lo que haya cambiado desde la ejecución anterior de la tarea.

Opción en la consola	Opción en la API	Descripción
Transfiera solo los datos que hayan cambiado	TransferMode es CHANGED.	Tras la transferencia completa inicial, DataSync copia solo los datos y metadatos que difieran entre la ubicación de origen y la de destino.
Transfiere todos los datos	TransferMode es ALL.	DataSync copia todo el contenido de la fuente al destino sin comparar las diferencias entre las ubicaciones.

Opciones de manejo de archivos y objetos

Puede controlar algunos aspectos del DataSync tratamiento de los archivos u objetos en la ubicación de destino. Por ejemplo, DataSync puede eliminar archivos del destino que no estén en el origen.

Opción en la consola	Opción en la API	Descripción
Conservar los archivos borrados	PreserveDeletedFiles	Especifica si DataSync mantiene los archivos u objetos en la ubicación de destino que no existen en el origen. Si configura su tarea para eliminar objetos de su bucket de Amazon S3, es posible que se le apliquen cargos por duración mínima de almacenamiento para determinadas clases de almacenamiento. Para obtener información detallada, consulta Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3.  Warning No puede configurar su tarea para que elimine los datos del destino y, además, transfiera todos los datos. Cuando transfieres todos los datos, DataSync no escanea tu ubicación

Opción en la consola	Opción en la API	Descripción
		de destino y no sabe qué eliminar.
Sobrescribe los archivos	OverwriteMode	Especifica si DataSync modifica los datos en la ubicación de destino cuando los datos de origen o los metadatos han cambiado. Si no configura la tarea para sobrescribir los datos, los datos de destino no se sobrescribirán aunque los datos de origen sean diferentes. Si la tarea sobrescribe objetos, es posible que se apliquen cargos adicionales para determinadas clases de almacenamiento (por ejemplo, por la recuperación o por la eliminación anticipada). Para obtener información detallada, consulta Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3.

Opciones de gestión de metadatos

DataSync puede conservar los metadatos de archivos y objetos durante una transferencia. Los metadatos que DataSync se pueden conservar dependen de los sistemas de almacenamiento involucrados y de si esos sistemas utilizan una estructura de metadatos similar.

Antes de configurar la tarea, asegúrese de entender cómo se gestionan [los DataSync metadatos y los archivos especiales](#) cuando se transfieren entre las ubicaciones de origen y destino.

Important

DataSync admite las transferencias desde y hacia determinados sistemas de almacenamiento en la nube de terceros, como Google Cloud Storage e IBM Cloud Object Storage, que gestionan los metadatos del sistema de una forma que no es totalmente compatible con S3. Para estas transferencias, DataSync intenta copiar atributos de metadatos como `ContentType`, `ContentEncoding`, `ContentLanguage`, y haciendo `CacheControl` el mejor esfuerzo posible. Si el sistema de almacenamiento de destino no aplica estos atributos, se ignorarán durante la verificación de la tarea.

Opción en la consola	Opción en la API	Descripción
Propiedad de la copia	Gid y Uid	Especifica si DataSync copia la propiedad de los archivos y carpetas POSIX, como el ID de grupo de los propietarios del archivo y el ID de usuario del propietario del archivo.
Copiar permisos	PosixPermissions	Especifica si DataSync copia los permisos POSIX de los archivos y carpetas del origen al destino.
Copiar las marcas de tiempo	Atime y Mtime	Especifica si DataSync copia los metadatos de la marca de tiempo del origen al destino.
Copiar las etiquetas del objeto	ObjectTags	Especifica si DataSync conserva las etiquetas asociadas a los objetos al transferirlos entre sistemas de almacenamiento de objetos.

Opción en la consola	Opción en la API	Descripción
Propiedad de la copia DACLs, y SACLs	SecurityDescriptorCopyFlags es OWNER_DACL_SACL .	DataSync copia lo siguiente: • El propietario del objeto. • listas de acceso discrecional de NTFS (DACLs), que determinan si se debe conceder el acceso a un objeto. • Listas de control de acceso al sistema NTFS (SACLs), que utilizan los administradores para registrar los intentos de acceso a un objeto protegido. Nota: no SACLs se copian si utiliza la versión 1.0 de SMB. Se copian DACLs y SACLs requieren la concesión de permisos específicos al usuario de Windows que DataSync utilice SMB para acceder a su ubicación. Para obtener más información, consulte Crear una ubicación para SMB, FSx Windows File Server o FSx ONTAP (según el tipo de ubicación de la transferencia).

Opción en la consola	Opción en la API	Descripción
Copie la propiedad y DACLs	SecurityDescriptorCopyFlags es OWNER_DACL .	DataSync copia lo siguiente: • El propietario del objeto. • DACLs, que determinan si se debe conceder el acceso a un objeto. DataSync no se copiará SACLs al seleccionar esta opción.
No copies la propiedad o ACLs	SecurityDescriptorCopyFlags es NONE.	DataSync no copia ningún dato de propiedad o permiso. Los objetos que DataSync escriben en la ubicación de destino son propiedad del usuario cuyas credenciales se proporcionan DataSync para acceder al destino. Los permisos de los objetos de destino se determinan en función de los permisos configurados en el servidor de destino.

Configurar las opciones de gestión de archivos, objetos y metadatos

Puede configurar el modo en DataSync que se gestionan los archivos, objetos y metadatos al crear, editar o iniciar la tarea de transferencia.

Mediante la consola de DataSync

Las siguientes instrucciones describen cómo configurar las opciones de gestión de archivos, objetos y metadatos al crear una tarea.

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.

2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. En Modo transferencia, elija una de las siguientes opciones:

- Transfiera solo los datos que hayan cambiado
- Transfiere todos los datos

Para obtener más información sobre estas opciones, consulte [Opciones del modo de transferencia](#).

5. Seleccione Conservar los archivos eliminados si DataSync desea mantener los archivos u objetos en la ubicación de destino que no existen en el origen.

Si no selecciona esta opción y la tarea elimina objetos del bucket de Amazon S3, es posible que se apliquen cargos mínimos por la duración de almacenamiento para determinadas clases de almacenamiento. Para obtener información detallada, consulta [Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3](#).

 Warning

No puede desactivar esta opción y activar la opción Transferir todos los datos. Al transferir todos los datos, DataSync no escanea la ubicación de destino y no sabe qué eliminar.

6. Seleccione Sobrescribir archivos si DataSync desea modificar los datos en la ubicación de destino cuando cambien los datos de origen o los metadatos.

Si la tarea sobrescribe objetos, es posible que se apliquen cargos adicionales para determinadas clases de almacenamiento (por ejemplo, por la recuperación o por la eliminación anticipada). Para obtener información detallada, consulta [Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3](#).

Si no elige esta opción, los datos de destino no se sobrescribirán aunque los datos de origen sean diferentes.

7. En Opciones de transferencia, selecciona cómo quieres DataSync gestionar los metadatos. Para obtener más información sobre las opciones, consulte [Opciones de gestión de metadatos](#).

 Important

Las opciones que aparecen en la consola dependen de las ubicaciones de origen y destino de la tarea. Puede que tengas que expandir la configuración adicional para ver algunas de estas opciones.

- Propiedad de la copia
- Copiar permisos
- Copiar las marcas de tiempo
- Copiar las etiquetas del objeto
- Propiedad de la copia DACLs, y SACLs
- Propiedad de la copia y DACLs
- No copie la propiedad o ACLs

Uso de la DataSync API

Puede configurar las opciones de gestión de archivos, objetos y metadatos mediante el uso del `Options` parámetro con cualquiera de las siguientes operaciones:

- [CreateTask](#)
- [StartTaskExecution](#)
- [UpdateTask](#)

Configurar cómo se AWS DataSync verifica la integridad de los datos

Durante una transferencia, AWS DataSync utiliza la verificación por suma de comprobación para comprobar la integridad de los datos que copias de una ubicación a otra. También puedes configurarlo DataSync para que realice una verificación adicional al final de la transferencia.

Opciones de verificación de datos

Utilice la siguiente información como ayuda para decidir si desea DataSync realizar estas comprobaciones adicionales y de qué manera.

Opción de la consola	Opción de la API	Descripción
Compruebe únicamente los datos transferidos (recomendado)	VerifyMode es ONLY_FILE_S_TRANSFERRED .	DataSync calcula la suma de verificación de los datos transferidos (incluidos los metadatos) en la ubicación de origen. Al final de la transferencia, DataSync compara esta suma de verificación con la suma de verificación calculada con los mismos datos en el destino. Es conveniente utilizar esta opción cuando la transferencia se realice a S3 Glacier Flexible Retrieval o a las clases de almacenamiento de S3 Glacier Deep Archive. Para obtener más información, consulte Consideraciones sobre las clases de almacenamiento con las transferencias de Amazon S3.
Verifica todos los datos	VerifyMode es POINT_IN_TIME_CONSISTENT .	Al final de la transferencia, DataSync comprueba todo el origen y el destino para comprobar que ambas ubicaciones estén completamente sincronizadas.

Opción de la consola	Opción de la API	Descripción
		 Note No se admite cuando la tarea utiliza el modo mejorado.

Configuración de la verificación de datos

Puede configurar las opciones de verificación de datos al crear una tarea, actualizarla o iniciar la ejecución de una tarea.

Mediante la consola de DataSync

Las siguientes instrucciones describen cómo configurar las opciones de verificación de datos al crear una tarea.

Cómo configurar la verificación de los datos usando la consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. Para verificar, elija una de las siguientes opciones:
 - Compruebe únicamente los datos transferidos (recomendado)
 - Verifica todos los datos
 - No verifique los datos después de la transferencia

Mediante la API de DataSync

Puede configurar la forma en DataSync que se verifican los datos mediante el `VerifyMode` parámetro con cualquiera de las siguientes operaciones:

- [CreateTask](#)
- [UpdateTask](#)
- [StartTaskExecution](#)

Configuración de los límites de ancho de banda para la tarea de AWS DataSync

Puede configurar los límites de ancho de banda de la red para su AWS DataSync tarea y para cada una de sus ejecuciones.

 Note

No se aplica a las [tareas del modo mejorado](#).

Limitación del ancho de banda para una tarea

Configure un límite de ancho de banda al crear, editar o iniciar una tarea.

Mediante la consola de DataSync

Las siguientes instrucciones describen cómo configurar un límite de ancho de banda para la tarea en el momento de crearla.

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. En Límite de ancho de banda, elija una de las siguientes opciones:
 - Seleccione Usar disponibles para usar todo el ancho de banda de la red disponible para cada una de las ejecuciones de la tarea.
 - Seleccione Establecer límite de ancho de banda (MiB/s) e introduzca el ancho de banda máximo que desee utilizar DataSync para la ejecución de cada tarea.

Uso de la API DataSync

Puede configurar el límite del ancho de banda de una tarea mediante el parámetro `BytesPerSecond` con cualquiera de las siguientes operaciones:

- [CreateTask](#)
- [UpdateTask](#)
- [StartTaskExecution](#)

Limitación del ancho de banda para la ejecución de una tarea

Puede modificar el límite del ancho de banda para la ejecución de una tarea en estado de ejecución o en cola.

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación, expanda Transferencia de datos y, a continuación, seleccione Tareas.
3. Elija la tarea y, a continuación, seleccione Historial para ver las ejecuciones de la tarea.
4. Elija la ejecución de la tarea que desee modificar y, a continuación, seleccione Editar.
5. En el cuadro de diálogo, elija una de las siguientes acciones:
 - Seleccione Usar disponibles para usar todo el ancho de banda de la red disponible para cada una de las ejecuciones de la tarea.
 - Seleccione Establecer límite de ancho de banda (MiB/s) e introduzca el ancho de banda máximo que desee utilizar DataSync para la ejecución de la tarea.
6. Seleccione Save changes (Guardar cambios).

El nuevo límite de ancho de banda entrará en vigor en 60 segundos.

Mediante la API de DataSync

Puede modificar el límite de ancho de banda para la ejecución de una tarea en ejecución o en cola utilizando el BytesPerSecond parámetro que acompaña a la operación. [UpdateTaskExecution](#)

Programar cuándo se ejecuta AWS DataSync la tarea

Puede configurar un programa de AWS DataSync tareas para transferir datos periódicamente entre ubicaciones de almacenamiento.

Cómo funciona DataSync la programación de tareas

Una DataSync tarea programada se ejecuta con la frecuencia que especifique, con un intervalo mínimo de 1 hora. Puede crear un programación de tareas mediante expresiones Cron o Rate.

 Important

No puede programar una tarea para que se ejecute en un intervalo superior a 1 hora.

Uso de expresiones Cron

Use expresiones Cron para las programaciones de tareas que se ejecuten a una hora y un día específicos. Por ejemplo, aquí le explicamos cómo configurar una programación de tareas en el AWS CLI que se ejecute a las 12:00 UTC cada miércoles y domingo.

```
cron(0 12 ? * SUN,WED *)
```

Uso de expresiones Rate

Utilice expresiones Rate para los programas de tareas que se ejecuten a intervalos regulares, por ejemplo cada 12 horas. Por ejemplo, así es como puede configurar un programa de tareas en el AWS CLI que se ejecute cada 12 horas:

```
rate(12 hours)
```

 Tip

Para obtener más información sobre la sintaxis de las expresiones cron y rate, consulta la [Guía del EventBridge usuario de Amazon](#).

Creación de un cronograma de DataSync tareas

Puedes programar la frecuencia con la que se ejecuta tu tarea mediante la DataSync consola o la DataSync API. AWS CLI

Uso de la DataSync consola

Las siguientes instrucciones describen cómo configurar una programación al crear una tarea. Puede modificar la programación más adelante al editar la tarea.

En la consola, algunas opciones de programación permiten especificar la hora exacta a la que se ejecutará la tarea (por ejemplo, todos los días a las 22:30). Si no incluye una hora en estas opciones, la tarea se ejecutará en el momento en que la cree (o actualice).

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. En Frecuencia de la programación, elija una de las siguientes opciones:
 - Elija Not Scheduled (No programada) si no desea que la tarea se ejecute siguiendo una programación.
 - Elija Hourly (Cada hora) y, a continuación, elija el minuto de la hora en que quiere que se ejecute la tarea.
 - Elija Daily (A diario) e introduzca la hora UTC a la que desea que se ejecute la tarea.
 - Elija Weekly (Cada semana) y el día de la semana e introduzca la hora UTC a la que desea que se ejecute la tarea.
 - Elija Days of the week (Días de la semana), seleccione el día o los días concretos e introduzca la hora UTC a la que debe ejecutarse la tarea, con el formato HH:MM.
 - Elija Custom (Personalizado) y, a continuación, seleccione Expresión Cron o expresión Rate. Introduzca su programa de tareas con un intervalo mínimo de 1 hora.

Usando el AWS CLI

Puede crear una programación para la DataSync tarea mediante el `--schedule` parámetro con el `start-task-execution` comando `create-taskupdate-task`, o.

Las siguientes instrucciones describen cómo hacer esto con el comando `create-task`.

1. Copie el siguiente 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. Para el parámetro `--source-location-arn`, especifique el nombre de recurso de Amazon (ARN) de la ubicación desde la que transfiere los datos.
3. Para el parámetro `--destination-location-arn`, especifique el ARN de la ubicación a la que transfiere los datos.
4. Para el parámetro `--schedule`, especifique una expresión Cron o Rate para su programación.

En el ejemplo, la expresión Cron *`cron(0 12 ? * SUN,WED *)`* establece una programación de la tarea que se ejecuta a las 12:00 UTC cada miércoles y domingo.

5. Ejecute el comando `create-task` para crear la tarea con una programación.

Pausar un programa de DataSync tareas

Puede haber situaciones en las que necesite pausar la programación de DataSync tareas. Por ejemplo, es posible que tenga que detener temporalmente una transferencia periódica para solucionar un problema con la tarea o realizar tareas de mantenimiento en el sistema de almacenamiento.

DataSync podría deshabilitar la programación de tareas automáticamente por los siguientes motivos:

- La tarea falla repetidamente con el mismo error.
- [Deshabilite un Región de AWS](#) que esté utilizando su tarea.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Tareas.
3. Elija la tarea para la que desee pausar la programación y, a continuación, elija Editar.
4. En Programar, desactive Activar programación. Elija Guardar cambios.

Usando el AWS CLI

1. Copie el siguiente 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. Para el parámetro `--task-arn`, especifique el ARN de la tarea para la que desea pausar la programación.
3. Para el parámetro `--schedule`, haga lo siguiente:
 - Para `ScheduleExpression`, especifique una expresión Cron o Rate para su programación.

En el ejemplo, la expresión `cron(0 12 ? * SUN,WED *)` establece una programación de la tarea que se ejecuta a las 12:00 UTC cada miércoles y domingo.
 - Para `Status`, especifique `DISABLED` para pausar la programación de la tarea.
4. Ejecute el comando `update-task`.
5. Para reanudar la programación, ejecute el mismo comando `update-task` con el valor `Status` establecido en `ENABLED`.

Comprobar el estado de un programa de DataSync tareas

Puede ver si su programación de DataSync tareas está habilitada.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Tareas.
3. En la columna Programación, compruebe si la programación de la tarea está habilitada o deshabilitada.

Usando el AWS CLI

1. Copie el siguiente comando `describe-task`:

```
aws datasync describe-task \  

```

```
--task-arn arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh
```

2. Para el parámetro `--task-arn`, especifique el ARN de la tarea sobre la que desea obtener información.
3. Ejecute el comando `describe-task`.

Recibirá una respuesta que proporciona detalles sobre su tarea, incluida su programación. (El siguiente ejemplo se centra principalmente en la configuración de la programación de la tarea y no muestra una respuesta de `describe-task` completa).

El ejemplo muestra que la programación de la tarea se ha deshabilitado manualmente. Si la programación está deshabilitada por el DataSync SERVICE, verá un mensaje de error que le ayudará `DisabledReason` a entender por qué la tarea sigue fallando. Para obtener más información, 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."
  },
  ...
}
```

Etiquetar tus tareas AWS DataSync

Las etiquetas son pares clave-valor que te ayudan a administrar, filtrar y buscar tus AWS DataSync recursos. Puedes añadir hasta 50 etiquetas a cada DataSync tarea y ejecución de tareas.

Por ejemplo, puede crear una tarea para realizar una migración de datos de gran tamaño y etiquetarla con la clave **Project** y el valor **Large Migration**. Para una mejor organización de la migración, puede etiquetar una ejecución de la tarea con la clave **Transfer Date** y el valor **May 2021** (es posible que se etiqueten las siguientes ejecuciones de las tareas **June 2021**, **July 2021**, etc.).

Etiquetar tu tarea DataSync

Solo puede etiquetar la DataSync tarea al crearla.

Mediante la consola de DataSync

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. En la página Configurar ajustes, seleccione Añadir etiqueta nueva para etiquetar la tarea.

Usando el AWS CLI

1. Copie el siguiente 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 los siguientes parámetros en el comando:
 - `--source-location-arn`: especifique el nombre de recurso de Amazon (ARN) de la ubicación de origen en la transferencia.
 - `--destination-location-arn`: especifique el ARN de la ubicación de destino en la transferencia.
 - `--tags`: especifique las etiquetas que desea aplicar a la tarea.

Si hay más de una etiqueta, separe cada par clave-valor con un espacio.

3. (Opcional) Especifique otros parámetros que tengan sentido para su escenario de transferencia.

Para obtener una lista de `--options`, consulte el comando [create-task](#).

4. Ejecute el comando `create-task`.

Recibirá una respuesta que le mostrará la tarea que acaba de crear.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:123456789012:task/task-
abcdef01234567890"
}
```

Para ver las etiquetas que ha añadido a esta tarea, puede utilizar el [list-tags-for-resource](#) comando.

Etiquetar la ejecución de la DataSync tarea

Puede etiquetar cada ejecución de la DataSync tarea.

Si la tarea ya tiene etiquetas, recuerde lo siguiente sobre el uso de etiquetas en la ejecución de tareas:

- Si inicia la tarea con la consola, las etiquetas creadas por el usuario se aplicarán de forma automática a la ejecución de la tarea. Sin embargo, no se aplicarán las etiquetas creadas por el sistema que comiencen por `aws` :.
- Si empiezas la tarea con la DataSync API o AWS CLI, sus etiquetas no se aplican automáticamente a la ejecución de la tarea.

Mediante la consola de DataSync

Para añadir, editar o eliminar etiquetas de la ejecución de una tarea, debe iniciar la tarea con las opciones de anulación.

1. Abre la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Tareas.
3. Elija la tarea.
4. Seleccione Iniciar y, a continuación, elija una de las siguientes opciones:
 - Iniciar con los valores predeterminados: aplica cualquier etiqueta asociada a la tarea.
 - Comenzar con las opciones principales: permite añadir, editar o eliminar etiquetas para la ejecución de esta tarea en particular.

Usando el AWS CLI

1. Copie el siguiente 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 los siguientes parámetros en el comando:

- `--task-arn`: especifique el ARN de la tarea que desea iniciar.
- `--tags`: especifique las etiquetas que desea aplicar a esta ejecución específica de la tarea.

Si hay más de una etiqueta, separe cada par clave-valor con un espacio.

3. (Opcional) Especifique otros parámetros que tengan sentido para su situación.

Para obtener más información, consulte el comando [start-task-execution](#).

4. Ejecute el comando `start-task-execution`.

Recibirá una respuesta que muestra la ejecución de la tarea que usted acaba de iniciar.

```
{  
  "TaskExecutionArn": "arn:aws:datasync:us-east-2:123456789012:task/task-  
  abcdef01234567890"  
}
```

Para ver las etiquetas que ha añadido a esta tarea, puede utilizar el [list-tags-for-resource](#) comando.

Iniciar una tarea para transferir los datos

Una vez creada la tarea de AWS DataSync transferencia, puede empezar a mover los datos. Cada ejecución de una tarea se denomina ejecución de tarea. Para obtener información sobre lo que ocurre durante la ejecución de una tarea, consulte [Cómo DataSync transfiere los archivos, objetos y directorios](#).

Important

Si planea transferir datos a o desde una ubicación de Amazon S3, consulte [cómo DataSync pueden afectar los cargos por solicitud de S3](#) y la [página de DataSync precios](#) antes de empezar.

Inicio de la tarea

Una vez que haya creado la tarea, podrá empezar a mover los datos de inmediato.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Tareas.
3. Elija la tarea que desee ejecutar.

Asegúrese de que la tarea esté en el estado Disponible. También puede seleccionar múltiples tareas.

4. Seleccione Acciones y, a continuación, elija una de las siguientes opciones:
 - Iniciar: ejecuta la tarea (o las tareas, si ha seleccionado más de una).
 - Comenzar con las opciones principales: le permite modificar algunos de los ajustes de la tarea antes de empezar a mover los datos. Cuando esté preparado, elija Iniciar.
5. Seleccione Ver detalles de la ejecución para ver los detalles de la ejecución de la tarea en ejecución.

Usando el AWS CLI

Para iniciar la DataSync tarea, solo tiene que especificar el nombre de recurso de Amazon (ARN) de la tarea que desea ejecutar. A continuación, se muestra un ejemplo de comando `start-task-execution`:

```
aws datasync start-task-execution \  
  --task-arn 'arn:aws:datasync:region:account-id:task/task-id'
```


En el siguiente ejemplo, se inicia una tarea con algunos ajustes distintos de los valores predeterminados de la tarea:

```
aws datasync start-task-execution \  
  --override-options VerifyMode=NONE,OverwriteMode=NEVER,PosixPermissions=NONE
```

El comando devuelve un ARN para la ejecución de la tarea, similar al del siguiente ejemplo:

```
{  
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:209870788375:task/  
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"  
}
```

Note

Cada agente puede ejecutar una sola tarea a la vez.

Uso de la API DataSync

Puede iniciar la tarea mediante la [StartTaskExecution](#) operación. Utilice la [DescribeTaskExecution](#) operación para obtener detalles sobre la ejecución de la tarea en ejecución.

Una vez iniciada, puede [comprobar el estado de la ejecución de la tarea](#) mientras DataSync copia sus datos. También puede [limitar el ancho de banda de la ejecución de la tarea](#), en caso de ser necesario.

Estados de ejecución de las tareas

Al iniciar una DataSync tarea, es posible que veas estos estados. (Los [estados de las tareas son diferentes a los estados](#) de ejecución de las tareas).

Estado de la consola	Estado de la API	Descripción
En cola	QUEUED	La ejecución de otra tarea se está ejecutando y utilizando el mismo DataSync agente. Para obtener más información, consulte Saber cuándo la tarea está en cola .

Estado de la consola	Estado de la API	Descripción
Launching (inicio o lanzamiento)	LAUNCHING	DataSync está inicializando la ejecución de la tarea. Este estado por lo general se realiza rápidamente, pero puede tardar hasta varios minutos.
Preparación	PREPARING	DataSync está determinando qué datos se van a transferir. La preparación puede tardar solo unos minutos, unas horas o incluso más, en función del número de archivos, objetos o directorios que haya en ambas ubicaciones y de la forma en que configure la tarea. El funcionamiento de la preparación también depende del modo de la tarea. Para obtener más información, consulte ¿Cómo DataSync se prepara la transferencia de datos.
Transferencia	TRANSFERRING	DataSync está realizando la transferencia de datos real.
Verificando	VERIFYING	DataSync está verificando la integridad de sus datos al final de la transferencia.
Success	SUCCESS	La ejecución de la tarea se realizó correctamente.
Cancelling	CANCELLING	La ejecución de la tarea está en proceso de ser cancelada.
Error	ERROR	Falló la ejecución de la tarea.

Saber cuándo la tarea está en cola

Al ejecutar varias tareas (por ejemplo, si está [transfiriendo un conjunto de datos grande](#)), DataSync puede poner las tareas en cola para que se ejecuten en serie (primero en entrar, primero en salir). Algunos ejemplos de casos en los que esto ocurre son:

- Ejecutas diferentes tareas que utilizan el mismo DataSync agente. Si bien puede usar el mismo agente para varias tareas, un agente solo puede ejecutar una tarea a la vez.
- La ejecución de una tarea está en curso y se inician ejecuciones adicionales de la misma tarea utilizando distintos [filtros](#) o [manifiestos](#).

En cada ejemplo, las tareas en cola no se inician hasta que finaliza la tarea que tienen por delante.

Cancelación de la ejecución de la tarea

Puede detener cualquier ejecución de DataSync tareas en ejecución o en cola.

Cómo cancelar una ejecución de tarea a través de la consola

1. Abra la AWS DataSync consola en. <https://console.aws.amazon.com/datasync/>
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Tareas.
3. Seleccione el ID de la tarea para la tarea en ejecución que desea supervisar.

El estado de la tarea debe ser En ejecución.

4. Seleccione Historial para ver las ejecuciones de la tarea.
5. Seleccione la ejecución de la tarea que desee detener y, a continuación, elija Detener.
6. En el cuadro de diálogo, elija Detener.

Para cancelar una tarea en ejecución o en cola mediante la DataSync API, consulte [CancelTaskExecution](#).

Supervisión de sus AWS DataSync transferencias

La supervisión es importante para mantener la fiabilidad y el rendimiento de tus actividades de AWS DataSync transferencia. Recomendamos que recopile los datos de monitoreo para que le resulte más sencillo eliminar los errores que se produzcan. Sin embargo DataSync, antes de comenzar a monitorear, cree un plan de monitoreo que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de supervisión va a utilizar?
- ¿Quién se encargará de realizar las tareas de supervisión?
- ¿Quién debería recibir una notificación cuando surjan problemas?

AWS proporciona varios servicios y herramientas para la supervisión DataSync. Puede configurar algunas de estas para que realicen la labor de monitoreo automáticamente para usted; sin embargo, otras requieren intervención manual. Le recomendamos que automatice las tareas de supervisión en la medida de lo posible.

Temas

- [Descripción de los contadores de rendimiento de transferencia de datos](#)
- [Supervisión de las transferencias de datos con CloudWatch las métricas de Amazon](#)
- [Supervise sus transferencias de datos con informes de tareas](#)
- [Supervisión de las transferencias de datos con Amazon CloudWatch Logs](#)
- [Registrar llamadas a la AWS DataSync API con AWS CloudTrail](#)
- [Supervisión de eventos mediante Amazon EventBridge](#)
- [Supervisión AWS DataSync con herramientas manuales](#)

Descripción de los contadores de rendimiento de transferencia de datos

Al [iniciar una tarea](#), AWS DataSync proporciona contadores para ayudar a realizar un seguimiento del rendimiento y el progreso de la transferencia de datos.

Utilice la siguiente información para comprender qué representa cada contador. Puede ver estos contadores en la DataSync consola o en una [DescribeTaskExecution](#) respuesta. Algunos contadores no están disponibles en todos los [modos de tarea](#).

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
–	BytesWritten	Mejorado, básico	El número de bytes lógicos que DataSync realmente se escriben en la ubicación de destino.
Rendimiento de datos	–	Mejorado, básico	La velocidad a la que se DataSync escriben los bytes lógicos en la ubicación de destino. Si lo utilizas DescribeTaskExecution, la forma de calcular este contador depende del modo de tarea: • Modo mejorado: divide entre BytesWritten TotalDuration • Modo básico: dividir BytesWritten por TransferDuration
Datos transferidos	BytesTransferred	Mejorado, básico	El número de bytes que se DataSync envían a la red antes de la compresión

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
			(si la compresión es posible). Para conocer el número de bytes transferidos a través de la red, consulte el contador de rendimiento de la red (en la consola) o BytesCompressed (in DescribeTaskExecution).
Eliminado del destino	FilesDeleted	Mejorado, básico	El número de archivos, objetos y directorios que DataSync realmente se eliminan en la ubicación de destino. Si no configuras la tarea para eliminar datos del destino que no estén en la fuente: • Si se eliminan del destino, no se muestra en la consola. • FilesDeleted siempre muestra un valor de 0.

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
–	EstimatedBytesToTransfer	Mejorado, básico	El número de bytes lógicos que se DataSync espera escribir en la ubicación de destino.
–	EstimatedFilesToDelete	Mejorado, básico	El número de archivos, objetos y directorios que se DataSync espera eliminar en la ubicación de destino. Si no configura la tarea para eliminar datos del destino que no estén en el origen, el valor siempre será 0.

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
–	EstimatedFilesToTransfer	Mejorado, básico	La cantidad de archivos, objetos y directorios que se DataSync espera transferir a través de la red. Este valor se calcula mientras DataSync se prepara la transferencia. La forma en que se calcula depende principalmente del modo de transferencia que utilices: • Si el modo de transferencia está configurado para transferir solo los datos que hayan cambiado: el cálculo se basa en comparar el contenido de las ubicaciones de origen y destino y determinar la diferencia que se debe transferir. La diferencia puede incluir: • Todo lo que se añada o

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
			modifique en la ubicación de origen. • Todo lo que se encuentre en ambas ubicaciones y que se modifique en el destino después de una transferencia inicial (a menos que configure la tarea para no sobrescribir los datos en el destino). • (Solo en el modo básico) El número de elementos que DataSync se van a eliminar (si configura la tarea para eliminar los datos del destino). • Si el modo de transferencia está configurado para transferir todos los datos: el cálculo se basa únicamente en los elementos

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
			que DataSync se encuentran en la ubicación de origen.
Rendimiento de archivos	–	Mejorado, básico	La velocidad a la que se DataSync transfieren en archivos, objetos y directorios a través de la red. Si lo estás usando DescribeTaskExecution, la forma de calcular este contador depende del modo de tarea que utilices: • Modo mejorado: divide entre <code>FilesTransferred</code> <code>TotalDuration</code> • Modo básico: dividir <code>FilesTransferred</code> por <code>TransferDuration</code>

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
–	FilesFailed	Mejorado	El número de objetos que DataSync no se pueden preparar, transferir, verificar ni eliminar durante la ejecución de la tarea. Si hay errores, puede verlos junto a los contadores de la consola de destino preparados, transferidos, omitidos y eliminados, respectivamente.

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
Listado en la fuente	FilesListed.AtSource	Mejorado	El número de objetos que DataSync se encuentran en la ubicación de origen. • En el caso de un manifiesto, solo se DataSync muestra lo que hay en el manifiesto (y no todo lo que se encuentra en la ubicación de origen). • Con un filtro de inclusión, solo DataSync muestra lo que coincide con el filtro de tu ubicación de origen. • Con un filtro de exclusión, DataSync muestra todo lo que hay en la ubicación de origen antes de aplicar el filtro.

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
–	FilesListed.AtDestinationForDelete	Mejorado	El número de objetos que DataSync se encuentran en la ubicación de destino. Este contador solo se aplica si configura la tarea para eliminar datos del destino que no estén en la fuente.

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
Rendimiento de la red*	BytesCompressed	Mejorado, básico	El número de bytes físicos que se DataSync transfiere a través de la red después de la compresión (si la compresión es posible). Este número suele ser inferior al de los datos transferidos (en la consola) o BytesTransferred (en DescribeTaskExecution), a menos que los datos no se puedan comprimir. * — En el modo mejorado, el rendimiento de la red no se muestra en la consola.

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
Porcentaje de compresión	–	Basic	El porcentaje de datos de transferencia que se DataSync comprimieron antes de enviarlos a través de la red. Si lo estás usando DescribeTaskExecution, puedes calcular este contador con <code>1 - BytesCompressed / BytesWritten</code>.

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
¿Preparado	FilesPrepared	Mejorado	El número de objetos que DataSync se intentarán transferir tras comparar las ubicaciones de origen y destino. En la consola, este contador también puede mostrar el número de objetos que se DataSync omiten durante la preparación. Para obtener más información, consulte ¿Cómo DataSync se prepara la transferencia de datos. Este contador no se aplica si configuras la tarea para transferir todos los datos. En ese escenario, DataSync copia todo desde el origen hasta el destino sin comparar las diferencias entre las ubicaciones.

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
Velocidad de procesamiento	–	Mejorado, básico	La velocidad a la que DataSync lee los archivos, objetos y directorios en la ubicación de origen. La velocidad de procesamiento se basa en varias CloudWatch métricas. Las métricas exactas dependen del modo de tarea que utilices. Modo mejorado: - FilesListedSource - FilesPrepared - FilesTransferred - FilesVerified Modo básico: - FilesPreparedSource - FilesPreparedDestination - FilesTransferred

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
			- FilesVerifiedSource - FilesVerifiedDestination
Restante	–	Basic	El número restante de archivos, objetos y directorios que se DataSync espera transferir a través de la red. Si lo está utilizando o DescribeTaskExecution, puede calcular este contador FilesTransferred restando de EstimatedFilesToTransfer

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
Omitido *	FilesSkipped	Mejorado, básico	El número de archivos, objetos y directorios que se DataSync omiten durante la transferencia. * — En el modo mejorado, Skipped no aparece en la consola. En su lugar, los elementos omitidos se incluyen en el contador Preparado cuando se transfieren solo los datos que han cambiado o en el contador Transferido cuando se transfieren todos los datos.

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
Transferidos	FilesTransferred	Mejorado, básico	El número de archivos, objetos y directorios que se DataSync transferir en a través de la red. Este valor se actualiza periódicamente durante la ejecución de la tarea cuando se lee algo del origen y se envía a través de la red. Si DataSync no se puede transferir algo, este valor puede ser inferior a EstimatedFilesToTransfer. Este valor también puede ser mayor que EstimatedFilesToTransfer en algunos casos. Este contador es específico de la implementación para algunos tipos de ubicaciones, así que no lo utilices como una indicación exacta de lo que se está transfiriendo

Consola	DescribeTaskExecution	Compatibilidad con el modo tarea	Descripción
			ni para supervisar la ejecución de la tarea. En la consola, este contador también puede mostrarte el número de objetos que se DataSync omiten durante la transferencia de una tarea en modo mejorado. Para obtener más información, consulte ¿Cómo se DataSync transfieren tus datos?
Verificado	FilesVerified	Mejorado, básico	El número de archivos, objetos y directorios que se DataSync verifica durante la transferencia. Al configurar la tarea para comprobar únicamente los datos transferidos, DataSync no comprueba los directorios en algunas situaciones ni los archivos u objetos que no se transfieren.

Supervisión de las transferencias de datos con CloudWatch las métricas de Amazon

Amazon CloudWatch proporciona métricas para realizar un seguimiento del rendimiento de las DataSync transferencias y solucionar problemas relacionados con la tarea de transferencia.

Puedes monitorizar el rendimiento AWS DataSync de las transferencias mediante CloudWatch las métricas de Amazon. DataSync Las métricas se envían automáticamente CloudWatch en intervalos de 5 minutos (independientemente de cómo [configures el registro](#)). Las métricas se conservan durante un período de 15 meses.

Para ver CloudWatch las métricas DataSync, puedes usar las siguientes herramientas:

- La CloudWatch consola
- La CloudWatch CLI
- La CloudWatch API
- La DataSync consola (en la página de detalles de la ejecución de la tarea)

Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).

CloudWatch métricas para DataSync

DataSync las métricas utilizan el espacio de `aws/datasync` nombres y proporcionan métricas para las siguientes dimensiones:

- `AgentId`— El identificador único del agente (si la tarea utiliza un agente).
- `TaskId`— El identificador único de la tarea. Adopta el formato `task-01234567890abcdef`.

El espacio de nombres de `aws/datasync` incluye las siguientes métricas. Algunas métricas no están disponibles en todos los [modos de tarea](#).

CloudWatch métrica	Compatibilidad con el modo tarea	Descripción
<code>BytesCompressed</code>	Basic	El número de bytes físicos que se DataSync transfiere a través de la red después de la compresión (si la

CloudWatch métrica	Compatibilidad con el modo tarea	Descripción
		compresión es posible). Este número suele ser inferior a, <code>BytesTransferred</code> a menos que los datos no se puedan comprimir. Unidad: bytes
<code>BytesPreparedDestination</code>	Basic	El número de bytes lógicos que DataSync se preparan en la ubicación de destino. Unidad: bytes
<code>BytesPreparedSource</code>	Basic	El número de bytes lógicos que DataSync se preparan en la ubicación de origen. Unidad: bytes
<code>BytesTransferred</code>	Basic	El número de bytes que se DataSync envían a la red antes de la compresión (si la compresión es posible). Para conocer el número de bytes transferidos a través de la red, consulte la <code>BytesCompressed</code> métrica. Unidad: bytes
<code>BytesVerifiedDestination</code>	Basic	El número de bytes lógicos que se DataSync verifican en la ubicación de destino. Unidad: bytes
<code>BytesVerifiedSource</code>	Basic	El número de bytes lógicos que se DataSync verifican en la ubicación de origen. Unidades: bytes
<code>BytesWritten</code>	Mejorado, básico	El número de bytes lógicos que se DataSync escriben en la ubicación de destino. Unidad: bytes

CloudWatch métrica	Compatibilidad con el modo tarea	Descripción
FilesDeleted	Mejorado, básico	El número de archivos, objetos y directorios que se DataSync eliminan en la ubicación de destino. Si no configura la tarea para eliminar datos del destino que no estén en el origen, el valor siempre será 0. Unidad: recuento
FilesListedSource	Mejorado	El número de objetos que DataSync se encuentran en la ubicación de origen. Unidad: recuento
FilesPrepared	Mejorado	El número de objetos que DataSync se intentarán transferir tras comparar las ubicaciones de origen y destino. Para obtener más información, consulte ¿Cómo DataSync se prepara la transferencia de datos. Esta métrica no se aplica si configuras la tarea para transferir todos los datos. En ese escenario, DataSync copia todo desde el origen hasta el destino sin comparar las diferencias entre las ubicaciones. Unidad: recuento
FilesPreparedDestination	Basic	El número de archivos, objetos y directorios que DataSync se prepara en la ubicación de destino. Unidad: recuento
FilesPreparedSource	Basic	El número de archivos, objetos y directorios que DataSync se prepara en la ubicación de origen. Unidad: recuento

CloudWatch métrica	Compatibilidad con el modo tarea	Descripción
FilesSkipped	Basic	El número de archivos, objetos y directorios que se DataSync omiten durante la transferencia. Unidad: recuento
FilesTransferred	Mejorado, básico	El número de archivos, objetos y directorios que se DataSync transfieren a través de la red. Este valor se actualiza periódicamente durante la ejecución de la tarea cuando se lee algo del origen y se envía a través de la red.  Note Este valor puede ser inferior al EstimatedFilesToTransfer de una DescribeTaskExecution respuesta si DataSync no se transfiere algo. Este valor también puede ser mayor que EstimatedFilesToTransfer en algunos casos. Esta métrica es específica de la implementación para algunos tipos de ubicación, por tanto, no la utilice como indicador exacto de lo que se transfirió o para monitorizar la ejecución de tareas. Unidad: recuento
FilesVerified	Mejorado	El número de objetos que se DataSync verifica durante la transferencia. Unidad: recuento

CloudWatch métrica	Compatibilidad con el modo tarea	Descripción
FilesVerifiedDestination	Basic	El número de archivos, objetos y directorios que se DataSync verifica en la ubicación de destino. Unidad: recuento
FilesVerifiedSource	Basic	El número de archivos, objetos y directorios que se DataSync verifica en la ubicación de origen. Unidad: recuento

Supervise sus transferencias de datos con informes de tareas

Los informes de tareas proporcionan información detallada sobre lo que se AWS DataSync intenta transferir, omitir, verificar y eliminar durante la ejecución de una tarea. Para obtener más información, consulte [Cómo DataSync transfiere los archivos, objetos y directorios](#).

Los informes de tareas se generan en formato JSON. Puede personalizar el nivel de detalle de los informes:

- [Los informes de tareas únicamente resumidos](#) proporcionan los detalles necesarios sobre la ejecución de la tarea, como el número de archivos transferidos y si DataSync pueden verificar la integridad de los datos de esos archivos.
- Los [informes de tareas estándar](#) incluyen un resumen e informes detallados que enumeran cada archivo, objeto o carpeta que se DataSync intenta transferir, omitir, verificar o eliminar. Con un informe de tareas estándar, también puede especificar el [nivel de informe](#) para mostrar solo los errores de la ejecución de la tarea o tanto aciertos como errores.

Casos de uso

Estas son algunas situaciones en las que los informes de tareas pueden ayudarle a supervisar y auditar sus transferencias de datos:

- Al migrar millones de archivos, identifique rápidamente los archivos que DataSync tienen problemas para transferirse.
- Verifica chain-of-custody los procesos de tus archivos.

Resumen de los informes de tareas

Un informe que es solo un resumen de la ejecución de una tarea incluye los siguientes detalles:

- El Cuenta de AWS que ejecutó la tarea
- Ubicaciones de origen y destino
- El número total de archivos, objetos y carpetas que se han omitido, transferido, verificado y eliminado
- El total de bytes (lógicos y físicos) que se han transferido
- Si la ejecución de la tarea se ha completado, se ha cancelado o si se producido un error
- Las horas de inicio y finalización (incluido el tiempo total de la transferencia)
- La configuración de la tarea (como los límites de ancho de banda, la verificación de la integridad de los datos y otras opciones para la DataSync transferencia)

Informes de tareas estándar

Un informe de tareas estándar incluye un [resumen](#) de la ejecución de la tarea, además de informes detallados de lo que se DataSync intenta transferir, omitir, verificar y eliminar.

Temas

- [Nivel del informe](#)
- [Informes transferidos](#)
- [Informes de omisión](#)
- [Informes de verificación](#)
- [Informes de eliminación](#)

Nivel del informe

Con los informes de tareas estándar, puede elegir uno de los siguientes niveles de informe:

- Solo errores
- Éxitos y errores (básicamente una lista de todo lo que ha ocurrido durante la ejecución de la tarea)

Por ejemplo, es posible que desees ver qué archivos DataSync se omitieron correctamente durante la transferencia y cuáles no. Es posible que los archivos que se DataSync omitieron correctamente sean aquellos que desee excluir DataSync a propósito porque ya existen en la ubicación de destino. Sin embargo, si se omite un error, por ejemplo, podría indicar que DataSync no tiene los permisos adecuados para leer un archivo.

Informes transferidos

Una lista de archivos, objetos y directorios que se DataSync intentaron transferir durante la ejecución de la tarea. Un informe de transferencia incluye los siguientes detalles:

- Las rutas de los datos transferidos
- Qué se ha transferido (contenido, metadatos o ambos)
- Los metadatos, que incluyen el tipo de datos, el tamaño del contenido (solo objetos y archivos) y más
- La hora en que se ha transferido un elemento
- La versión del objeto (si el destino es un bucket de Amazon S3 que tiene habilitado el control de versiones)
- Si se ha sobrescrito algo en el destino
- Si un artículo se ha transferido correctamente

Note

Al mover datos entre depósitos de S3, el prefijo que especifique en su [ubicación de origen](#) puede aparecer en su informe (o en los CloudWatch registros de Amazon), incluso si ese prefijo no existe como objeto en su ubicación de destino. (En la DataSync consola, es posible que también veas que este prefijo aparece como datos omitidos o verificados).

Informes de omisión

Una lista de archivos, objetos y directorios que DataSync se encuentran en la ubicación de origen pero que no se han intentado transferir. Los motivos por los que DataSync se omiten los datos

pueden depender de varios factores, como la forma en que se configuran las tareas y los permisos del sistema de almacenamiento. Estos son algunos ejemplos:

- Uno de los archivos de la ubicación de origen existe en las ubicaciones de origen y de destino. El archivo del origen no se ha modificado desde la ejecución anterior de la tarea. Como [solo transfiere datos que han cambiado](#), DataSync no transferirá ese archivo la próxima vez que ejecute la tarea.
- Un objeto que existe en ambas ubicaciones cambia en el origen. Al ejecutar la tarea, DataSync omite este objeto en el destino porque la tarea no [sobrescribe los datos del](#) destino.
- DataSync omite un objeto del origen que utiliza una [clase de almacenamiento de archivos y no](#) se restaura. Debes restaurar un objeto archivado para DataSync poder leerlo.
- DataSync omite un archivo, objeto o directorio de la ubicación de origen porque no puede leerlo. Si esto ocurre y no es lo esperado, comprueba los permisos de acceso del almacenamiento y asegúrate de que DataSync puede leer lo que se omitió.

Un informe de omisión incluye los siguientes detalles:

- Las rutas de los datos omitidos
- La hora en que se ha omitido un elemento
- La razón por la que se ha omitido
- Si un elemento se ha omitido correctamente

Note

Los informes de omisión pueden ser extensos si incluyen aciertos y errores, se configura la tarea para [transferir solo los datos que han cambiado](#) y los datos de origen ya existen en el destino.

Informes de verificación

Una lista de archivos, objetos y directorios de los que se DataSync intentó comprobar la integridad durante la ejecución de la tarea. Un informe de verificación incluye los siguientes detalles:

- Las rutas de los datos verificados
- La hora en que se ha verificado un elemento

- El motivo del error en la verificación (si lo hubiera)
- Las SHA256 sumas de control de origen y destino (solo archivos)
- Si un elemento se ha verificado correctamente

Tenga en cuenta lo siguiente acerca de los informes verificados:

- Cuando configura la tarea para [verificar solo los datos transferidos](#), DataSync no verifica los directorios en algunas situaciones ni los archivos u objetos que no se transfieren. En cualquier caso, DataSync no incluye datos no verificados en este informe.
- Si utilizas el [modo mejorado](#), la verificación puede tardar más de lo habitual si transfieres objetos grandes.

Informes de eliminación

Una lista de archivos, directorios y objetos que se eliminaron durante la ejecución de la tarea. DataSync genera este informe solo si [configura la tarea](#) para eliminar datos de la ubicación de destino que no estén en la fuente. Un informe de eliminación incluye los siguientes detalles:

- Las rutas de los datos eliminados
- Si un elemento se ha eliminado correctamente
- La hora en que se ha eliminado un elemento

Ejemplos de informes de tareas

El nivel de detalle del informe de tareas depende de usted. Estos son algunos ejemplos de informes de datos transferidos con la siguiente configuración:

- Tipo de informe: estándar
- Nivel de informe: éxitos y errores

Note

Los informes utilizan la norma ISO-8601 para el formato de marca de tiempo. Las horas aparecen en UTC y se miden en nanosegundos. Este comportamiento difiere de la forma en que se miden otras métricas de los informes de tareas. Por ejemplo, [los detalles de la](#)

[ejecución de las tareas](#), tales como `TransferDuration` y `VerifyDuration`, se miden en milisegundos.

Los informes de tareas del modo mejorado utilizan un esquema algo diferente al de los informes de tareas del modo básico. Los siguientes ejemplos pueden ayudarle a saber qué esperar de sus informes en función del [modo de tarea](#) que utilice.

Ejemplo de informes de datos transferidos con estado de éxito

Los siguientes informes muestran las transferencias correctas de un objeto denominado `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": "jTqRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
    "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": "jqtRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
      "TransferTimestamp": "2022-01-07T16:59:45.747270957Z",
      "TransferType": "CONTENT_AND_METADATA",
      "TransferStatus": "SUCCESS"
    }]
  }

```

Ejemplo de informes de datos transferidos con estado de error

Los siguientes informes proporcionan ejemplos de casos en los que no se DataSync puede transferir un objeto denominado `object1.txt`.

Enhanced mode

Este informe muestra que no DataSync pueden acceder a un objeto nombrado `object1.txt` debido a un problema de AWS KMS permisos. (Si aparece un error como este, consulte [Acceso a buckets de S3 mediante el cifrado del 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

Este informe muestra que un objeto denominado `object1.txt` no se transfirió debido a un problema con los permisos del bucket de S3. (Si aparece un error como este, consulte [Proporcionar DataSync acceso a los depósitos de 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": "jqtRtX3jN4J2G8k0sFSGYK1f35KqpAVP",
    "TransferTimestamp": "2022-01-07T16:59:45.747270957Z",
    "TransferType": "CONTENT_AND_METADATA",
    "TransferStatus": "FAILED",
    "FailureReason": "S3 Get Object Failed",
    "FailureCode": 40974
  }]
}

```

Limitaciones

- Los informes de tareas individuales no pueden superar los 5 MB. Si va a copiar una gran cantidad de archivos, es posible que el informe de tareas se divida en varios informes.
- Hay situaciones en las que la creación de informes de tareas puede afectar al rendimiento de la transferencia de datos. Por ejemplo, puede que lo note cuando la conexión de red tiene una alta latencia y los archivos que está transfiriendo son pequeños o si solo está copiando los cambios en los metadatos.

Crear tus informes de DataSync tareas

AWS DataSync los informes de tareas solo pueden ser un resumen de la ejecución de la tarea o un conjunto de informes detallados sobre lo que se DataSync intenta transferir, omitir, verificar y eliminar.

Requisitos previos

Antes de poder crear un informe de tarea, debe ejecutar las siguientes tareas.

Temas

- [Creación de un bucket de S3 para sus informes de tarea](#)
- [Permite DataSync cargar informes de tareas a tu bucket de S3](#)

Creación de un bucket de S3 para sus informes de tarea

Si aún no tiene uno, [cree un depósito de S3](#) donde DataSync pueda cargar su informe de tareas. Los informes se almacenan en la clase de almacenamiento S3 Standard.

Le recomendamos lo siguiente para este bucket:

- Si planea transferir datos a un bucket de S3, no utilice el mismo bucket para el informe de tareas si [desactiva la opción Conservar los archivos eliminados](#). De lo contrario, DataSync eliminará todos los informes de tareas anteriores cada vez que ejecute una tarea, ya que esos informes no existen en su ubicación de origen.
- Para evitar una configuración compleja de los permisos de acceso, asegúrate de que el grupo de informes de tareas esté en la misma región Cuenta de AWS y en la misma región que la tarea de DataSync transferencia.

Permite DataSync cargar informes de tareas a tu bucket de S3

Debe configurar un rol AWS Identity and Access Management (de IAM) que le permita DataSync cargar un informe de tareas en su bucket de S3.

En la DataSync consola, puede crear un rol de IAM que, en la mayoría de los casos, incluya automáticamente los permisos para cargar un informe de tareas en su bucket. Tenga en cuenta que es posible que este rol generado automáticamente no satisfaga sus necesidades desde el punto de vista de los privilegios mínimos. Esta función tampoco funcionará si el bucket está cifrado con una clave gestionada por el cliente AWS Key Management Service (AWS KMS) (SSE-KMS). En estos casos, puede crear el rol de forma manual siempre que dicho rol haga al menos lo siguiente:

- [Evita el problema del suplente confuso entre servicios](#) en la entidad de confianza del rol.

En el siguiente ejemplo completo se muestra cómo se pueden utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves contextuales para evitar que se confunda con el problema de los adjuntos. 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 cargar un informe de tareas a su bucket de S3.

El siguiente ejemplo lo hace incluyendo la acción de `s3:PutObject` solo para un prefijo específico (`reports/`) en el bucket.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "s3:PutObject"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:s3:::your-task-reports-bucket/reports/*"
  }]
}
```

- Si el bucket de S3 está cifrado con una clave SSE-KMS gestionada por el cliente, la [política de la clave](#) debe incluir la función de IAM que se DataSync utiliza para acceder al bucket.

Para obtener más información, consulte [Acceso a buckets de S3 mediante el cifrado del servidor](#).

Creación de un informe de tareas de tipo solo resumen

Puede configurar un informe de tareas que incluya un [resumen solo](#) al crear la DataSync tarea, iniciarla o actualizarla.

Los siguientes pasos muestran cómo configurar un informe de tareas de tipo solo resumen al crear una tarea.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. Desplácese hacia abajo hasta la sección Informe de tareas. En Tipo de informe, seleccione Solo resumen.

5. Para el depósito de informes de S3, elija un depósito de S3 en el que DataSync desee cargar el informe de tareas.

 Tip

Si planea transferir datos a un bucket de S3, no utilice el mismo bucket para el informe de tareas si [desactiva la opción Conservar los archivos eliminados](#). De lo contrario, DataSync eliminará todos los informes de tareas anteriores cada vez que ejecute una tarea, ya que esos informes no existen en su ubicación de origen.

6. En Carpeta, introduce un prefijo para usarlo en tu informe de tareas cuando lo DataSync cargues en tu bucket de S3 (por ejemplo, **reports/**).

Asegúrese de incluir el carácter delimitador adecuado al final del prefijo. Este carácter normalmente es una barra inclinada (/). Para obtener más información, consulte [Organizar objetos con prefijos](#) en la Guía del usuario de Amazon S3.

7. En Rol de IAM, realice una de las operaciones siguientes:
 - Elija Generar automáticamente para crear DataSync automáticamente un rol de IAM con los permisos necesarios para acceder al bucket de S3.

Si DataSync anteriormente creó un rol de IAM para este bucket de S3, ese rol se elige de forma predeterminada.

- Elija un rol de IAM personalizado que haya creado.

En algunos casos, es posible que tenga que crear el rol por sí mismo. Para obtener más información, consulte [Permite DataSync cargar informes de tareas a tu bucket de S3](#).

 Important

Si el bucket de S3 está cifrado con una clave SSE-KMS administrada por el cliente, la política de la clave debe incluir la función de IAM que se DataSync utiliza para acceder al bucket.

Para obtener más información, consulte [Acceso a buckets de S3 mediante el cifrado del servidor](#).

8. Termine de crear la tarea y, a continuación, [inicie la tarea](#) para empezar a transferir los datos.

Cuando se complete la transferencia, podrá [ver el informe de la tarea](#).

Uso del AWS CLI

1. Copie el siguiente 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 el parámetro `--source-location-arn`, especifique el nombre de recurso de Amazon (ARN) de la ubicación de origen en la transferencia. `us-east-1` Sustitúyalo por el correspondiente Región de AWS, `123456789012` sustitúyalo por el Cuenta de AWS número correspondiente y `12345678abcdefgh` sustitúyalo por el identificador de ubicación de origen correspondiente.
3. Para el parámetro `--destination-location-arn`, especifique el ARN de la ubicación de destino en la transferencia. Sustituya por `us-east-1` el correspondiente Región de AWS, `123456789012` sustitúyalo por el Cuenta de AWS número correspondiente y `abcdefgh12345678` sustitúyalo por el identificador de ubicación de destino correspondiente.
4. Para el parámetro `--task-report-config`, haga lo siguiente:
 - `Subdirectory`— `reports/` Sustitúyalo por el prefijo del bucket de S3 en el que desee DataSync cargar los informes de tareas.

Asegúrese de incluir el carácter delimitador adecuado al final del prefijo. Este carácter normalmente es una barra inclinada (/). Para obtener más información, consulte [Organizar objetos con prefijos](#) en la Guía del usuario de Amazon S3.

- **S3BucketArn:** especifique el ARN del bucket de S3 donde desea cargar su informe de tareas.

 Tip

Si planea transferir datos a un bucket de S3, no utilice el mismo bucket para el informe de tareas si [desactiva la opción Conservar los archivos eliminados](#). De lo contrario, DataSync eliminará todos los informes de tareas anteriores cada vez que ejecute una tarea, ya que esos informes no existen en su ubicación de origen.

- **BucketAccessRoleArn**— Especifique la función de IAM que permite DataSync cargar un informe de tareas en su bucket de S3.

Para obtener más información, consulte [Permite DataSync cargar informes de tareas a tu bucket de S3](#).

 Important

Si su depósito de S3 está cifrado con una clave SSE-KMS gestionada por el cliente, la política de la clave debe incluir la función de IAM que se DataSync utiliza para acceder al depósito.

Para obtener más información, consulte [Acceso a buckets de S3 mediante el cifrado del servidor](#).

- **OutputType:** especifique SUMMARY_ONLY.

Para obtener más información, consulte [Resumen de los informes de tareas](#).

5. Ejecute el comando `create-task` para crear la tarea.

Obtendrá una respuesta como la siguiente, en la que se muestra el ARN de la tarea que ha creado. Necesitará este ARN para ejecutar el comando `start-task-execution`.

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
}
```

6. Copie el siguiente 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 el parámetro `--task-arn`, especifique el ARN de la tarea que está iniciando. Utilice el ARN que ha recibido al ejecutar el comando `create-task`.
8. Ejecute el comando `start-task-execution`.

Cuando se complete la transferencia, podrá [ver el informe de la tarea](#).

Creación de un informe de tareas estándar

Puede configurar un [informe de tareas estándar](#) al crear su DataSync tarea, iniciarla o actualizarla.

Los siguientes pasos muestran cómo configurar un informe de tareas de tipo estándar al crear una tarea.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. Desplácese hacia abajo hasta la sección Informe de tareas. En Tipo de informe, seleccione Informe estándar.
5. En Nivel de informe, elija una de las siguientes opciones:
 - Solo errores: el informe de tareas incluye solo los problemas relacionados con lo que se DataSync intentó transferir, omitir, verificar y eliminar.
 - Éxitos y errores: el informe de tareas incluye lo que se DataSync ha transferido, omitido, verificado y eliminado correctamente y lo que no.
 - Personalizado: le permite elegir si desea ver solamente los errores o los éxitos y errores para aspectos específicos del informe de tareas.

Por ejemplo, puede seleccionar Éxitos y errores para la lista de archivos transferidos, pero Solo errores para el resto del informe.

6. Si va a realizar la transferencia a un bucket de S3 que utiliza el control de versiones de objetos, deje la opción Incluir versiones de objetos de Amazon S3 seleccionada si desea que su informe incluya la nueva versión de cada objeto transferido.
7. En el caso del segmento de informes de S3, elija un depósito de S3 en el que desee DataSync cargar el informe de tareas.

 Tip

Si planea transferir datos a un bucket de S3, no utilice el mismo bucket para el informe de tareas si [desactiva la opción Conservar los archivos eliminados](#). De lo contrario, DataSync eliminará todos los informes de tareas anteriores cada vez que ejecute una tarea, ya que esos informes no existen en su ubicación de origen.

8. En Carpeta, introduce un prefijo para usarlo en tu informe de tareas cuando lo DataSync cargues en tu bucket de S3 (por ejemplo, **reports/**). Asegúrese de incluir el carácter delimitador adecuado al final del prefijo. Este carácter normalmente es una barra inclinada (/). Para obtener más información, consulte [Organizar objetos con prefijos](#) en la Guía del usuario de Amazon S3.
9. En Rol de IAM, realice una de las operaciones siguientes:

- Elija Generar automáticamente para crear DataSync automáticamente un rol de IAM con los permisos necesarios para acceder al bucket de S3.

Si DataSync anteriormente creó un rol de IAM para este bucket de S3, ese rol se elige de forma predeterminada.

- Elija un rol de IAM personalizado que haya creado.

En algunos casos, es posible que tenga que crear el rol por sí mismo. Para obtener más información, consulte [Permite DataSync cargar informes de tareas a tu bucket de S3](#).

 Important

Si el bucket de S3 está cifrado con una clave SSE-KMS administrada por el cliente, la política de la clave debe incluir la función de IAM que se DataSync utiliza para acceder al bucket.

Para obtener más información, consulte [Acceso a buckets de S3 mediante el cifrado del servidor](#).

10. Termine de crear la tarea e [inicie la tarea](#) para empezar a transferir los datos.

Cuando se complete la transferencia, podrá [ver el informe de la tarea](#).

Uso del AWS CLI

1. Copie el siguiente 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 el parámetro --source-location-arn, especifique el ARN de la ubicación de origen en la transferencia. Sustituya por *us-east-1* el correspondiente Región de AWS, *123456789012* sustitúyalo por el Cuenta de AWS número correspondiente y *12345678abcdefgh* sustitúyalo por el identificador de ubicación de origen correspondiente.
3. Para el parámetro --destination-location-arn, especifique el ARN de la ubicación de destino en la transferencia. Sustituya por *us-east-1* el correspondiente Región de AWS, *123456789012* sustitúyalo por el Cuenta de AWS número correspondiente y *abcdefgh12345678* sustitúyalo por el identificador de ubicación de destino correspondiente.
4. Para el parámetro --task-report-config, haga lo siguiente:
 - Subdirectory— *reports/* Sustitúyalo por el prefijo del bucket de S3 en el que desee DataSync cargar los informes de tareas. Asegúrese de incluir el carácter delimitador adecuado al final del prefijo. Este carácter normalmente es una barra inclinada (/). Para obtener más información, consulte [Organizar objetos con prefijos](#) en la Guía del usuario de Amazon S3.
 - S3BucketArn: especifique el ARN del bucket de S3 donde desea cargar su informe de tareas.

 Tip

Si planea transferir datos a un bucket de S3, no utilice el mismo bucket para el informe de tareas si [desactiva la opción Conservar los archivos eliminados](#). De lo contrario, DataSync eliminará todos los informes de tareas anteriores cada vez que ejecute una tarea, ya que esos informes no existen en su ubicación de origen.

- `BucketAccessRoleArn`— Especifique la función de IAM que permite DataSync cargar un informe de tareas en su bucket de S3.

Para obtener más información, consulte [Permite DataSync cargar informes de tareas a tu bucket de S3](#).

 Important

Si su depósito de S3 está cifrado con una clave SSE-KMS gestionada por el cliente, la política de la clave debe incluir la función de IAM que se DataSync utiliza para acceder al depósito.

Para obtener más información, consulte [Acceso a buckets de S3 mediante el cifrado del servidor](#).

- `OutputType`: especifique el informe de STANDARD.

Para obtener más información, consulte [Informes de tareas estándar](#) Tipos de informes de tareas.

- (Opcional) `ReportLevel`: especifique si desea `ERRORS_ONLY` (opción predeterminada) o `SUCCESSES_AND_ERRORS` en su informe.
- (Opcional) `ObjectVersionIds`: si va a realizar la transferencia a un bucket de S3 que utiliza el control de versiones de objetos, especifique `NONE` si no desea incluir la nueva versión para cada objeto transferido en el informe.

Esta opción está configurada en `INCLUDE` de forma predeterminada.

- (Opcional) `Overrides`: personalice el `ReportLevel` de un aspecto concreto del informe.

Por ejemplo, es posible que desee consultar `SUCCESSES_AND_ERRORS` la lista de lo que se DataSync elimina en su ubicación de destino, pero `ERRORS_ONLY` prefiera ver todo lo demás.

En este ejemplo, añadiría la siguiente opción `Overrides` al parámetro `--task-report-config`:

```
"Overrides":{
  "Deleted":{
    "ReportLevel":"SUCSESSES_AND_ERRORS"
  }
}
```

Si no usa `Overrides`, todo el informe usará el `ReportLevel` que usted especifique.

5. Ejecute el comando `create-task` para crear la tarea.

Obtendrá una respuesta como la siguiente, en la que se muestra el ARN de la tarea que ha creado. Necesitará este ARN para ejecutar el comando `start-task-execution`.

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:123456789012:task/task-12345678abcdefgh"
}
```

6. Copie el siguiente 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 el parámetro `--task-arn`, especifique el ARN de la tarea que está ejecutando. Utilice el ARN que ha recibido al ejecutar el comando `create-task`.
8. Ejecute el comando `start-task-execution`.

Cuando se complete la transferencia, podrá [ver el informe de la tarea](#).

Ver tus informes de DataSync tareas

DataSync crea informes de tareas para cada ejecución de tareas. Cuando la ejecución se complete, encontrará el informe de la tarea pertinente en su bucket de S3. Los informes de tareas se organizan con prefijos que incluyen IDs las tareas y sus ejecuciones.

Para ayudar a localizar los informes de tareas en el bucket de S3, utilice estos ejemplos:

- Informe de tareas de tipo solo resumen: *reports-prefix/Summary-Reports/task-id-folder/task-execution-id-folder*

- Informe de tareas estándar: *reports-prefix*/Detailed-Reports/*task-id-folder*/*task-execution-id-folder*

Como los informes de tareas están en formato JSON, tiene varias opciones para verlos:

- Visualizar un informe con [Amazon S3 Select](#).
- Visualice los informes mediante AWS servicios como AWS Glue Amazon Athena y Amazon QuickSight Para obtener más información sobre la visualización de los informes de tareas, consulte el [blog sobre almacenamiento de AWS](#).

Supervisión de las transferencias de datos con Amazon CloudWatch Logs

Puede supervisar su AWS DataSync transferencia mediante CloudWatch los registros. Le recomendamos que configure la tarea para registrar al menos la información básica (como los errores de transferencia).

DataSync Permitir cargar registros a un grupo de CloudWatch registros

Para [configurar el registro](#) de su DataSync tarea, necesita un grupo de CloudWatch registros que DataSync tenga permiso para enviar registros. Este acceso se configura mediante un rol AWS Identity and Access Management (IAM). La forma en que esto funcione específicamente depende del [modo de tarea](#).

Enhanced mode

Con el modo mejorado, envía DataSync automáticamente los registros de tareas a un grupo de registros denominado `/aws/datasync`. Si ese grupo de registros no existe en la suya Región de AWS, DataSync crea el grupo de registros en su nombre mediante un [rol vinculado al servicio](#) de IAM al crear la tarea.

Basic mode

Existen dos formas de configurar un grupo de CloudWatch registros para una DataSync tarea mediante el modo Básico. En la consola, puede crear automáticamente un rol de IAM que, en la mayoría de los casos, incluya los permisos DataSync necesarios para cargar registros. Tenga en cuenta que es posible que este rol generado automáticamente no satisfaga sus necesidades desde el punto de vista de los privilegios mínimos.

Si desea utilizar un grupo de CloudWatch registros existente o va a crear sus tareas mediante programación, debe crear el rol de IAM usted mismo.

El siguiente ejemplo es una política de IAM que concede estos permisos.

```
{
  "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:*:*"
    }
  ]
}
```

La política utiliza Condition declaraciones para garantizar que solo DataSync las tareas de la cuenta especificada tengan acceso al grupo de CloudWatch registros especificado. Recomendamos utilizar las claves de contexto de condición global [aws:SourceArn](#) y [aws:SourceAccount](#) en estas declaraciones de Condition para evitar el problema de los suplentes confusos entre servicios. Para obtener más información, consulte [Prevención de la sustitución confusa entre servicios](#).

Para especificar la DataSync tarea o las tareas, *region* sustitúyalo por el Región de AWS código de región de la ubicación de las tareas (por ejemplo, *us-west-2*) y *account-id* sustitúyelo por el Cuenta de AWS identificador de la cuenta que contiene las tareas. Para especificar el grupo de CloudWatch registros, sustituya los mismos valores. También puede modificar la declaración de Resource para que se dirija a grupos de registro específicos. Para obtener más información sobre el uso de SourceArn y SourceAccount, consulte [Claves de contexto de condición globales](#) en la Guía del usuario de IAM.

Para aplicar la política, guarde esta instrucción en un archivo del equipo local. A continuación, ejecute el siguiente AWS CLI comando para aplicar la política de recursos. Para utilizar este comando de ejemplo, sustituya *full-path-to-policy-file* por la ruta del archivo que contiene la declaración de política.

```
aws logs put-resource-policy --policy-name trust-datasync --policy-document  
file:///full-path-to-policy-file
```

 Note

Ejecute este comando utilizando el mismo Cuenta de AWS Región de AWS lugar donde activó su DataSync agente.

Para obtener más información, consulta la [Guía del usuario CloudWatch de Amazon Logs](#).

Configurar el registro para su DataSync tarea

Se recomienda configurar al menos algún nivel de registro para la DataSync tarea.

Antes de empezar

DataSync necesita permiso para cargar registros en un grupo de CloudWatch registros. Para obtener más información, consulte [DataSync Permitir cargar registros a un grupo de CloudWatch registros](#).

Mediante la consola de DataSync

Las siguientes instrucciones describen cómo configurar el CloudWatch registro al crear una tarea. También puede configurar el registro al editar una tarea.

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.

2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos; luego, seleccione Tareas y, a continuación, seleccione Crear tarea.
3. Configure las ubicaciones de origen y destino de la tarea.

Para obtener más información, consulte [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

4. En la página Configurar ajustes, seleccione un [modo de tarea](#) y cualquier otra opción.

Puede que te interesen algunas de las siguientes opciones:

- Especifique qué datos desea transferir mediante un [manifiesto](#) o [filtros](#).
 - Configure cómo [gestionar los metadatos de los archivos](#) y [verificar la integridad de los datos](#).
5. En Registro, elija una de las siguientes opciones:
 - Registrar información básica, como los errores de transferencia: publique registros solo con la información básica (como los errores de transferencia).
 - Registre todos los objetos y archivos transferidos: publique los registros de todos los archivos u objetos que DataSync transfiera y compruebe la integridad de los datos.
 - No genere registros
 6. Realice una de las siguientes acciones en función del modo de tarea que utilice para crear o especificar un grupo de CloudWatch registros:

Enhanced mode

Al elegir Crear tarea, utiliza (o crea) DataSync automáticamente un grupo de registros denominado `/aws/datasync`.

Basic mode

En el CloudWatch caso de un grupo de registros, especifique un grupo de registros en el que DataSync tenga permiso para cargar registros mediante una de las siguientes acciones:

- Elija Generar automáticamente para crear automáticamente un grupo de registros que permita DataSync cargar registros en él.
- Elija un grupo de registro ya existente en la Región de AWS actual.

Si elige un grupo de registros existente, asegúrese de que [DataSync tiene permiso](#) para cargar registros en ese grupo de registros.

7. Seleccione Crear tarea.

Ya está listo para [comenzar su tarea](#).

Usando el AWS CLI

1. Copie el siguiente 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. Para `--source-location-arn`, especifique el nombre de recurso de Amazon (ARN) de la ubicación de origen.
3. Para `--destination-location-arn`, especifique el ARN de la ubicación de destino.

Si realizas una transferencia entre Regiones de AWS nuestras cuentas, asegúrate de que el ARN incluya la otra región o ID de cuenta.

4. Para `--task-mode`, especifique `ENHANCED` o `BASIC`.
5. (Recomendado) Para `--name`, especifique un nombre para la tarea que pueda recordar.
6. Para `LogLevel`, especifique una de las siguientes opciones:
 - `BASIC`— Publique los registros solo con información básica (como errores de transferencia).
 - `TRANSFER`— Publique los registros de todos los archivos u objetos que DataSync transfiera y compruebe la integridad de los datos.
 - `NONE`— No genere registros.
7. Para `--cloudwatch-log-group-arn`, especifique el ARN de un grupo de CloudWatch registros.

⚠ Important

Si el suyo `--task-mode` es `ENHANCED`, no necesita especificar esta opción. Para obtener más información, consulte [DataSync Permitir cargar registros a un grupo de CloudWatch registros](#).

8. Ejecute el comando `create-task`.

Si el comando se ejecuta correctamente, recibirá una respuesta que le mostrará el ARN de la tarea que creó. Por ejemplo:

```
{
  "TaskArn": "arn:aws:datasync:us-east-1:111222333444:task/
task-08de6e6697796f026"
}
```

Ya está listo para [comenzar su tarea](#).

Uso de la DataSync API

Puede configurar el CloudWatch registro de la tarea mediante el `CloudWatchLogGroupArn` parámetro con cualquiera de las siguientes operaciones:

- [CreateTask](#)
- [UpdateTask](#)

Visualización de los registros de DataSync tareas

Al [iniciar la tarea](#), puede ver los registros de ejecución de la tarea mediante la CloudWatch consola o AWS CLI (entre otras opciones). Para obtener más información, consulta la [Guía del usuario CloudWatch de Amazon Logs](#).

DataSync proporciona registros estructurados en JSON para las tareas del modo mejorado. Las tareas del modo básico tienen registros no estructurados. Los siguientes ejemplos muestran cómo se muestran los errores de verificación en los registros del modo mejorado en comparación con los registros del 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
```

Registrar llamadas a la AWS DataSync API con AWS CloudTrail

AWS DataSync está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o una persona Servicio de AWS . DataSync CloudTrail captura todas las llamadas a la API DataSync como eventos. Las llamadas que se capturan incluyen las llamadas desde la DataSync consola y las llamadas en código a las operaciones de la DataSync API.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS DataSync. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar a AWS DataSync qué dirección IP se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

Trabajar con DataSync información en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS DataSync, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos del historial de eventos. Puedes ver, buscar y descargar eventos recientes en tu Cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de AWS DataSync, cree un registro de seguimiento. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra todos los eventos Regiones de AWS de la misma AWS partición y entrega los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas DataSync las acciones son registradas por CloudTrail. (Para obtener más información, consulta la [referencia DataSync de la API](#)).

Por ejemplo, las llamadas a las ListLocations operaciones CreateAgentCreateTask, y generan entradas en los archivos de CloudTrail registro.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales raíz o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

Para obtener más información, consulte [CloudTrail userIdentity elemento de](#) la Guía del AWS CloudTrail usuario.

Descripción de las entradas de los archivos de DataSync registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la CreateTask operación.

```
{
  "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"
}

```

Supervisión de eventos mediante Amazon EventBridge

EventBridge Los eventos de Amazon describen los cambios en DataSync los recursos. Puede configurar reglas para asignar estos eventos y dirigirlos a una o más secuencias o funciones de destino. Los eventos se emiten en la medida de lo posible.

DataSync eventos de transferencia

Los siguientes EventBridge eventos están disponibles para DataSync transferencias.

Agent state changes

Evento	Descripción
Online	El agente está configurado correctamente y listo para su uso. Este es el estado de ejecución normal de un agente.
Sin conexión	El agente ha estado fuera de contacto con el DataSync servicio durante cinco minutos o más. Esto puede suceder por varias razones. Para obtener más información, consulte ¿Qué hago si mi agente está desconectado?

Location state changes

Evento	Descripción
¿Agregando	DataSync es añadir una ubicación.
Disponible	La ubicación se ha creado y se encuentra disponible para su uso.

Task state changes

Evento	Descripción
Disponible	La tarea se creó y está lista para empezar.

Agent state changes

Running

La tarea está en curso y funciona correctamente.

No disponible

La tarea no está configurada correctamente y no se puede utilizar. Es posible que vea este evento cuando un agente asociado a la tarea se desconecte.

En cola

Otra tarea consiste en ejecutar y utilizar el mismo agente. DataSync ejecuta las tareas en serie (primero en entrar, primero en salir).

Task execution state changes

Evento

Descripción

En cola

La ejecución de otra tarea consiste en ejecutar y utilizar el mismo DataSync agente. Para obtener más información, consulte [Saber cuándo la tarea está en cola](#).

Launching (inicio o lanzamiento)

DataSync está inicializando la ejecución de la tarea. Este estado por lo general se realiza rápidamente, pero puede tardar hasta varios minutos.

Preparación

DataSync está determinando qué datos se van a transferir.

Este paso puede tardar solo unos minutos o unas horas, en función del número de archivos, objetos o directorios en ambas ubicaciones y de la forma en que configure la tarea. Es posible que la preparación tampoco se aplique a su tarea. Para obtener más información, consulte [¿Cómo DataSync se prepara la transferencia de datos](#).

Agent state changes

Transferencia	DataSync está realizando la transferencia de datos real.
Verificando	DataSync está realizando una comprobación de la integridad de los datos al final de la transferencia.
Success	La ejecución de la tarea se realizó correctamente.
Cancelling	La ejecución de la tarea está en proceso de ser cancelada.
Error	Falló la ejecución de la tarea.

Supervisión AWS DataSync con herramientas manuales

Puedes realizar un seguimiento de tus AWS DataSync transferencias desde la consola o la línea de comandos.

Supervise su transferencia mediante la DataSync consola

Puedes monitorear tu DataSync transferencia mediante la consola, que proporciona métricas en tiempo real, como los datos transferidos, el rendimiento de datos y archivos y la compresión de datos.

Para supervisar la transferencia mediante la consola DataSync

1. Tras [iniciar la DataSync tarea](#), selecciona Ver detalles de ejecución.
2. Consulte las métricas de su transferencia.

Monitoreo de transferencias mediante la AWS CLI

Puedes monitorizar tu DataSync transferencia mediante AWS Command Line Interface (AWS CLI).

Copie el siguiente comando `describe-task-execution`. Para utilizar este comando de ejemplo, sustituya *user input placeholders* por su propia información.

```
aws datasync describe-task-execution \
  --task-execution-arn 'arn:aws:datasync:region:account-id:task/task-id/execution/task-
  execution-id'
```

Este comando devuelve información acerca de la ejecución de una tarea similar a la que se muestra a continuación.

```
{
  "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"
    }
  }
}

```

- Si la ejecución de la tarea se realiza correctamente, el valor de Status (Estado) cambia a SUCCESS (CORRECTO). Para obtener información sobre el significado de los elementos de respuesta, consulte [DescribeTaskExecution](#).
- Si se produce un error en la ejecución, el resultado envía códigos de error que pueden ayudarle a solucionar problemas. Para obtener información sobre los códigos de error, consulte [TaskExecutionResultDetail](#).

Monitoreo de transferencias mediante la utilidad **watch**

Para monitorizar el progreso de su tarea en tiempo real desde la línea de comandos, puede utilizar la utilidad Unix `watch` estándar. Los valores de duración de la ejecución de la tarea se miden en milisegundos.

La `watch` utilidad no reconoce el DataSync alias. En el siguiente ejemplo, se muestra cómo invocar la CLI directamente. Para utilizar este comando de ejemplo, sustituya *user input placeholders* por su propia información.

```
# 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'"
```

Administrar AWS DataSync recursos

Aprenda a administrar sus AWS DataSync recursos, como los agentes, las ubicaciones y las tareas.

Administrar a tu DataSync agente

Una vez que active un DataSync agente, lo AWS administra por usted (incluidas las actualizaciones de software). [Más información](#)

Probar la conectividad y los recursos del sistema de su DataSync agente

Si bien AWS gestiona el DataSync agente una vez que está desplegado y activado, es posible que en algunos casos necesite cambiar la configuración del agente o solucionar un problema. [Más información](#)

Sustituir a tu agente DataSync

Para reemplazar a un DataSync agente, debe crear uno nuevo y actualizar las ubicaciones que utilicen el agente anterior. [Más información](#)

Limpiar DataSync los recursos

Si los usaste DataSync para una prueba o simplemente ya no necesitas sus recursos, elimínalos para que no te cobren por ellos. [Más información](#)

Reutilizar la infraestructura de un DataSync agente

Después de eliminar un recurso de agente DataSync, puede seguir utilizando la máquina virtual del agente o la EC2 instancia de Amazon para activar un agente nuevo. [Más información](#)

Administrar a tu AWS DataSync agente

Una vez que [active un AWS DataSync agente](#), AWS administra el dispositivo de la máquina virtual (VM) por usted.

Actualizaciones del software del agente

AWS actualiza automáticamente el software del agente, incluido el sistema operativo subyacente y los paquetes de DataSync software relacionados.

DataSync actualiza su agente solo cuando está inactivo. Por ejemplo, su agente no se actualizará hasta que se complete la transferencia.

Es posible que el agente se desconecte brevemente después de las actualizaciones. Esto puede ocurrir, por ejemplo, poco después de la [activación del agente](#), cuando AWS lo actualice.

Important

- DataSync parchea los agentes de forma automática y periódica para mantener su seguridad y estabilidad. DataSync los agentes utilizan Amazon Linux 2 como sistema operativo base. Puede ver el estado actual de los problemas de vulnerabilidades y exposiciones comunes (CVE) detectados en el [Amazon Linux Security Center](#). Los parches CVE se aplican automáticamente en un plazo de 30 días a partir de su fecha de lanzamiento, tal y como se indica en el Amazon Linux Security Center. La aplicación de parches se realiza siempre que el agente esté en línea y no esté ejecutando activamente la ejecución de una tarea.
- DataSync no admite la actualización manual de un EC2 agente de Amazon con las directivas cloud-init. Si actualizas un agente de esta manera, es posible que surjan problemas de interoperabilidad y no DataSync puedas activar o usar el agente.

Estados de los agentes

En la siguiente tabla se describe el estado de los DataSync agentes.

Estado del agente	Significado
Online	El agente está configurado correctamente y listo para su uso. Este es el estado de ejecución normal de un agente.

Estado del agente	Significado
Sin conexión	El agente ha estado fuera de contacto con el DataSync servicio durante cinco minutos o más. Esto puede suceder por varias razones. Para obtener más información, consulte ¿Qué hago si mi agente está desconectado?

Solución de problemas del agente

Si bien AWS administra el DataSync agente por usted, hay situaciones en las que puede que necesite volver a trabajar directamente con él. Por ejemplo, si el agente se desconecta o pierde la conexión con el sistema de almacenamiento en las instalaciones, puede intentar resolver estos problemas en la [consola local del agente](#).

Para obtener más información, consulte la sección sobre [solución de problemas de DataSync los agentes](#).

Realizar el mantenimiento de su agente

Si bien AWS gestiona el AWS DataSync agente una vez desplegado y activado, es posible que en algunos casos necesite cambiar la configuración del agente o solucionar un problema. Estos son algunos ejemplos de por qué debería trabajar con su agente a través de su consola local:

- Asigne manualmente una dirección IP al agente.
- Cómo comprobar los recursos del sistema de su agente.

Important

No necesitas usar la consola local del agente para disfrutar de una DataSync funcionalidad estándar.

Acceso a la consola local de su agente

La forma de acceder a la consola local depende del tipo de agente que esté utilizando.

Acceso a la consola local (VMware ESXiLinux KVM o Microsoft Hyper-V)

Por motivos de seguridad, no puede conectarse remotamente a la consola local de la máquina virtual (VM) del DataSync agente.

- Si es la primera vez que utiliza la consola local, inicie sesión en la máquina virtual con las credenciales predeterminadas. El nombre de usuario y la contraseña predeterminados son **admin** y **password**, respectivamente.

Note

Le recomendamos que cambie la contraseña predeterminada. Para ello, introduzca **5** (o **6** para VMware VMs) en el menú principal de la consola y ejecute el `passwd` comando para cambiar la contraseña.

Acceso a la consola local (Amazon EC2)

Para conectarte a la consola local de un EC2 agente de Amazon, debes usar SSH.

Antes de empezar: asegúrate de que el grupo de seguridad de la EC2 instancia permita el acceso mediante SSH (puerto TCP 22).

1. Abra un terminal y copie el siguiente comando `ssh`:

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

- Para */path/key-pair-name* ello, especifique la ruta y el nombre de archivo (`.pem`) de la clave privada necesaria para conectarse a la instancia.
 - En *instance-user-name*, especifique `admin`.
 - Para *instance-public-ip-address*, especifica la dirección IP pública de la instancia.
2. Ejecute el comando `ssh` para conectarse a la instancia.

Una vez conectado, se muestra el menú principal de la consola local del agente.

Configuración de los ajustes de DHCP y DNS de su agente

La configuración de red predeterminada del agente es DHCP (Dynamic Host Configuration Protocol). Con DHCP, al agente se le asigna automáticamente una dirección IP. En algunos casos, es posible que tenga que asignar manualmente la IP del agente como una dirección IP estática, como se describe a continuación.

1. Inicie sesión en la consola local del agente.
2. En el menú principal AWS DataSync Activación y configuración, introduzca **1** para empezar a configurar la red.
3. Elija una de las siguientes opciones en el menú Network Configuration (Configuración de red).

Para	Haga lo siguiente
Obtener información sobre el adaptador de red	Escriba 1. Aparecerá una lista de nombres de adaptador y se le pedirá que introduzca el nombre de un adaptador, por ejemplo, eth0. Si el adaptador que especifique está en uso, se mostrará la siguiente información acerca del adaptador: • Dirección MAC (Media Access Control) • Dirección IP • Máscara de red • Dirección IP del agente • Estado de habilitación de DHCP Puede utilizar el mismo nombre de adaptador cuando configure una dirección IP estática

Para	Haga lo siguiente
	(opción 3) que cuando configure el adaptador de ruta predeterminada del agente (opción 5).
Configuración de DHCP	Escriba 2. Se le pedirá que configure la interfaz de red para utilizar DHCP.
Configurar una dirección IP estática para el agente	Escriba 3. Se le solicita que introduzca el nombre del adaptador de red.  Important Si su agente ya se ha activado, debe apagarlo y reiniciarlo desde la DataSync consola para que los ajustes surtan efecto.

Para	Haga lo siguiente
Restablecer toda la configuración de red del agente a DHCP	Escriba 4. Todas las interfaces de red se configuran para utilizar DHCP.  Important Si su agente ya se ha activado, debe apagarlo y reiniciarlo desde la DataSync consola para que la configuración surta efecto.
Establecer el adaptador de ruta predeterminada del agente	Escriba 5. Se mostrarán los adaptadores disponibles para su agente y se le pedirá que seleccione uno de los adaptadores, por ejemplo, eth0.
Edite la configuración del sistema de nombres de dominio (DNS) de su agente	Escriba 6. Se muestran los adaptadores disponibles de los servidores DNS primario y secundario. Se le pedirá que proporcione la dirección IP nueva.

Para	Haga lo siguiente
Ver la configuración de DNS del agente	Escriba 7. Se muestran los adaptadores disponibles de los servidores DNS primario y secundario.  Note En algunas versiones del VMware hipervisor, puede editar la configuración del adaptador en este menú.
Ver tablas de ruteo	Escriba 8. Se muestra la ruta predeterminada del agente.

Comprobación de los recursos del sistema de su agente

Al iniciar sesión en la consola del agente, se comprueban automáticamente los núcleos de la CPU virtual, el tamaño del volumen raíz y la RAM. Si hay algún error o advertencia, aparece marcado en la pantalla del menú de la consola con un banner que proporciona información detallada sobre dichos errores o advertencias.

Si no hay errores ni advertencias cuando se inicia la consola, el menú muestra texto de color blanco. La opción Ver comprobación de recursos del sistema mostrará (0 Errors).

Si hay errores o advertencias, el menú de la consola muestra el número de errores y advertencias, en rojo y amarillo respectivamente, en un banner situado en la parte superior del menú. Por ejemplo, (1 ERROR, 1 WARNING).

Cómo comprobar los recursos del sistema de su agente

1. Inicie sesión en la consola local del agente.

2. En el menú principal AWS DataSync Activación - Configuración, introduzca **4** para ver los resultados de la comprobación de los recursos del sistema.

La consola muestra un mensaje [OK], [WARNING] o [FAIL] para cada recurso, como se describe en la tabla siguiente.

En el caso de EC2 las instancias de Amazon, la comprobación de los recursos del sistema verifica que el tipo de instancia sea una de las instancias con DataSync las que se recomienda su uso. Si el tipo de instancia coincide con esa lista, se muestra un único resultado en texto de color verde de la siguiente manera.

[OK] Instance Type Check

Si la EC2 instancia de Amazon no está en la lista recomendada, la comprobación de recursos del sistema verifica los siguientes recursos.

- Comprobación de los núcleos de la CPU: se necesitan al menos cuatro núcleos.
- Comprobación del tamaño del disco: se requiere un mínimo de 80 GB de espacio disponible en disco.
- Comprobación de la RAM:
 - 32 GB de RAM asignados a la instancia para ejecutar tareas con hasta 20 millones de archivos, objetos o directorios.
 - 64 GB de RAM asignados a la instancia para ejecutar tareas con más de 20 millones de archivos, objetos o directorios.
- Comprobación de los indicadores de CPU: la CPU de la máquina virtual del agente debe tener uno de los indicadores SSSE3 o un conjunto de SSE4 instrucciones.

Si la EC2 instancia de Amazon no está en la lista de instancias recomendadas DataSync, pero tiene recursos suficientes, el resultado de la comprobación de los recursos del sistema mostrará cuatro resultados, todos en texto verde.

Se verifican los mismos recursos para los agentes implementados en Hyper-V, la máquina virtual basada en el núcleo de Linux (KVM) y. VMware VMs

VMware También se comprueba la versión compatible de los agentes; las versiones no compatibles provocan un error de alerta. Las versiones compatibles incluyen VMware las versiones 6.5 y 6.7.

Sincronizar la hora de su agente VMware

Si utiliza un [VMware agente](#), puede ver o editar la configuración del servidor del Protocolo de tiempo de red (NTP) y sincronizar la hora del agente con el host del hipervisor. VMware

1. Inicie sesión en la [consola local del agente](#).
2. En el menú principal AWS DataSync Activación - Configuración, introduzca. **5**
3. En el menú System Time Management (Administración de la hora del sistema), elija una de las siguientes opciones:

Para	Haga lo siguiente
Visualización y sincronización de la hora de la máquina virtual con la hora del servidor NTP	Escriba 1. Se muestra la hora actual del agente. El agente determina la diferencia horaria entre su agente y el servidor NTP y le pide que sincronice las horas. En algunas situaciones, es posible que el tiempo de un agente se quede corto. Por ejemplo, es posible que se produzca una interrupción prolongada de la red y que el host y el agente del hipervisor no reciban actualizaciones horarias, por lo que la hora del agente es diferente a la hora real. Cuando hay una desviación de hora como esta, se produce una discrepancia entre las horas declaradas cuando se producen operaciones (tales como las instantáneas) y las horas reales a las que se producen las operaciones.
Editar la configuración del servidor NTP	Escriba 2. Se le solicitará que proporcione una configuración de servidor NTP.

Para	Haga lo siguiente
Ver la configuración del servidor NTP	Escriba 3. Se mostrará la configuración del servidor NTP.

Ejecutar comandos relacionados con el mantenimiento para su agente

En la consola local de su DataSync agente, puede realizar algunas tareas de mantenimiento y diagnosticar problemas con su agente.

Cómo ejecutar un comando de configuración o diagnóstico en la consola local del agente

1. Inicie sesión en la [consola local del agente](#).
2. En el menú principal AWS DataSync Activación y configuración, introduzca **5** (o para **6** una VMware máquina virtual) en la línea de comandos.
3. Utilice los siguientes comandos para llevar a cabo las siguientes tareas con su agente.

Comando	Descripción
dig	Buscar información de DNS sobre el host.
diskclean	Efectuar una limpieza de disco.
exit	Volver al menú de configuración de la consola.
h	Mostrar una lista de los comandos disponibles.
ifconfig	Mostrar o configura las interfaces de red.
ip	Mostrar o configurar el enrutamiento, los dispositivos y los túneles.
iptables	Configure y mantenga el filtrado IPv4 de paquetes y la traducción de direcciones de red (NAT).

Comando	Descripción
ncport	Probar la conectividad a un puerto TCP de red específico.
nping	Utilizar información para solucionar problemas de red.
save-iptables	Guardar las reglas de firewall de la tabla IP de forma permanente.
save-routing-table	Guardar una entrada de la tabla de enrutamiento recién agregada.
sslcheck	Comprobar si un certificado SSL es válido.
tcptraceroute	Recopilar la salida traceroute del tráfico TCP a un destino.

- Seguir instrucciones en pantalla.

Sustituir a su AWS DataSync agente

Para sustituir a un AWS DataSync agente, debe crear uno nuevo y actualizar las ubicaciones de transferencia que utilicen el agente anterior.

Creación de un agente nuevo

Para crear un DataSync agente nuevo, sigue el mismo proceso que cuando creaste el agente anterior:

- [Implemente un agente](#) en su entorno de almacenamiento.
- [Elija un punto final de servicio](#) con el que el agente se comunique AWS.
- [Configure la red](#) para que el agente pueda comunicarse con el almacenamiento y AWS.
- [Activación del agente](#).
- Una vez activado, anote el nombre de recurso de Amazon (ARN) del agente.

Necesitas este ARN al actualizar tu DataSync ubicación para usar el nuevo agente.

Actualización de su ubicación con el nuevo agente

Una vez que hayas creado un nuevo agente, puedes actualizar una DataSync ubicación existente para usar este agente. En la mayoría de los casos, también tendrá que volver a introducir las credenciales de acceso para actualizar la ubicación. Esto se debe a que DataSync almacena las credenciales de ubicación de forma que solo su agente pueda usarlas.

Uso de la DataSync consola

Las siguientes instrucciones describen cómo actualizar las ubicaciones con un agente nuevo mediante la DataSync consola.

NFS

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones.
3. Seleccione la versión que desea actualizar y, a continuación, elija Editar.
4. En Agentes, elija su nuevo agente.

Puede elegir más de un agente si va a sustituir a [varios agentes](#) para una ubicación.

5. Elija Guardar cambios.

SMB

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones.
3. Seleccione la versión que desea actualizar y, a continuación, elija Editar.
4. En Agentes, elija su nuevo agente.

Puede elegir más de un agente si va a sustituir a [varios agentes](#) para una ubicación.

5. En Contraseña, introduzca la contraseña del usuario que puede montar su servidor de archivos SMB y que tiene permiso para acceder a los archivos y carpetas involucrados en la transferencia.
6. Elija Guardar cambios.

HDFS

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones.
3. Seleccione la versión que desea actualizar y, a continuación, elija Editar.
4. En Agentes, elija su nuevo agente.

Puede elegir más de un agente si va a sustituir a [varios agentes](#) para una ubicación.

5. Si utiliza la autenticación Kerberos, cargue el archivo Keytab y el archivo de configuración de Kerberos.
6. Elija Guardar cambios.

Object storage

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones.
3. Seleccione la versión que desea actualizar y, a continuación, elija Editar.
4. En Agentes, elija su nuevo agente.

Puede elegir más de un agente si va a sustituir a [varios agentes](#) para una ubicación.

5. Si su ubicación requiere credenciales, introduzca la clave secreta que le permite acceder DataSync a su depósito de almacenamiento de objetos.
6. Elija Guardar cambios.

Azure Blob Storage

Haga lo siguiente para actualizar su Microsoft Azure Blob Storage ubicación:

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones.
3. Seleccione la versión que desea actualizar y, a continuación, elija Editar.
4. En Agentes, elija su nuevo agente.

Puede elegir más de un agente si va a sustituir a [varios agentes](#) para una ubicación.

5. En el caso del token SAS, introduzca el [token de firma de acceso compartido \(SAS\)](#) que permite acceder DataSync a su almacenamiento de blobs.
6. Elija Guardar cambios.

Usando el AWS CLI

En las siguientes instrucciones se describe cómo actualizar las ubicaciones con un agente nuevo mediante la AWS CLI. (También puede hacerlo mediante la [DataSync API](#)).

NFS

1. Copie el siguiente 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 el parámetro `--location-arn`, especifique el ARN de la ubicación de NFS que va a actualizar.
3. Para la opción `--on-prem-config` del parámetro `AgentArns`, especifique el ARN de su nuevo agente.

Puede elegir más de un ARN si va a sustituir a [varios agentes](#) para una ubicación.

4. Ejecute el comando `update-location-nfs` para actualizar la ubicación.

SMB

1. Copie el siguiente 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 el parámetro `--location-arn`, especifique el ARN de la ubicación de SMB que va a actualizar.
3. Para la opción `--agent-arns` del parámetro, especifique el ARN de su nuevo agente.

Puede elegir más de un ARN si va a sustituir a [varios agentes](#) para una ubicación.

4. Para el parámetro `--password`, especifique la contraseña del usuario que puede montar el servidor de archivos SMB y que tiene permiso para acceder a los archivos y carpetas involucrados en la transferencia.
5. Ejecute el comando `update-location-smb` para actualizar la ubicación.

HDFS

1. Copie el siguiente 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 el parámetro `--location-arn`, especifique el ARN de la ubicación de HDFS que va a actualizar.
3. Para la opción `--agent-arns` del parámetro, especifique el ARN de su nuevo agente.

Puede elegir más de un ARN si va a sustituir a [varios agentes](#) para una ubicación.

4. Si utiliza la autenticación Kerberos, incluya los parámetros `--kerberos-keytab` y `--kerberos-krb5-conf`:
 - Para el parámetro `--kerberos-keytab`, especifique la tabla de claves de Kerberos (keytab) que contiene asignaciones entre la entidad principal Kerberos definida y las claves cifradas.

Puede especificar el archivo keytab proporcionando la dirección del archivo.

- Para el parámetro `--kerberos-krb5-conf`, especifique el archivo que contiene la configuración de su dominio Kerberos.

Puede especificar el archivo `krb5.conf` proporcionando la dirección del archivo.

Si utiliza una autenticación simple, no es necesario incluir estos parámetros relacionados con Kerberos en el comando.

5. Ejecute el comando `update-location-hdfs` para actualizar la ubicación.

Object storage

1. Copie el siguiente 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 el parámetro `--location-arn`, especifique el ARN la ubicación de almacenamiento del objeto que va a actualizar.
3. Para la opción `--agent-arns` del parámetro, especifique el ARN de su nuevo agente.

Puede elegir más de un ARN si va a sustituir a [varios agentes](#) para una ubicación.

4. Haga lo siguiente en función de si la ubicación de almacenamiento de objetos requiere credenciales de acceso:
 - Si su ubicación requiere credenciales: para el `--secret-key` parámetro, especifique la clave secreta que permite acceder DataSync a su depósito de almacenamiento de objetos.
 - Si su ubicación requiere credenciales: especifique cadenas vacías para los parámetros `--access-key` y `--secret-key`. A continuación, se muestra un ejemplo 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. Ejecute el comando `update-location-object-storage` para actualizar la ubicación.

Azure Blob Storage

1. Copie el siguiente 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 el `--location-arn` parámetro, especifique el ARN del Azure Blob Storage ubicación que está actualizando.
3. Para la opción `--agent-arns` del parámetro, especifique el ARN de su nuevo agente.

Puede elegir más de un ARN si va a sustituir a [varios agentes](#) para una ubicación.

4. Para la Token opción del `--sas-configuration` parámetro, especifique el [token SAS](#) que permite acceder DataSync a su almacenamiento de blobs.
5. Ejecute el comando `update-location-azure-blob` para actualizar la ubicación.

Pasos a seguir a continuación

1. [Elimine a su antiguo agente](#). Si tiene alguna DataSync tarea en ejecución con este agente, espere a que esas tareas finalicen antes de eliminarla.
2. Si necesita reemplazar los agentes en varias ubicaciones, repita los pasos anteriores.
3. Cuando haya terminado, podrá reanudar la [ejecución de sus tareas](#).

Note

Sustitución de agentes para tareas programadas: si sustituye un agente por una [tarea programada](#), debe iniciar esa tarea manualmente si el nuevo agente utiliza un tipo de [punto de conexión de servicio](#) diferente al del agente anterior. Si no ejecuta la tarea manualmente antes de su próxima ejecución programada, se producirá un error en la tarea.

Por ejemplo, si su agente anterior utilizaba un punto de conexión de servicio público, pero el nuevo agente usa un punto de conexión de VPC, inicie esa tarea manualmente mediante la consola o la operación `StartTaskExecution`. Después de eso, la tarea volverá a ejecutarse según lo programado.

AWS DataSync Recursos de filtrado

Puede filtrar sus AWS DataSync ubicaciones y tareas mediante las `ListLocations` operaciones de `ListTasks` API del AWS CLI. Por ejemplo, recupere una lista de sus tareas más recientes.

Parámetros de filtrado

Puede utilizar filtros de API para acotar la lista de recursos devueltos por `ListTasks` y `ListLocations`. Por ejemplo, para recuperar todas las ubicaciones de Amazon S3, puede utilizar `ListLocations` con el nombre del filtro `LocationType S3` y `Operator Equals`.

Para filtrar los resultados de la API, debe especificar un nombre, un operador y un valor de filtro.

- **Name:** el nombre del filtro que se está utilizando. Cada llamada a la API admite una lista de filtros que están disponibles para ella (por ejemplo, `LocationType` para `ListLocations`).
- **Values:** los valores por los que quiere filtrar. Por ejemplo, es posible que desee mostrar solo las ubicaciones de Amazon S3.
- **Operator:** el operador que se utiliza para comparar los valores de los filtros (por ejemplo, `Equals` o `Contains`).

En la siguiente tabla se muestran los operadores disponibles.

Operador	Tipos de clave
<code>Equals</code>	Cadena, número
<code>NotEquals</code>	Cadena, número
<code>LessThan</code>	Número
<code>LessThanOrEqualTo</code>	Número
<code>GreaterThan</code>	Número
<code>GreaterThanOrEqualTo</code>	Número
<code>In</code>	Cadena
<code>Contains</code>	Cadena
<code>NotContains</code>	Cadena
<code>BeginsWith</code>	Cadena

Filtrado por ubicación

ListLocations admite los siguientes nombres de filtro:

- **LocationType**: filtra según el tipo de ubicación:
 - SMB
 - NFS
 - HDFS
 - OBJECT_STORAGE
 - S3
 - OUTPOST_S3
 - FSX_WINDOWS
 - FSX_LUSTRE
 - FSX_OPENZFS_NFS
 - FSX_ONTAP_NFS
 - FSX_ONTAP_SMB
- **LocationUri**: filtra el identificador uniforme de recursos (URI) asignado a la ubicación, tal como lo devuelve la llamada a la API DescribeLocation* (por ejemplo, s3://*bucket-name/your-prefix* para las ubicaciones de Amazon S3).
- **CreationTime**: filtra según el momento en que se creó la ubicación. El formato de entrada es yyyy-MM-dd:mm:ss, en Hora Universal Coordinada (UTC).

En el siguiente AWS CLI ejemplo, se enumeran todas las ubicaciones de tipo Amazon S3 que tienen un URI de ubicación que comienza con la cadena "s3://amzn-s3-demo-bucket" y que se crearon el 15 de diciembre de 2019 a las 17:15:20 UTC o después.

```
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}]
```

Este comando devuelve un resultado similar al siguiente.

```
{  
  "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/"
}
]
```

Filtrado por etiquetas

ListTasks admite los siguientes nombres de filtro.

- **LocationId**: filtra las ubicaciones de origen y destino en los valores del nombre de recurso de Amazon (ARN).
- **CreationTime**: filtra según el momento en que se creó la ubicación. El formato de entrada es yyyy-MM-dd:mm:ss en UTC.

En el siguiente AWS CLI ejemplo, se muestra la sintaxis al filtrar. LocationId

```
aws datasync list-tasks \
  --filters Name=LocationId,Values=arn:aws:datasync:us-east-1:your-account-id:location/your-location-id,Operator=Contains
```

El resultado de este comando debería ser similar a lo siguiente.

```
{
  "Tasks": [
    {
      "TaskArn": "arn:aws:datasync:us-east-1:your-account-id:task/your-task-id",
      "Status": "AVAILABLE",
      "Name": "amzn-s3-demo-bucket"
    }
  ]
}
```

Limpiar tus AWS DataSync recursos

Si los usaste AWS DataSync para una prueba o no necesitas los AWS recursos que creaste, elimínalos para que no se te cobre por los recursos que no planeas usar.

Note

Si tienes DataSync recursos en una [región opcional](#) que inhabilitas, esos recursos no se eliminarán automáticamente. Los recursos seguirán ahí si vuelves a activar esa región.

Eliminar un agente DataSync

Al eliminar un agente de AWS DataSync, el recurso de agente deja de estar asociado al tuyo Cuenta de AWS y no se puede deshacer.

Tenga en cuenta que al eliminar un agente de su entorno de almacenamiento DataSync no se elimina su máquina virtual (VM) ni su EC2 instancia de Amazon. Puede eliminar la máquina virtual o la instancia, o reutilizarla para activar un agente nuevo.

Requisitos previos

No elimines un agente hasta que actualices o elimines los DataSync recursos que dependen de él. Si va a sustituir a un agente, [actualice las ubicaciones de transferencia](#) con el nuevo agente. Si no va a sustituir a un agente, elimine primero las [tareas](#) y [ubicaciones](#) de transferencia que usa ese agente.

Eliminación del agente

1. Abre la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, elija Agentes.
3. Elija el agente que desea eliminar.
4. Elija Eliminar, escriba **delete** en el cuadro de texto que aparece y seleccione Eliminar.
5. Si no planea [reutilizar la infraestructura del agente](#) para otras DataSync actividades, elimine la EC2 instancia de Amazon o la máquina virtual del agente para eliminarla de su entorno de almacenamiento.

Reutilizar la infraestructura de un DataSync agente

Puede eliminar un recurso de agente de la EC2 instancia de Amazon o VM subyacente del agente DataSync y seguir utilizándola para activar un agente nuevo.

Cómo reutilizar la infraestructura de un agente

1. [Pruebe la conexión del agente a AWS](#). Si las pruebas de red pasan, vaya al paso siguiente.

Las pruebas de red deben pasar antes de continuar con el siguiente paso.

2. [Elimine el recurso del agente](#) de la EC2 instancia de Amazon o VM del agente, DataSync pero no la elimine.
3. Repita el paso 1 para AWS volver a probar la conexión del agente. Si las pruebas de red pasan, vaya al paso siguiente.
4. Unos tres minutos después de eliminar el recurso del agente DataSync, compruebe si el puerto 80 está abierto en la máquina virtual del agente o en la EC2 instancia de Amazon. Si es así, vaya al siguiente paso.
5. [Active un agente nuevo](#) con la EC2 instancia de Amazon o VM existente.

Puede activar el nuevo agente en un punto de servicio diferente Región de AWS y con otro tipo de [punto final de servicio](#). Cuenta de AWS [Si utiliza un tipo de punto de conexión de servicio diferente, debe ajustar la configuración de la red](#).

Eliminar una DataSync ubicación

Como práctica recomendada, elimine las AWS DataSync ubicaciones que ya no necesite.

Para eliminar una ubicación mediante la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones.
3. Seleccione la ubicación que desea eliminar.
4. Elija Delete (Eliminar). Ingrese **delete** para confirmar la eliminación y luego, elija Eliminar.

Eliminar una DataSync tarea

Si ya no necesita una AWS DataSync tarea, puede eliminarla y sus AWS recursos relacionados.

Requisitos previos

Al ejecutar una tarea, crea y administra DataSync automáticamente las [interfaces de red](#) para el tráfico de transferencia de datos. Cuando elimina una tarea, también elimina las interfaces de red relacionadas con esta, siempre que tenga los siguientes permisos:

- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`

Estos permisos están disponibles en la política AWS gestionada `AWSDataSyncFullAccess`. Para obtener más información, consulte [AWS políticas gestionadas para AWS DataSync](#).

Eliminación de la tarea

Cuando elimine una tarea, esta no se podrá restaurar.

Uso de la DataSync consola

1. Abra la AWS DataSync consola en <https://console.aws.amazon.com/datasync/>.
2. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Tareas.
3. Seleccione la tarea que quiere eliminar.
4. Seleccione Actions (Acciones) y, a continuación, seleccione Delete (Eliminar).
5. En el cuadro de diálogo (Confirmación), elija Delete (Eliminar).

Usando el AWS CLI

1. Copie el siguiente comando `delete-task`:

```
aws datasync delete-task \  
    --task-arn "task-to-delete"
```

2. Para el parámetro `--task-arn`, especifique el nombre de recurso de Amazon (ARN) de la tarea que está eliminando (por ejemplo, `arn:aws:datasync:us-east-2:123456789012:task/task-012345678abcd0123`).
3. Ejecute el comando `delete-task`.

Seguridad en AWS DataSync

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los [programas de conformidad de AWS](#). Para obtener más información acerca de los programas de conformidad que se aplican a AWS DataSync, consulte [Servicios de AWS en el ámbito del programa de conformidad](#).
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos vigentes.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza DataSync. Los siguientes temas muestran cómo configurarlo DataSync para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus DataSync recursos.

Temas

- [Protección de datos en AWS DataSync](#)
- [Gestión de identidad y acceso en AWS DataSync](#)
- [Validación de conformidad para AWS DataSync](#)
- [Resiliencia en AWS DataSync](#)
- [Seguridad de infraestructura en AWS DataSync](#)
- [Proteger las credenciales de ubicación de almacenamiento](#)

Protección de datos en AWS DataSync

AWS DataSync transfiere datos de forma segura entre sistemas de almacenamiento autogestionados y servicios AWS de almacenamiento y también entre servicios AWS de almacenamiento. La forma en que se cifran los datos de almacenamiento en tránsito depende en parte de las ubicaciones implicadas en la transferencia.

Una vez completada la transferencia, los datos en reposo son cifrados por el sistema o el servicio que los almacena (no DataSync).

Temas

- [AWS DataSync cifrado en tránsito](#)
- [AWS DataSync cifrado en reposo](#)
- [Privacidad del tráfico entre redes](#)

AWS DataSync cifrado en tránsito

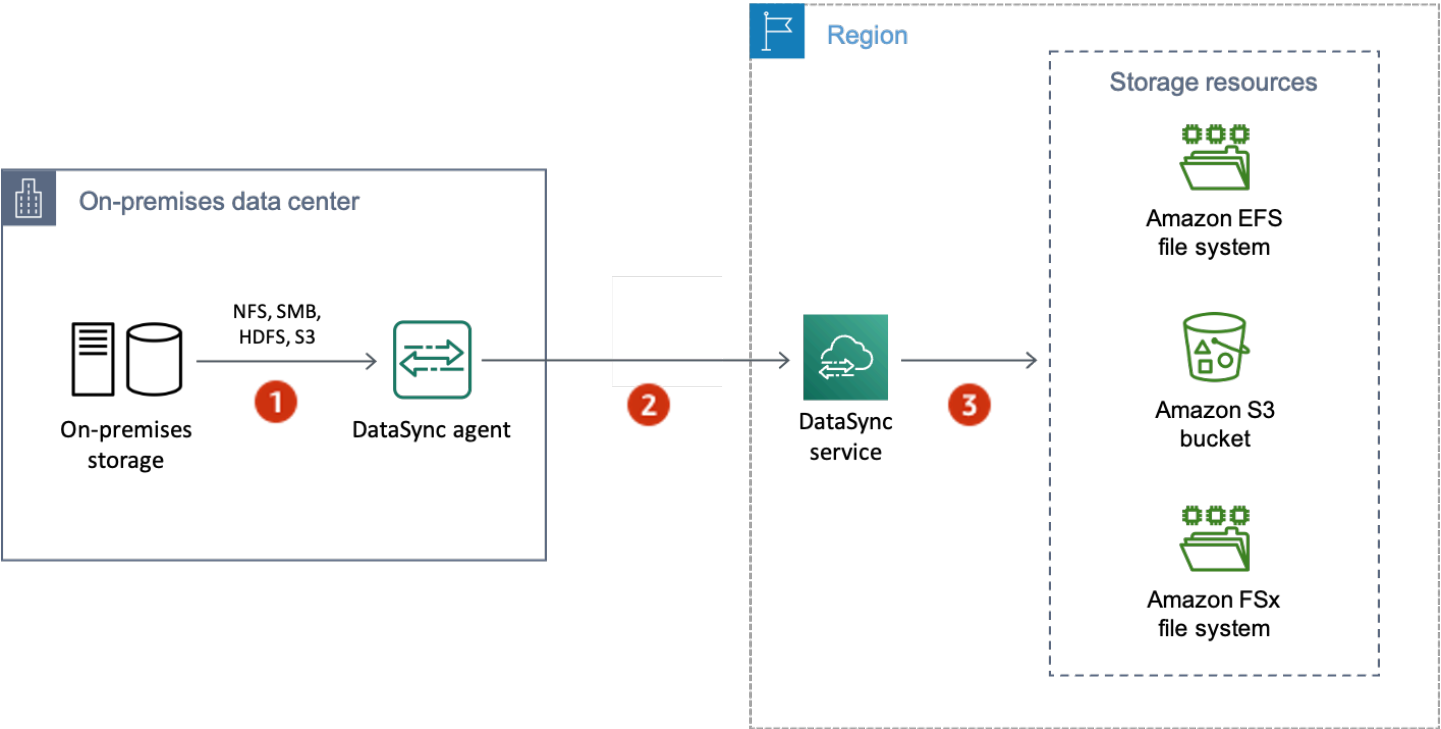
Los datos de almacenamiento (incluidos los metadatos) se cifran en tránsito, pero la forma en que se cifran durante la transferencia depende de las ubicaciones de origen y destino.

Al conectarse con una ubicación, DataSync utiliza las opciones más seguras que ofrece el protocolo de acceso a los datos de esa ubicación. Por ejemplo, cuando se conecta a un sistema de archivos mediante el bloque de mensajes del servidor (SMB), DataSync utiliza las funciones de seguridad que proporciona SMB.

Conexiones de red en una transferencia

DataSync requiere tres conexiones de red para copiar datos: una conexión para leer datos desde una ubicación de origen, otra para transferir datos entre ubicaciones y una más para escribir datos en una ubicación de destino.

El siguiente diagrama es un ejemplo de las conexiones de red que se DataSync utilizan para transferir datos desde un sistema de almacenamiento local a un servicio AWS de almacenamiento. Para entender dónde se producen las conexiones y cómo se protegen los datos a medida que se transfieren por cada conexión, consulte la tabla adjunta.



Referencia	Conexiones de red	Descripción
1	Lectura de datos de la ubicación de origen	DataSync se conecta mediante el protocolo del sistema de almacenamiento para acceder a los datos (por ejemplo, SMB o la API de Amazon S3). Para esta conexión, los datos se protegen mediante las funciones de seguridad del sistema de almacenamiento, a menos que DataSync no las admita. Por ejemplo, DataSync actualmente no admite la autenticación Kerberos con servidores de archivos NFS ni cuando se utiliza el cifrado TDE con HDFS.
2	Transferencia de datos entre ubicaciones	Para esta conexión, DataSync cifra todo el tráfico de la red con una seguridad de capa de transporte mutua (mTLS) 1.3.

Referencia	Conexiones de red	Descripción
3	Escritura de datos en la ubicación de destino	Al igual que con la ubicación de origen, DataSync se conecta mediante el protocolo del sistema de almacenamiento para acceder a los datos. Los datos vuelven a protegerse mediante las funciones de seguridad del sistema de almacenamiento, a menos que DataSync no las admita.

Descubra cómo se cifran sus datos en tránsito cuando se DataSync conecta a los siguientes servicios AWS de almacenamiento:

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

Cifrados TLS

Al transferir datos entre ubicaciones, DataSync utiliza diferentes cifrados TLS. El cifrado TLS depende del tipo de punto final del servicio con el que se comunique el agente. DataSync (Para obtener más información, consulte [Elección de un punto de conexión de servicio para su agente de AWS DataSync](#)).

Contenido

- [Puntos de conexión de VPC o públicos](#)
- [Puntos de conexión de FIPS](#)

Puntos de conexión de VPC o públicos

Para los puntos finales del servicio de nube privada virtual (VPC) y pública, DataSync utiliza uno de los siguientes cifrados TLS:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_ (ecd_h_x25519) SHA384
- TLS_ECDHE_RSA_CON_0_05_ (ECDH_x25519CHACHA2) POLY13 SHA256
- TLS_ECDHE_RSA_CON_AES_128_GCM_ (ecd_h_x25519SHA256)

Puntos de conexión de FIPS

Para los puntos finales del servicio del Estándar Federal de Procesamiento de Información (FIPS), utiliza el siguiente cifrado TLS: DataSync

- TLS_AES_128_GCM_ (secp256r1) SHA256

AWS DataSync cifrado en reposo

Como AWS DataSync es un servicio de transferencia, por lo general no administra los datos almacenados en reposo. Los servicios y sistemas de almacenamiento DataSync compatibles son responsables de proteger los datos en ese estado. Sin embargo, hay algunos datos relacionados con el servicio que se DataSync administran en reposo.

¿Qué se cifra?

Los únicos datos que se DataSync gestionan en reposo se refieren a los detalles que se necesitan para completar la transferencia. DataSync almacena los siguientes datos con cifrado completo en reposo en Amazon DynamoDB:

- Configuraciones de tareas (por ejemplo, detalles sobre las ubicaciones de la transferencia).
- Credenciales de usuario que permiten a su DataSync agente autenticarse con una ubicación. Estas credenciales se cifran mediante las claves públicas de su agente. El agente puede descifrar estas claves según sea necesario con sus claves privadas.

Para obtener más información, consulte [DynamoDB encryption](#) en la Guía para desarrolladores de Amazon DynamoDB.

Administración de claves

No puede administrar las claves de cifrado que se DataSync utilizan para almacenar información en DynamoDB relacionada con la ejecución de la tarea. Esta información incluye las configuraciones de las tareas y las credenciales que los agentes utilizan para autenticarse en una ubicación de almacenamiento.

¿Qué no está cifrado?

Aunque DataSync no controla la forma en que se cifran los datos de almacenamiento en reposo, le recomendamos configurar las ubicaciones con el nivel de seguridad más alto que admitan. Por ejemplo, puede cifrar objetos con claves de cifrado administradas por Amazon S3 (SSE-S3) o claves (KMS) AWS Key Management Service (AWS SSE-KMS).

Obtenga más información sobre cómo los servicios de AWS almacenamiento cifran los datos en reposo:

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

Privacidad del tráfico entre redes

Recomendamos configurar las ubicaciones de origen y destino con el nivel de seguridad más alto que admita cada una de ellas. Al conectarse a una ubicación, AWS DataSync funciona con la versión más segura del protocolo de acceso a datos que utiliza el sistema de almacenamiento. Además, valore limitar el tráfico de subred a los protocolos y servicios conocidos.

DataSync asegura la conexión entre las ubicaciones, incluso entre Cuentas de AWS, y las zonas de disponibilidad Regiones de AWS, mediante el uso de Transport Layer Security (TLS) 1.3.

Gestión de identidad y acceso en AWS DataSync

AWS utiliza credenciales de seguridad para identificarlo y concederle acceso a sus AWS recursos. Puede utilizar las funciones de AWS Identity and Access Management (IAM) para permitir que

otros usuarios, servicios y aplicaciones utilicen sus AWS recursos de forma completa o limitada, sin compartir sus credenciales de seguridad.

De forma predeterminada, las identidades de IAM (usuarios, grupos y roles) no tienen permiso para crear, ver o modificar AWS recursos. Para permitir que los usuarios, grupos y roles accedan a AWS DataSync los recursos e interactúen con la DataSync consola y la API, te recomendamos que utilices una política de IAM que les conceda permiso para usar los recursos y las acciones de API específicos que necesiten. A continuación, adjunte la política a la identidad de IAM que requiere el acceso. Para obtener información general de los elementos básicos de una política, consulte [Administración de acceso para AWS DataSync](#).

Temas

- [Administración de acceso para AWS DataSync](#)
- [AWS políticas gestionadas para AWS DataSync](#)
- [Políticas administradas por el cliente para AWS DataSync](#)
- [Cómo utilizar roles vinculados a servicios de DataSync](#)
- [Permisos para etiquetar DataSync los recursos durante la creación](#)
- [Prevención de la sustitución confusa entre servicios](#)

Administración de acceso para AWS DataSync

Cada AWS recurso es propiedad de un Cuenta de AWS. Los permisos de creación o acceso a un recurso se rigen por políticas de permisos. Un administrador de cuentas puede adjuntar políticas de permisos a las identidades AWS Identity and Access Management (IAM). Algunos servicios (por ejemplo AWS Lambda) también permiten adjuntar políticas de permisos a los recursos.

Note

Un administrador de la cuenta es un usuario con privilegios en una Cuenta de AWS. Para obtener más información, consulte [Prácticas recomendadas de IAM](#) en la Guía del usuario de IAM.

Temas

- [DataSync recursos y operaciones](#)

- [Titularidad de los recursos](#)
- [Administración del acceso a los recursos](#)
- [Especificación de elementos de política: acciones, efectos, recursos y entidades principales](#)
- [Especificación de las condiciones de una política](#)

DataSync recursos y operaciones

En DataSync, los recursos principales son el agente, la ubicación, la tarea y la ejecución de la tarea.

Estos recursos tienen nombres de recursos de Amazon (ARNs) exclusivos asociados a ellos, como se muestra en la siguiente tabla.

Tipo de recurso	Formato de ARN
ARN del agente	<code>arn:aws:datasync: <i>region</i>:<i>account-id</i> :agent/<i>agent-id</i></code>
ARN de ubicación	<code>arn:aws:datasync: <i>region</i>:<i>account-id</i> :location/ <i>location-id</i></code>
ARN de tarea	<code>arn:aws:datasync: <i>region</i>:<i>account-id</i> :task/<i>task-id</i></code>
ARN de ejecución de tarea	<code>arn:aws:datasync: <i>region</i>:<i>account-id</i> :task/<i>task-id</i>/executio n/ <i>exec-id</i></code>

Para conceder permisos para operaciones de API específicas, como la creación de una tarea, DataSync define un conjunto de acciones que puede especificar en una política de permisos. Una operación de la API puede requerir permisos para más de una acción.

Titularidad de los recursos

El propietario del recurso es el Cuenta de AWS que creó el recurso. Es decir, el propietario del recurso es el Cuenta de AWS de la entidad principal (por ejemplo, un rol de IAM) que autentica la solicitud que crea el recurso. Los siguientes ejemplos ilustran cómo funciona:

- Si utilizas las credenciales de tu cuenta raíz Cuenta de AWS para crear una tarea, eres el propietario del recurso (en DataSync, el recurso es la tarea). Cuenta de AWS
- Si crea una función de IAM en su cuenta Cuenta de AWS y concede permisos para la `CreateTask` acción a ese usuario, el usuario puede crear una tarea. Sin embargo, la propietaria del recurso de tarea será su Cuenta de AWS, a la que pertenece el usuario.
- Si crea un rol de IAM Cuenta de AWS con permisos para crear una tarea, cualquier persona que pueda asumir el rol podrá crear una tarea. Usted Cuenta de AWS, al que pertenece el rol, es el propietario del recurso de la tarea.

Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

Note

En esta sección se analiza el uso de IAM en el contexto de DataSync. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte [What is IAM?](#) (¿Qué es IAM?) en la Guía del usuario de IAM. Para obtener más información acerca de la sintaxis y las descripciones de la política de IAM, consulte [Referencia de políticas AWS Identity and Access Management](#) en la Guía del usuario de IAM.

Las políticas asociadas a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM) y las políticas asociadas a un recurso se denominan políticas basadas en recursos. DataSync solo admite políticas basadas en la identidad (políticas de IAM).

Temas

- [Políticas basadas en identidad](#)
- [Políticas basadas en recursos](#)

Políticas basadas en identidad

Puede gestionar el acceso a los DataSync recursos con las políticas de IAM. Estas políticas pueden ayudar a un Cuenta de AWS administrador a hacer lo siguiente: DataSync

- Otorgue permisos para crear y administrar DataSync recursos: cree una política de IAM que permita Cuenta de AWS a un rol de IAM crear y administrar DataSync recursos, como agentes, ubicaciones y tareas.
- Otorgue permisos a un rol en otro Cuenta de AWS o en uno Servicio de AWS: cree una política de IAM que conceda permisos a un rol de IAM en otro rol o en uno diferente. Cuenta de AWS Servicio de AWS Por ejemplo:
 1. El administrador de la Cuenta A crea un rol de IAM y adjunta una política de permisos al rol que concede permisos sobre los recursos de la Cuenta A.
 2. El administrador de la cuenta A asocia una política de confianza al rol que identifica la cuenta B como la entidad principal que puede asumir el rol.

Para conceder un Servicio de AWS permiso para asumir el rol, el administrador de la cuenta A puede especificar una Servicio de AWS como principal en la política de confianza.

3. El administrador de la cuenta B puede entonces delegar permisos para asumir el rol a usuarios de la cuenta B. Esto permite a los usuarios del rol de la cuenta B crear u obtener acceso a recursos de la cuenta A.

Para obtener más información sobre el uso de IAM para delegar permisos, consulte [Access management](#) (Administración de accesos) en la Guía del usuario de IAM.

A continuación, se muestra un ejemplo de política que concede permisos para todas las acciones List* en todos los recursos. Esta acción es de solo lectura y no permite modificar los recursos.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllListActionsOnAllResources",
      "Effect": "Allow",
      "Action": [
        "datasync:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

Para obtener más información sobre el uso de políticas basadas en la identidad con DataSync, consulte Políticas administradas y [Políticas AWS administradas](#) por el [cliente](#). Para obtener más información sobre identidades de IAM, consulte la [Guía del usuario de IAM](#).

Políticas basadas en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede adjuntar una política a un bucket de Amazon S3 para administrar los permisos de acceso a dicho bucket. Sin embargo, DataSync no admite políticas basadas en recursos.

Especificación de elementos de política: acciones, efectos, recursos y entidades principales

Para cada DataSync recurso, el servicio define un conjunto de operaciones de API (consulte [Acciones](#)). Para conceder permisos para estas operaciones de API, DataSync define un conjunto de acciones que puedes especificar en una política. Por ejemplo, para el DataSync recurso, se definen las siguientes acciones: `CreateTaskDeleteTask`, y `DescribeTask`. Para realizar una operación API pueden ser necesarios permisos para más de una acción.

A continuación se indican los elementos más básicos de la política:

- **Recurso:** en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para los recursos de DataSync, puede utilizar el carácter comodín (`*`) en políticas de IAM. Para obtener más información, consulte [DataSync recursos y operaciones](#).
- **Acción:** utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, según el `Effect` elemento especificado, el `datasync:CreateTask` permiso permite o deniega al usuario los permisos para realizar la DataSync `CreateTask` operación.
- **Efecto:** especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser `Allow` o `Deny`. Si no concede acceso de forma explícita a (`Allow`) un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso. Para obtener más información, consulte [Autorización](#) en la Guía del usuario de IAM.
- **Entidad principal:** en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. En el caso de las políticas basadas en

recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad para la que desea recibir los permisos (solo se aplica a las políticas basadas en recursos). DataSync no admite políticas basadas en recursos.

Para obtener más información acerca de la sintaxis y las descripciones de las políticas de IAM, consulte [Referencia de políticas de AWS Identity and Access Management IAM](#) en la Guía del usuario de IAM.

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de IAM para especificar las condiciones en las que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte [Condición](#) en la Guía del usuario de IAM.

Cómo expresar condiciones, se usan claves de condición predefinidas. No hay claves de condición específicas para DataSync. Sin embargo, hay claves AWS de condición amplias que puede utilizar según convenga. Para obtener una lista completa de las teclas AWS anchas, consulte [las claves disponibles](#) en la Guía del usuario de IAM.

AWS políticas gestionadas para AWS DataSync

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para [crear políticas administradas por el cliente de IAM](#) que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las [políticas AWS administradas](#) en la Guía del usuario de IAM.

Servicios de AWS mantener y actualizar las políticas AWS gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política gestionada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no

eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos Servicios de AWS los recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte [Políticas administradas de AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

AWS política gestionada: `AWSDataSyncReadOnlyAccess`

Puede adjuntar la política `AWSDataSyncReadOnlyAccess` a las identidades de IAM.

Esta política otorga permisos de solo lectura 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 gestionada: AWSDDataSyncFullAccess

Puede adjuntar la política `AWSDDataSyncFullAccess` a las identidades de IAM.

Esta política otorga permisos administrativos DataSync y es necesaria para AWS Management Console acceder al servicio. `AWSDDataSyncFullAccess` proporciona acceso completo a las operaciones de la DataSync API y a las operaciones que interactúan con los recursos relacionados (como los buckets de Amazon S3, los sistemas de archivos de Amazon EFS, AWS KMS las claves y los secretos de Secrets Manager). La política también otorga permisos a Amazon CloudWatch, incluida la creación de grupos de registros y la creación o actualización de una 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 gestionada: AWSDataSyncServiceRolePolicy

No puede adjuntar la política `AWSDataSyncServiceRolePolicy` a las identidades de IAM. Esta política está asociada a un rol vinculado al servicio que permite DataSync realizar acciones en su nombre. Para obtener más información, consulte [Cómo utilizar roles vinculados a servicios de DataSync](#).

Esta política concede permisos administrativos que permiten al rol vinculado al servicio crear CloudWatch registros de Amazon para DataSync las tareas mediante el modo mejorado.

Actualizaciones de políticas

Cambio	Descripción	Fecha
AWSDataSyncFullAccess: cambio	DataSync declaraciones de permiso modificadas para: <code>AWSDataSyncFullAccess</code> Las declaraciones actualizadas eliminan las condiciones de etiquetado de los permisos que se DataSync utilizan para crear secretos de Secrets Manager.	13 de mayo de 2025
AWSDataSyncFullAccess: cambio	DataSync agregó nuevos permisos para <code>AWSDataSyncFullAccess</code> : • <code>secretsmanager:CreateSecret</code> • <code>secretsmanager:PutSecretValue</code> • <code>secretsmanager>DeleteSecret</code> • <code>secretsmanager:UpdateSecret</code>	7 de mayo de 2025

Cambio	Descripción	Fecha
	Estos permisos permiten DataSync crear, editar y eliminar AWS Secrets Manager secretos.	
AWSDataSyncFullAccess: cambio	DataSync agregó nuevos permisos paraAWSDataSy ncFullAccess : • secretsmanager:Lis tSecrets • kms:ListAliases • kms:DescribeKey Estos permisos permiten DataSync recuperar los metadatos sobre sus AWS Secrets Manager secretos y AWS KMS claves, incluidos los alias asociados a sus claves.	23 de abril de 2025

Cambio	Descripción	Fecha
AWSDataSyncServiceRolePolicy : cambio	DataSync agregó nuevos permisos a la <code>AWSDataSyncServiceRolePolicy</code> y política que usa el rol vinculado al DataSync servicio: <code>AWSServiceRoleForDataSync</code> • <code>secretsmanager:DescribeSecret</code> • <code>secretsmanager:GetSecretValue</code> Estos permisos permiten DataSync leer los metadatos y los valores de los secretos gestionados por. AWS Secrets Manager	15 de abril de 2025
AWSDataSyncServiceRolePolicy : política nueva	DataSync agregó una política que utiliza el rol DataSync vinculado al servicio. <code>AWSServiceRoleForDataSync</code> Esta nueva política gestionada crea automáticamente CloudWatch registros de Amazon para DataSync las tareas que utilizan el modo mejorado.	30 de octubre de 2024

Cambio	Descripción	Fecha
AWSDataSyncFullAccess: cambio	DataSync agregó un nuevo permiso paraAWSDataSy ncFullAccess : • iam:CreateServiceL inkedRole Este permiso le permite DataSync crear funciones vinculadas a un servicio para usted.	30 de octubre de 2024
AWSDataSyncFullAccess: cambio	DataSync agregó un nuevo permiso para: AWSDataSy ncFullAccess • ec2:DescribeRegions Este permiso te permite elegir regiones opcionales al crear una DataSync tarea para realizar transferencias entre Regiones de AWS ellas.	22 de julio de 2024
AWSDataSyncFullAccess: cambio	DataSync agregó un nuevo permiso paraAWSDataSy ncFullAccess : • s3:ListBucketVersi ons Este permiso te permite elegir una versión específica de tu DataSync manifiesto.	16 de febrero de 2024

Cambio	Descripción	Fecha
<u>AWSDataSyncFullAccess:</u> cambio	DataSync agregó nuevos permisos 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> Estos permisos le ayudan a crear DataSync agentes y ubicaciones para Amazon EFS, Amazon FSx for NetApp ONTAP, Amazon S3 y S3 en Outposts.	2 de mayo de 2023
DataSync comenzó a rastrear los cambios	DataSync comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	1 de marzo de 2021

Políticas administradas por el cliente para AWS DataSync

Además de las políticas AWS gestionadas, también puedes crear tus propias políticas basadas en la identidad AWS DataSync y adjuntarlas a las identidades AWS Identity and Access Management (de IAM) que requieren esos permisos. Las políticas administradas por el cliente son políticas independientes que usted administra en su propia Cuenta de AWS.

Important

Antes de empezar, le recomendamos que conozca los conceptos básicos y las opciones para administrar el acceso a sus recursos. DataSync Para obtener más información, consulte [Administración de acceso para AWS DataSync](#).

Al crear una política gestionada por el cliente, debe incluir declaraciones sobre DataSync las operaciones que se pueden utilizar en determinados AWS recursos. El siguiente ejemplo tiene dos instrucciones (fíjese en los elementos `Action` y en los elementos `Resource` de ambas):

```
{
  "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": "*"
    }
  ]
}
```

Las declaraciones de política hacen lo siguiente:

- La primera instrucción concede permisos para realizar la acción `datasync:DescribeTask` en determinados recursos de la tarea de transferencia especificando un nombre de recurso de Amazon (ARN) con un carácter comodín (*).
- La segunda instrucción concede permisos para realizar la acción `datasync:ListTasks` en todas las tareas especificando solo un carácter comodín (*).

Ejemplos de políticas administradas por los clientes

En el siguiente ejemplo, las políticas administradas por el cliente otorgan permisos para varias DataSync operaciones. Las políticas funcionan si utilizas el AWS Command Line Interface (AWS CLI) o un AWS SDK. Para usar estas políticas en la consola, también debe usar la política administrada `AWSDataSyncFullAccess`.

Temas

- [Ejemplo 1: Crear una relación de confianza que permita acceder DataSync a su bucket de Amazon S3](#)
- [Ejemplo 2: Permite DataSync leer y escribir en tu bucket de Amazon S3](#)
- [Ejemplo 3: Permitir DataSync cargar registros a grupos de CloudWatch registros](#)

Ejemplo 1: Crear una relación de confianza que permita acceder DataSync a su bucket de Amazon S3

El siguiente es un ejemplo de una política de confianza que permite DataSync asumir una función de IAM. Esta función permite acceder DataSync a un bucket de Amazon S3. Para evitar el [problema de los suplentes confusos entre servicios](#), recomendamos utilizar las claves de contexto de condición `aws:SourceAccount` y `aws:SourceArn` global en la 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:*"
            }
        }
    }
}

```

Ejemplo 2: Permite DataSync leer y escribir en tu bucket de Amazon S3

El siguiente ejemplo de política otorga DataSync los permisos mínimos para leer y escribir datos en un bucket de S3 que se utiliza como ubicación de destino.

Note

El valor de `aws:ResourceAccount` debe ser el ID de cuenta propietario del bucket de Amazon S3 especificado en la 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"
        }
      }
    }
  ]
}

```

Ejemplo 3: Permitir DataSync cargar registros a grupos de CloudWatch registros

DataSync requiere permisos para poder subir registros a tus grupos de CloudWatch registros de Amazon. Puede usar grupos de CloudWatch registros para monitorear y depurar sus tareas.

Para ver una política de IAM de ejemplo en la que se conceden dichos permisos, consulte [DataSync Permitir cargar registros a un grupo de CloudWatch registros](#).

Cómo utilizar roles vinculados a servicios de DataSync

AWS DataSync [usa roles vinculados al AWS Identity and Access Management servicio \(IAM\)](#). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. DataSync Los roles vinculados al servicio están predefinidos DataSync e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Temas

- [Uso de roles para DataSync](#)

Uso de roles para DataSync

AWS DataSync [usa roles vinculados al AWS Identity and Access Management servicio \(IAM\)](#). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. DataSync Los roles vinculados al servicio están predefinidos DataSync e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración DataSync , ya que no es necesario añadir manualmente los permisos necesarios. DataSync define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo DataSync puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus DataSync recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte los [AWS servicios que funcionan con IAM y busque los servicios con](#) la palabra Sí en la columna Funciones vinculadas a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados al servicio para DataSync

DataSync utiliza el rol vinculado al servicio denominado `AWSServiceRoleForDataSync`: permite realizar operaciones esenciales DataSync para transferir la ejecución de tareas, incluida la lectura de secretos de los eventos y grupos de registros y la creación de AWS Secrets Manager grupos de CloudWatch registros.

El rol `AWSService RoleForDataSync` vinculado al servicio confía en que los siguientes servicios asuman el rol:

- `datasync.amazonaws.com`

El rol vinculado al servicio usa la política AWS administrada denominada [AWSDataSyncServiceRolePolicy](#), que permite DataSync realizar las siguientes acciones en los 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}"
      }
    }
  }
]
```



```
]
}
```

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de DataSync

No necesita crear manualmente un rol vinculado a servicios. Al crear una DataSync tarea en la AWS Management Console, la o la AWS API AWS CLI, DataSync crea automáticamente la función vinculada al servicio.

En la API AWS CLI o en la AWS API, puede crear una función vinculada al servicio con el nombre del servicio. `datasync.amazonaws.com` Para obtener más información, consulte [Crear un rol vinculado a un servicio](#) en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear una DataSync tarea, vuelve a DataSync crear el rol vinculado al servicio para usted.

Si elimina este rol vinculado a servicios, puede utilizar el mismo proceso de IAM para volver a crear el rol.

Modificación de un rol vinculado a servicios de DataSync

DataSync no permite editar el rol vinculado al `AWSServiceRoleForDataSync` servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de DataSync

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol.

Note

Si el DataSync servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar DataSync los recursos utilizados por el AWSService RoleForDataSync

1. [Elimine los DataSync agentes](#) utilizados por la tarea (si los hay).
2. [Elimine las ubicaciones de la tarea.](#)
3. [Elimine la tarea.](#)

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSService RoleForDataSync servicio. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de DataSync

DataSync admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte [Puntos de conexión y Regiones de AWS](#).

Permisos para etiquetar DataSync los recursos durante la creación

Algunas acciones de la AWS DataSync API de creación de recursos te permiten especificar etiquetas al crear el recurso. Puede utilizar etiquetas de recursos para implementar el control de acceso basado en atributos (ABAC). Para obtener más información, consulta [¿Para qué sirve el ABAC? AWS](#) en la Guía del usuario de IAM.

Para permitir que los usuarios etiqueten los recursos durante su creación, es preciso que tengan permisos para utilizar la acción que crea el recurso (por ejemplo, `datasync:CreateAgent` o

`datasync:CreateTask`). Si se especifican etiquetas en la acción de creación de recursos, los usuarios también deben tener permisos explícitos para usar la acción `datasync:TagResource`.

La acción `datasync:TagResource` solo se evalúa si se aplican etiquetas durante la acción de creación de recursos. Por lo tanto, un usuario que tenga permisos para crear un recurso (suponiendo que no existan condiciones de etiquetado) no necesita permisos para utilizar la acción `datasync:TagResource` si no se especifica ninguna etiqueta en la solicitud.

Sin embargo, si el usuario intenta crear un recurso con etiquetas, la solicitud dará un error si el usuario no tiene permisos para utilizar la acción `datasync:TagResource`.

Ejemplo de instrucciones de política de IAM

Utilice el siguiente ejemplo de declaraciones de política de IAM para conceder `TagResource` permisos a los usuarios que creen DataSync recursos.

La siguiente declaración permite a los usuarios etiquetar a un DataSync agente cuando lo crean.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "datasync:TagResource",
      "Resource": "arn:aws:datasync:region:account-id:agent/*"
    }
  ]
}
```

La siguiente declaración permite a los usuarios etiquetar una DataSync ubicación cuando la crean.

JSON

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

```

        "Effect": "Allow",
        "Action": "datasync:TagResource",
        "Resource": "arn:aws:datasync:region:account-id:location/*"
    }
]
}

```

La siguiente declaración permite a los usuarios etiquetar una DataSync tarea al crearla.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "datasync:TagResource",
      "Resource": "arn:aws:datasync:region:account-id:task/*"
    }
  ]
}

```

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición [aws:SourceAccount](#) global [aws:SourceArn](#) las claves de contexto en las políticas de recursos para limitar los permisos que se AWS DataSync otorgan a otro servicio al recurso. Si utiliza claves de contexto de condición global y el valor de `aws:SourceArn` contiene el ID de cuenta, el valor de `aws:SourceAccount` y la

cuenta en el valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utiliza en la misma instrucción de política. Utiliza `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utilice `aws:SourceAccount` si quiere que cualquier recurso de esa cuenta se asocie al uso entre servicios.

El valor de `aws:SourceArn` debe incluir el ARN de DataSync ubicación con el que DataSync se puede asumir la función de IAM.

La forma más eficaz de protegerse contra el problema del suplente confuso es utilizar la clave de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo o si está especificando varios recursos, utilice los caracteres comodines (*) para las partes desconocidas. Estos son algunos ejemplos de cómo hacerlo para: DataSync

- Para limitar la política de confianza a una DataSync ubicación existente, incluya el ARN completo de la ubicación en la política. DataSync asumirá la función de IAM solo cuando se trate de esa ubicación en particular.
- Al crear una ubicación de Amazon S3 DataSync, no conoce el ARN de la ubicación. En estas situaciones, utilice el siguiente formato para la clave de `aws:SourceArn`: `arn:aws:datasync:us-east-2:123456789012:*`. Este formato valida la partición (aws), el identificador de cuenta y la región.

El siguiente ejemplo completo muestra cómo se pueden utilizar las claves de contexto `aws:SourceArn` y las condiciones `aws:SourceAccount` globales en una política de confianza para evitar el problema de los diputados confusos con DataSync ellas.

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 ver más ejemplos de políticas que muestran cómo se pueden utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves contextuales con ellas DataSync, consulte los siguientes temas:

- [Cree una relación de confianza que le permita acceder DataSync a su bucket de Amazon S3](#)
- [Para configurar manualmente un rol de IAM para acceder a su bucket de Amazon S3](#)

Validación de conformidad para AWS DataSync

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa de cumplimiento](#) [Servicios de AWS](#) de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#).

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#).

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- [Cumplimiento de seguridad y gobernanza](#): en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- [Referencia de servicios válidos de HIPAA](#): muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- [AWS Recursos de](#) de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.

- [AWS Guías de cumplimiento para clientes](#): comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- [Evaluación de los recursos con reglas](#) en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Este Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la [Referencia de controles de Security Hub](#).
- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- [AWS Audit Manager](#)— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS DataSync

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puedes diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Note

Si una zona de disponibilidad a la que está migrando datos o desde la que está migrando datos falla mientras está ejecutando una DataSync tarea, la tarea también fallará.

Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte la [infraestructura AWS global](#).

Seguridad de infraestructura en AWS DataSync

Como servicio gestionado, AWS DataSync está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a DataSync través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Proteger las credenciales de ubicación de almacenamiento

DataSync usa [ubicaciones](#) para acceder a los recursos de almacenamiento que se encuentran en las instalaciones, en otras nubes o dentro de ellas. AWS Algunos tipos de ubicaciones requieren que proporcione credenciales, como una clave de acceso y una clave secreta o un nombre de usuario y una contraseña, para autenticarse en el sistema de almacenamiento. Al crear una DataSync ubicación que requiere credenciales para la autenticación, puede elegir una de las siguientes opciones para controlar cómo se almacena el secreto de sus credenciales:

- Guarde el secreto AWS Secrets Manager mediante un secreto administrado por el servicio cifrado con una clave predeterminada.
- Guarde el secreto AWS Secrets Manager utilizando un secreto administrado por el servicio cifrado con una AWS KMS clave que usted administre.

- Guarde el secreto AWS Secrets Manager con un secreto y una clave que usted cree y administre. DataSync accede a este secreto mediante una función de IAM que usted proporcione.

En todos los casos, el secreto de Secrets Manager se guarda en tu cuenta, lo que te permite actualizarlo según sea necesario, independientemente del DataSync servicio. Solo se te cobrará por el uso de los secretos que crees fuera de él DataSync. Los secretos creados y gestionados por DataSync llevan el prefijo `aws-datasync`.

Uso de un secreto administrado por el servicio cifrado con una clave predeterminada

Al crear tu DataSync ubicación, solo tienes que proporcionar la cadena secreta. DataSync crea un recurso secreto AWS Secrets Manager para almacenar el secreto que usted proporciona y lo cifra con la clave KMS de Secrets Manager predeterminada para su cuenta. Puedes cambiar el valor secreto directamente en Secrets Manager o actualizando la ubicación mediante la DataSync consola o el SDK. AWS CLI Cuando eliminas el recurso de ubicación o lo actualizas para usar un secreto personalizado, el recurso secreto se DataSync elimina automáticamente.

Note

Para crear, modificar y eliminar recursos secretos en Secrets Manager, DataSync debe tener los permisos adecuados. Para más información, consulte [Políticas administradas de AWS para DataSync](#).

Utilizar un secreto administrado por el servicio cifrado con una clave personalizada AWS KMS

Al crear la DataSync ubicación, proporciona el secreto y el ARN de la clave. AWS KMS DataSync crea automáticamente un recurso secreto AWS Secrets Manager para almacenar el secreto que proporcionas y lo cifra con tu AWS KMS clave. Puedes cambiar el valor secreto directamente en Secrets Manager o actualizando la ubicación mediante la DataSync consola o el SDK. AWS CLI Cuando eliminas el recurso de ubicación o lo actualizas para usar un secreto personalizado, el recurso secreto se DataSync elimina automáticamente.

Note

AWS KMS La clave debe utilizar un cifrado simétrico con el tipo de ENCRYPT_DECRYPT clave. Para obtener más información, consulte [Elegir una AWS Key Management Service clave](#) en la Guía del AWS Secrets Manager usuario.

Para crear, modificar y eliminar recursos secretos en Secrets Manager, DataSync debe tener los permisos adecuados. Para obtener más información, consulte [Políticas administradas de AWS : AWSDataSyncFullAccess](#).

Además de usar la política DataSync administrada correcta, también necesita los siguientes permisos:

```
{
  "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 Sustitúyala por el ARN de la clave KMS.

Para recuperar y descifrar el valor secreto, DataSync utiliza un rol vinculado a un servicio (SLR) para acceder a la clave. AWS KMS Para asegurarte de que DataSync puedes usar tu clave KMS, agrega lo siguiente a la declaración de política de la clave:

```
{
  "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 Sustitúyala por tu Cuenta de AWS ID.

Usando un secreto que tú administras

Antes de crear tu DataSync ubicación, [crea una entrada secreta](#). AWS Secrets Manager El valor del secreto solo debe contener la propia cadena secreta en texto plano. Al crear la DataSync ubicación, proporciona el ARN del secreto y una función de IAM que se DataSync utiliza para acceder tanto a su secreto como a la AWS KMS clave utilizada para cifrarlo. Para crear un rol de IAM con los permisos adecuados, haga lo siguiente:

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación situado a la izquierda, en Administración de acceso, elija Roles y luego Crear rol.
3. En la página Seleccione una entidad de confianza, en Tipo de entidad de confianza, elija AWS servicio.
4. En Caso de uso, elija una opción DataSync de la lista desplegable. Elija Siguiente.
5. En la página Agregar permisos, elija Siguiente. Introduzca un nombre para su función y, a continuación, elija Crear función.
6. En la página Roles, busque el rol que acaba de crear y seleccione el nombre.
7. En la página de detalles del rol, selecciona la pestaña Permisos. Seleccione Añadir permisos y, a continuación, Crear política integrada.
8. Seleccione la pestaña JSON y añada los siguientes permisos al editor de políticas:

JSON

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

```

        "Action": [
            "secretsmanager:GetSecretValue",
            "secretsmanager:DescribeSecret"
        ],
        "Resource": "your-secret-arn"
    }
]
}

```

your-secret-arn Sustitúyalo por el ARN de tu secreto de Secrets Manager.

9. Elija Siguiente. Introduzca un nombre para su política y, a continuación, elija Crear política.
10. (Recomendado) Para evitar el [problema del suplente confuso entre servicios](#), haga lo siguiente:
 - a. En la página de detalles del rol, selecciona la pestaña Relaciones de confianza. Elija Editar la política de confianza.
 - b. Actualice la política de confianza mediante el siguiente ejemplo, que incluye las claves de contexto de condición global de `aws:SourceArn` y `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. Elija Actualizar política.

Puede especificar este rol al crear su ubicación. Si tu secreto utiliza una AWS KMS clave gestionada por el cliente para el cifrado, también tendrás que actualizar la política de la clave para permitir el acceso desde la función que creaste en el procedimiento anterior. Para actualizar la política, añade lo siguiente a la declaración de política de tu AWS KMS clave:

```
{
  "Sid": "Allow DataSync use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam accountid:role/your-role-name"
  },
  "Action": "kms:Decrypt",
  "Resource": "*"
}
```

accountid Sustitúyala por tu Cuenta de AWS ID y *your-role-name* por el nombre de la función de IAM que creaste en el procedimiento anterior.

 Note

Cuando guardas secretos en Secrets Manager, Cuenta de AWS incurres en cargos. Para obtener más información acerca de los precios, consulte [Precios de AWS Secrets Manager](#).

AWS DataSync cuotas

Obtenga información sobre las cuotas y los límites de los recursos cuando trabaje con ellos AWS DataSync.

Límites del sistema de almacenamiento, de los archivos y de los objetos

En la siguiente tabla se describen los límites DataSync que existen al trabajar con sistemas de almacenamiento, archivos y objetos.

Descripción	Límite
Longitud máxima total de la ruta del archivo	4096 bytes
Longitud máxima del componente de la ruta del archivo (nombre de archivo, directorio o subdirectorios)	255 bytes
Longitud máxima del dominio de Windows	253 caracteres
Longitud máxima del nombre de host del servidor	255 caracteres
Longitud máxima del nombre del objeto de Amazon S3	1024 caracteres UTF-8

DataSync cuotas

En la siguiente tabla se describen las cuotas de DataSync recursos en una región específica Cuenta de AWS .

Recurso	Cuota	Ajustable
Cantidad máxima de tareas que puede crear	100	Sí

Recurso	Cuota	Ajustable
(Tareas en modo mejorado) Número máximo de objetos de origen y destino con los que DataSync se puede trabajar por ejecución de tarea Para obtener más información, consulte Cómo DataSync transfiere los archivos, objetos y directorios	Prácticamente ilimitado	N/A

Recurso	Cuota	Ajustable
(Tareas del modo básico) Número máximo de archivos, objetos y directorios de origen y destino con los que DataSync se puede trabajar por ejecución de tareas entre servicios de almacenamiento y AWS almacenamiento locales, autogestionados o en la nube Para obtener más información, consulte Cómo DataSync transfiere los archivos, objetos y directorios	50 millones  Important Recuerde lo siguiente acerca de esta cuota: • Si transfiere objetos de Amazon S3 con prefijos, los prefijos se tratan como directorios y se tienen en cuenta para la cuota. Por ejemplo, DataSync <code>s3://bucket/foo/bar.txt</code> consideraría dos directorios (<code>./y./foo/</code>) y un objeto (<code>bar.txt</code>). • Si su tarea consiste en trabajar con más de 20 millones de archivos, objetos o directorios, asegúrese de asignar un mínimo de 64 GB de RAM a su DataSync agente. Para obtener más información, consulte los requisitos de los	Sí  Tip En lugar de solicitar un aumento, puede crear tareas que se centren en directorios específicos mediante filtros de inclusión y exclusión. Para obtener más información, consulte Filtrar los

Recurso	Cuota	Ajustable
	agentes para DataSync las transferencias.	datos transferidos por DataSync.

Recurso	Cuota	Ajustable
(Tareas del modo básico) Número máximo de archivos, objetos y directorios de origen y destino con los que DataSync se puede trabajar por ejecución de tarea entre los servicios AWS de almacenamiento Para obtener más información, consulte Cómo DataSync transfiere los archivos, objetos y directorios	25 millones Important Si transfiere objetos de Amazon S3 con prefijos, los prefijos se tratan como directorios y se tienen en cuenta para la cuota. Por ejemplo, DataSync <code>s3://bucket/foo/bar.txt</code> consideraría dos directorios (<code>./y./foo/</code>) y un objeto (<code>bar.txt</code>).	Tip En lugar de solicitar un aumento, puede crear tareas que se centren en directorios específicos mediante filtros de inclusión y exclusión. Para obtener más información, consulte filtrar los

Recurso	Cuota	Ajustable
		datos transferidos por DataSync.
Rendimiento máximo por tarea (para transferencias que utilizan un DataSync agente)	10 Gbps	No
Rendimiento máximo por tarea (para transferencias que no utilizan un DataSync agente)	5 Gbps	No
Número máximo de caracteres que puede incluir en una cadena de filtro	102 400 caracteres	No
	 Note Si utilizas la DataSync consola, este límite incluye todos los personajes combinados en tus patrones de inclusión y exclusión.	
Número máximo de ejecuciones en cola para una sola tarea	50	No
Número máximo de ejecuciones simultáneas de tareas en modo mejorado	120	No
Número máximo de días que se conserva el historial de ejecuciones de tareas	30	No

Solicitud de un aumento de cuota

Puede solicitar un aumento de algunas DataSync cuotas. Los aumentos no se conceden de inmediato y pueden tardar un par de días en surtir efecto.

Cómo solicitar un aumento de cuota

1. Abra la consola de Service Quotas en <https://console.aws.amazon.com/servicequotas/>.
2. En el panel de navegación, elija servicios de AWS y después seleccione AWS DataSync.
3. Elija la cuota que quiere aumentar y, a continuación, seleccione Solicitar aumento a nivel de cuenta.
4. Introduzca la cantidad total que desea asignarle a la cuota y después seleccione Solicitar.

Si necesita aumentar una cuota diferente, rellene una solicitud independiente.

Solución de AWS DataSync problemas

Utilice la siguiente información para solucionar AWS DataSync problemas y errores.

Temas

- [Solución de problemas con los agentes DataSync](#)
- [Solución de problemas con DataSync las ubicaciones](#)
- [Solución de problemas con DataSync las tareas](#)
- [Solución de problemas de verificación de datos](#)
- [Solución de problemas con costes de almacenamiento en S3 superiores a los esperados con DataSync](#)

Solución de problemas con los agentes DataSync

Utilice la siguiente información como ayuda para solucionar problemas con los AWS DataSync agentes. Algunos de estos problemas pueden incluir:

- Problemas para conectarse a la consola local de un EC2 agente de Amazon
- No se pudo recuperar la clave de activación de un agente
- Problemas al activar un agente con un punto final de servicio de VPC
- Descubrir que un agente está desconectado

¿Cómo me conecto a la consola local de un EC2 agente de Amazon?

Para conectarte a la consola local de un EC2 agente de Amazon, debes usar SSH. Asegúrate de que el grupo de seguridad de la EC2 instancia permita el acceso mediante SSH (puerto TCP 22).

En un terminal, ejecute el siguiente comando `ssh` para conectarse a la instancia:

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

- Para */path/key-pair-name* ello, especifique la ruta y el nombre de archivo (`.pem`) de la clave privada necesaria para conectarse a la instancia.
- En *instance-user-name*, especifique `admin`.

- Para *instance-public-ip-address*, especifica la dirección IP pública de la instancia.

¿Qué significa el error Failed to retrieve agent activation key?

Al activar el DataSync agente, el agente se conecta al punto final del servicio que especifique para solicitar una clave de activación. Posiblemente, este error significa que la configuración de seguridad de la red está bloqueando la conexión.

Acción que debe ejecutarse

Si utiliza un punto de conexión del servicio de la nube privada virtual (VPC), verifique que la configuración del grupo de seguridad permite a su agente conectarse al punto de conexión de VPC. Para obtener información acerca de los puertos necesarios, consulte [Requisitos de red para puntos de conexión de servicio de VPC](#).

Si utiliza un punto de conexión público o del Estándar Federal de Procesamiento de la Información (Federal Information Processing Standard, FIPS), verifique que la configuración del firewall y del router permiten a su agente conectarse a dicho punto de conexión. Para obtener información, consulte [Requisitos de red para puntos de conexión de servicio públicos o FIPS](#).

Sigo sin poder activar un agente mediante un punto de conexión de servicio de VPC

Si sigues teniendo problemas para activar un DataSync agente con un punto final de servicio de VPC, consulta [No sé qué le pasa a mi agente. ¿Hay alguien que pueda ayudarme?](#)

¿Qué hago si mi agente está desconectado?

Es posible que tu DataSync agente esté desconectado por varios motivos, pero es posible que puedas volver a conectarlo. Antes de eliminar el agente y de crear otro nuevo, consulte la siguiente lista de verificación para comprender qué puede haber ocurrido.

- Póngase en contacto con el equipo de backup: si su agente está desconectado porque su máquina virtual (VM) se ha restaurado a partir de una instantánea o de una copia de seguridad, es posible que deba [reemplazar el agente](#).
- Comprueba si la máquina virtual o la EC2 instancia de Amazon del agente están apagadas: según el tipo de agente que utilices, intenta volver a activar la máquina virtual o la EC2 instancia si están apagadas. Una vez que se vuelva a activar, [comprueba la conectividad de red del agente](#) a AWS.

- Compruebe que el agente cumpla con los requisitos mínimos de hardware: es posible que su agente esté desconectado porque la configuración de su máquina virtual o EC2 instancia se modificó accidentalmente desde que se activó el agente. Por ejemplo, si la VM ya no tiene la memoria o el espacio mínimos requeridos, es posible que el agente aparezca desconectado. Para obtener más información, consulte [Requisitos para los agentes AWS DataSync](#).
- Espere a que finalicen las actualizaciones de software relacionadas con el agente: es posible que su agente se desconecte brevemente después de recibir [las actualizaciones de software proporcionadas por AWS](#). Si cree que este es el motivo por el que el agente está desconectado, espere un breve período de tiempo y verifique si el agente ha vuelto a conectarse.
- Compruebe la configuración del punto de enlace del servicio de VPC: si su agente sin conexión utiliza un punto de enlace de servicio público y también en la misma VPC para la que creó un punto de enlace del servicio de VPC DataSync, es posible que deba deshabilitar la [compatibilidad con DNS](#) privado para ese punto de enlace de VPC.

Si ninguno de estos motivos parece ser la razón por la que el agente está desconectado, es probable que tenga que [reemplazar el agente](#).

No sé qué le pasa a mi agente. ¿Hay alguien que pueda ayudarme?

Puedes permitir el acceso AWS Support a tu DataSync agente y ayudarte a solucionar problemas relacionados con el agente. Debe habilitar este acceso mediante la consola local del agente.

Para proporcionar Soporte acceso a su agente

1. [Inicie sesión en la consola local del agente](#).
2. Cuando se le solicite, introduzca **5** para abrir la línea de comandos (para VMware VMs, use **6**).
3. Introduzca **h** para abrir la ventana AVAILABLE COMMANDS (COMANDOS DISPONIBLES).
4. En la ventana COMANDOS DISPONIBLES, introduzca lo siguiente para conectarse a Soporte:

open-support-channel

Si utiliza el agente con puntos de conexión de VPC, debe proporcionar una dirección IP de punto de conexión de VPC para su canal de soporte, de la siguiente manera:

open-support-channel *vpc-ip-address*

Su firewall debe permitir que el puerto TCP 22 de entrada inicie un canal de soporte hacia AWS. Cuando se conecta a Soporte, le DataSync asigna un número de soporte. Apunte el número de soporte.

 Note

El número de canal no es un número de puerto TCP/UDP. En lugar de ello, realiza una conexión SSH (TCP 22) a los servidores y proporciona el canal de soporte para la conexión.

5. Cuando se haya establecido el canal de asistencia, proporciona tu número de servicio de asistencia para que Soporte puedan ayudarte a solucionar problemas.
6. Cuando la sesión de soporte finalice, pulse **Enter** para terminarla.
7. Introduzca **exit** para cerrar sesión en la consola DataSync local.
8. Siga las instrucciones para salir de la consola local.

Solución de problemas con DataSync las ubicaciones

Utilice la siguiente información como ayuda para solucionar problemas con las AWS DataSync ubicaciones. Algunos de estos problemas pueden incluir:

- Errores de permisos y montaje con ubicaciones de NFS
- Problemas de propiedad de los archivos
- Problemas para acceder a las ubicaciones SMB que utilizan la autenticación Kerberos
- Problemas de permisos y acceso con el almacenamiento de objetos, como las ubicaciones de Amazon S3 y Microsoft Azure Blob

Mi tarea ha fallado debido a un error de permisos de NFS denegados

Puede aparecer un mensaje de error de “permissions denied” si configura el servidor de archivos NFS con `root_squash` o `all_squash` y los archivos no tienen acceso de lectura.

Acción que debe ejecutarse

Para solucionar este problema, configure la exportación de NFS con `no_root_squash` o asegúrese de que los permisos para todos los archivos que desea transferir permiten el acceso de lectura a todos los usuarios.

Para acceder DataSync a los directorios, también debe habilitar el acceso de ejecución total. Para asegurarse de que el directorio se puede montar, en primer lugar, conéctese a cualquier equipo que tenga la misma configuración de red que el agente. A continuación, ejecute el siguiente comando de 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>
```

Si el problema sigue sin resolverse, póngase en contacto con el Centro [AWS Support](#).

Mi tarea ha fallado debido a un error de montaje de NFS

Es posible que aparezca el siguiente error al ejecutar una DataSync tarea que implica una ubicación de servidor de archivos NFS:

La tarea no pudo acceder a la ubicación `loc-1111222233334444a: x40016: mount.nfs: se agotó el tiempo de espera de la conexión`

Acciones que ejecutar

Haga lo siguiente hasta que se resuelva el error.

1. Asegúrese de que el servidor de archivos NFS y la exportación que especifique en su DataSync ubicación sean válidos. Si no lo son, elimine la ubicación y la tarea y, a continuación, cree una nueva ubicación y tarea que utilice un servidor de archivos de NFS válido y exporte. Para obtener más información, consulte [Mediante la consola de DataSync](#).
2. Compruebe la configuración del firewall entre el agente y el servidor de archivos de NFS. Para obtener más información, consulte [Requisitos de red para el almacenamiento autoadministrado en las instalaciones y otros tipos de almacenamiento periférico en la nube](#).
3. Asegúrese de que su agente pueda acceder al servidor de archivos de NFS y montar la exportación. Para obtener más información, consulte [Proporcionar DataSync acceso a los servidores de archivos NFS](#).
4. Si sigue apareciendo el error, abra un canal de soporte con Soporte. Para obtener más información, consulte [No sé qué le pasa a mi agente. ¿Hay alguien que pueda ayudarme?](#).

Mi tarea ha fallado debido a un error de montaje de Amazon EFS

Es posible que aparezca el siguiente error al ejecutar una DataSync tarea que implica una ubicación de Amazon EFS:

La tarea no pudo acceder a la ubicación loc-1111222233334444a: x40016: no se pudo conectar al destino de montaje de EFS con IP: 10.10.1.0.

Esto puede ocurrir si la ruta de montaje del sistema de archivos Amazon EFS que configuró con su ubicación se actualiza o elimina. DataSync no tiene conocimiento de estos cambios en el sistema de archivos.

Acción que debe ejecutarse

Elimine la ubicación y la tarea y [cree una nueva ubicación de Amazon EFS](#) con la nueva ruta de montaje.

La propiedad de los archivos no se mantiene con la transferencia NFS

Tras la transferencia, es posible que observe que los archivos de la ubicación de DataSync destino tienen un usuario IDs (UIDs) o grupo IDs (GIDs) diferente al de los archivos de la ubicación de origen. Por ejemplo, los archivos de su destino pueden tener un UID de 65534, 99 o nobody.

Esto puede suceder si un sistema de archivos implicado en la transferencia utiliza el mapeo de ID de la versión 4 de NFS, una función que DataSync no es compatible.

Acción que debe ejecutarse

Existen un par de opciones para solucionar este problema:

- Cree una nueva ubicación para el sistema de archivos que use la versión 3 de NFS en vez de la 4.
- Deshabilite el mapeo de ID de la versión 4 de NFS en el sistema de archivos.

Intente volver a hacer la transferencia. Cualquiera de estas opciones debería resolver el problema.

Mi tarea no puede acceder a una ubicación SMB que utilice Kerberos

DataSync los errores en las ubicaciones SMB que utilizan la [autenticación de Kerberos](#) suelen estar relacionados con la falta de coincidencia entre la ubicación y las configuraciones de Kerberos. También puede haber un problema de red.

No se pudo acceder a la ubicación

El siguiente error indica que puede haber problemas de configuración con la ubicación de SMB o con la configuración de Kerberos:

```
Task failed to access location
```

Compruebe lo siguiente:

- El servidor de archivos SMB que especifique para su ubicación es un nombre de dominio. En el caso de Kerberos, no puede especificar la dirección IP del servidor de archivos.
- El principal de Kerberos que especifique para su ubicación coincide con el principal que utilice para crear el archivo de tabla de claves de Kerberos (keytab). Los nombres principales distinguen entre mayúsculas y minúsculas.
- La contraseña de usuario asignada del principal de Kerberos no ha cambiado desde que creó el archivo keytab. Si la contraseña cambia (debido a la rotación de la contraseña o por algún otro motivo), es posible que la ejecución de la tarea no se ejecute correctamente y muestre el siguiente error:

La tarea no pudo acceder a la ubicación loc-1111222233334444a: x40015: kinit: no se pudo realizar la autenticación previa al obtener las credenciales iniciales

No se puede contactar con el dominio KDC

El siguiente error indica un problema de red:

```
kinit: Cannot contact any KDC for realm 'MYDOMAIN.ORG' while getting initial credentials"
```

Compruebe lo siguiente:

- El archivo de configuración de Kerberos (`krb5.conf`) que DataSync ha proporcionado contiene la información correcta sobre su dominio de Kerberos. Para ver un `krb5.conf` archivo de ejemplo, consulte Requisitos previos de autenticación de [Kerberos](#).
- El puerto del servidor del Centro de distribución de claves (KDC) de Kerberos está abierto. El puerto KDC suele ser el puerto TCP 88.
- La configuración de DNS de su red.

Mi tarea ha fallado debido a un error de entrada/salida

Puede recibir input/output error message if your storage system fails I/O solicitudes del DataSync agente. Entre los motivos más frecuentes se incluyen un fallo en el disco del servidor, cambios en la configuración del firewall o un fallo en el router de la red.

Si el error implica a un servidor de archivos de NFS o a un clúster del sistema de archivos distribuido de Hadoop (HDFS), siga estos pasos para resolver el error.

Acciones a realizar (NFS)

En primer lugar, compruebe las métricas y los registros del servidor de archivos de NFS para determinar si el problema se inició en el servidor de NFS. En caso afirmativo, resuelva el problema.

A continuación, compruebe que la configuración de la red no ha cambiado. Para comprobar si el servidor de archivos NFS está configurado correctamente y si DataSync puede acceder a él, haga lo siguiente:

1. Configure otro cliente de NFS en la misma subred de red en la que está configurado el agente de .
2. Monte el recurso compartido en dicho cliente.
3. Valide que el cliente pueda leer y escribir en el recurso compartido de forma correcta.

Acciones a realizar (HDFS)

Haga lo siguiente hasta que se resuelva el error:

1. Asegúrese de que el clúster HDFS permite que el DataSync agente se comuniquen con los puertos NameNode y DataNode el clúster.

En la mayoría de los clústeres, puede encontrar los números de puerto que utiliza el clúster en los siguientes archivos de configuración:

- Para encontrar el NameNode puerto, busque en el `core-site.xml` archivo debajo de la `fs.default.name` propiedad `fs.default` o (según la distribución de Hadoop).
 - Para encontrar el DataNode puerto, busque en el `hdfs-site.xml` archivo situado debajo de la `dfs.datanode.address` propiedad.
2. En el archivo `hdfs-site.xml`, compruebe que la propiedad `dfs.data.transfer.protection` solo tiene un valor. Por ejemplo:

```
<property>
  <name>dfs.data.transfer.protection</name>
  <value>privacy</value>
</property>
```

Error: **FsS3UnableToConnectToEndpoint**

DataSync no puede conectarse a su [ubicación de Amazon S3](#). Esto puede significar que no es posible acceder al bucket S3 de la ubicación o que la ubicación no se ha configurado correctamente.

Haga lo siguiente hasta que se resuelva el problema:

- Compruebe si DataSync puede [acceder a tu bucket de S3](#).
- Asegúrese de que la ubicación esté configurada correctamente mediante la DataSync consola o la operación [DescribeLocationS3](#).

Error: **FsS3HeadBucketFailed**

DataSync no puede acceder al depósito de S3 desde o hacia el que está realizando la transferencia. Compruebe si DataSync tiene permiso para acceder al bucket mediante la [HeadBucket](#) operación Amazon S3. Si necesitas ajustar tus permisos, consulte [Proporcionar DataSync acceso a los depósitos de S3](#).

La tarea falla y se produce un **Unable to list Azure Blobs on the volume root** error

Si la tarea de DataSync transferencia falla debido a un Unable to list Azure Blobs on the volume root error, es posible que haya un problema con el token de la firma de acceso compartido (SAS) o con su Azure la red de la cuenta de almacenamiento.

Acciones que ejecutar

Pruebe lo siguiente y vuelva a ejecutar la tarea hasta que se resuelva el problema:

- Asegúrese de que su [token SAS](#) tenga los permisos correctos para acceder a su Microsoft Azure Blob Storage.

- Si está ejecutando a su DataSync agente en Azure, configure su cuenta de almacenamiento para permitir el acceso desde la red virtual en la que reside su agente.
- Si ejecutas tu agente en Amazon EC2, configura tu Azure firewall de almacenamiento para permitir el acceso desde la dirección IP pública del agente.

Para obtener información sobre cómo configurar su Azure la red de la cuenta de almacenamiento, consulta la [Azure Blob Storage documentación](#).

Error: **FsAzureBlobVolRootListBlobsFailed**

El token de firma de acceso compartido (SAS) que se DataSync utiliza para acceder a su Microsoft Azure Blob Storage no tiene el permiso de lista.

Para resolver el problema, [actualise su ubicación](#) con un token que tenga el permiso de lista e intente ejecutar la tarea de nuevo.

Error: **SrcLocHitAccess**

DataSync no puede acceder a la ubicación de origen. Comprueba si DataSync tienes permiso para acceder a la ubicación e intenta ejecutar la tarea de nuevo.

Error: **SyncTaskErrorLocationNotAdded**

DataSync no puedes acceder a tu ubicación. Comprueba si DataSync tienes permiso para acceder a la ubicación e intenta ejecutar la tarea de nuevo.

La tarea con la ubicación de origen de S3 se produce un **GetObjectTagging** error **HeadObject** o se produce un error

Si está transfiriendo objetos con una versión específica IDs desde un bucket de S3, es posible que aparezca un error relacionado con HeadObject o GetObjectTagging. Por ejemplo, aquí hay un error relacionado con 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
```

Si ve alguno de estos errores, compruebe que la función de IAM que se DataSync utiliza para acceder a la ubicación de origen de S3 tenga los siguientes permisos:

- s3:GetObjectVersion
- s3:GetObjectVersionTagging

Si necesita actualizar su rol con estos permisos, consulte [Crear un rol de IAM para acceder DataSync a su ubicación de Amazon S3](#).

Solución de problemas con DataSync las tareas

Utilice la siguiente información como ayuda para solucionar problemas relacionados con AWS DataSync las tareas y su ejecución. Estos problemas pueden incluir problemas de configuración de tareas, ejecuciones de tareas bloqueadas y datos que no se transfieren como se esperaba.

Error: SyncOption valor no válido. Opción:

TransferMode, PreserveDeletedFiles, Valor: ALL, REMOVE.

Este error se produce cuando estás creando o editando la DataSync tarea y seleccionas la opción Transferir todos los datos y deseleccionas la opción Conservar los archivos eliminados.

Al transferir todos los datos, DataSync no escanea la ubicación de destino y no sabe qué eliminar.

La ejecución de la tarea falla y se produce un EniNotFounderror

Este error se produce cuando elimina una de las interfaces de red de la tarea en la nube privada virtual (VPC). Si la tarea está programada o en cola, se producirá un error si falta la [interfaz de red necesaria para transferir los datos](#).

Acciones que ejecutar

Para resolver este problema, dispone de las siguientes opciones:

- Reinicie la tarea manualmente. Al hacerlo, se DataSync crearán las interfaces de red que falten y que necesite para ejecutar la tarea.
- Si necesita limpiar los recursos de la VPC, asegúrese de no eliminar las interfaces de red relacionadas con una DataSync tarea que sigue utilizando.

Para ver las interfaces de red asignadas a la tarea, realice una de las siguientes acciones:

- Utilice la operación [DescribeTask](#). Puede ver las interfaces de red en los elementos de respuesta `SourceNetworkInterfaceArns` y `DestinationNetworkInterfaceArns`.
- En la EC2 consola de Amazon, busca tu ID de tarea (por ejemplo `task-f012345678abcdef0`) para encontrar sus interfaces de red.
- Considere la posibilidad de no ejecutar las tareas automáticamente. Esto podría incluir deshabilitar la programación o la puesta en cola de tareas (mediante DataSync la automatización o la automatización personalizada).

La ejecución de la tarea falla y se produce un error de «no se puede asignar memoria»

Si la DataSync tarea falla y aparece un error de «no se puede asignar memoria», esto puede significar varias cosas diferentes.

Acción que debe ejecutarse

Intente hacer lo siguiente hasta que el problema desaparezca:

- Si la transferencia involucra a un agente, asegúrate de que el agente cumpla con los requisitos de la [máquina virtual \(VM\)](#) o de la [EC2 instancia de Amazon](#).
- Divida la transferencia en varias tareas mediante [filtros](#). Es posible que estés intentando transferir más archivos u objetos de los que [puede gestionar una sola DataSync tarea](#).
- Si el problema persiste, póngase en [contacto con Soporte](#).

La ejecución de la tarea está en estado de inicio, pero parece que no ocurre nada

DataSync La tarea puede quedarse atascada con el estado de inicio, normalmente porque el agente está apagado o ha perdido la conectividad de red.

Acción que debe ejecutarse

Asegúrese de que el estado de su agente sea CONECTADO. Si el agente está DESCONECTADO, asegúrese de que esté encendido.

Si el agente está activado y la tarea sigue bloqueada en el estado INICIANDO, lo más probable es que exista un problema de conectividad de red entre el agente y AWS. Para obtener más información sobre cómo probar la conectividad de red, consulte [Verificar la conexión de su agente al servicio DataSync](#).

Si el problema persiste, consulte [No sé qué le pasa a mi agente. ¿Hay alguien que pueda ayudarme?](#).

La ejecución de la tarea parece estancada en el estado de preparación

El momento en que la tarea de DataSync transferencia pasa al estado de preparación depende de la cantidad de datos de la fuente y el destino de la transferencia y del rendimiento de esos sistemas de almacenamiento.

Cuando se inicia una tarea, DataSync realiza una lista de directorios recursiva para detectar todos los archivos, objetos, directorios y metadatos del origen y el destino. DataSync utiliza estos listados para identificar las diferencias entre los sistemas de almacenamiento y determinar qué copiar. Este proceso puede tardar unos minutos e incluso unas horas.

Acción que debe ejecutarse

No debería tener que hacer nada. Continúe esperando a que el estado de la tarea cambie a Transfiriendo. Si el estado sigue sin cambiar, póngase en contacto con el Centro [AWS Support](#).

La ejecución de la tarea se detiene antes de que finalice la transferencia

Si la ejecución de la DataSync tarea se detiene antes de tiempo, la configuración de la tarea puede incluir una Región de AWS que esté deshabilitada en la suya Cuenta de AWS.

Acciones que ejecutar

Haga lo siguiente para volver a ejecutar la tarea:

1. Compruebe el [estado de suscripción](#) de las regiones de su tarea y asegúrese de que estén habilitadas.

2. Vuelva a [iniciar la tarea](#).

Se produce un error en la ejecución de la tarea al transferirla desde un depósito de Google Cloud Storage

Como DataSync se comunica con Google Cloud Storage mediante la API de Amazon S3, existe una limitación que puede provocar que la DataSync transferencia no se realice correctamente si intentas copiar etiquetas de objetos. En tus CloudWatch registros aparece el siguiente mensaje relacionado con el problema:

[WARN] No se pudieron leer los metadatos del archivo/*your-bucket/your-object*: S3 No se pudo etiquetar el objeto: se continúa sin etiquetar

Para evitarlo, desactive la opción Copiar etiquetas de objetos al configurar los ajustes de la tarea de transferencia.

Hay discordancias entre las marcas de tiempo de ejecución de la tarea

Al mirar la DataSync consola o los CloudWatch registros de Amazon, es posible que notes que las horas de inicio y finalización de la ejecución de la DataSync tarea no coinciden con las marcas de tiempo que ves en otras herramientas de supervisión. [Esto se debe a que la consola y CloudWatch los registros tienen en cuenta el tiempo que tarda la ejecución de una tarea en el estado de inicio o de espera, mientras que otras herramientas no lo hacen.](#)

Es posible que notes esta discrepancia al comparar las marcas temporales de ejecución entre la DataSync consola o los CloudWatch registros y los siguientes lugares:

- Registra el sistema de archivos implicado en la transferencia
- La fecha de la última modificación de un objeto de Amazon S3 que DataSync escribió en
- Tráfico de red procedente del DataSync agente
- EventBridge Eventos de Amazon

La ejecución de la tarea falla debido a **NoMem** un error

Es posible que el conjunto de datos que intentas transferir sea demasiado grande DataSync. Si ve este error, póngase en contacto con el [Centro de AWS Support](#).

El objeto no se puede transferir a Azure Blob Storage con **user metadata key** error

Al transferir de un bucket de S3 a Azure Blob Storage, es posible que aparezca el siguiente error:

```
[ERROR] Failed to transfer file /user-metadata/file1: Azure Blob user metadata key must be a CSharp identifier
```

Esto significa que */user-metadata/file1* incluye los metadatos del usuario que no utilizan un identificador de C# válido. Para obtener más información, consulte la [documentación de Microsoft](#).

Hay una **/.aws-datasync** carpeta en la ubicación de destino

DataSync crea una carpeta llamada **/.aws-datasync** en su ubicación de destino para facilitar la transferencia de datos.

Aunque DataSync normalmente elimina esta carpeta después de la transferencia, puede haber situaciones en las que esto no suceda.

Acción que debe ejecutarse

Elimine esta carpeta en cualquier momento, siempre y cuando no tenga una tarea en ejecución copiando en esa ubicación.

No se pueden transferir enlaces simbólicos entre ubicaciones mediante SMB

Cuando finalice la ejecución de la tarea, aparecerá el siguiente error:

```
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.
```

Al realizar transferencias entre sistemas de almacenamiento SMB (como un servidor de archivos SMB y el sistema de archivos Amazon FSx for Windows File Server), es posible que veas las siguientes advertencias y errores en tus CloudWatch registros:

```
[WARN] Failed to read metadata for file /appraiser/symlink: No data available  
[ERROR] Failed to read metadata for directory /appraiser/symlink: No data available
```

Acción que debe ejecutarse

DataSync no admite la transferencia de enlaces simbólicos (o enlaces físicos) al realizar transferencias entre estos tipos de ubicaciones. Para obtener más información, consulte [Enlaces y directorios copiados por AWS DataSync](#).

Errores en el informe de la tarea

Es posible que te encuentres con uno de los siguientes errores al intentar supervisar la DataSync transferencia con un informe de tareas.

Mensaje de error	Solución
File path exceeds the maximum length of 4,096 characters. Cannot write to Task Report	N/A (no DataSync se puede transferir un archivo con una ruta que supere los 4.096 bytes) Para obtener más información, consulte Límites del sistema de almacenamiento, de los archivos y de los objetos.
Failed to upload Task Report(s) to S3 due to an invalid bucket or IAM role	Compruebe que el rol de DataSync IAM tiene los permisos adecuados para cargar un informe de tareas en su bucket de S3.
Execution error occurred prior to generating any Task Reports	Revise sus CloudWatch registros para identificar por qué falló la ejecución de la tarea.

Solución de problemas de verificación de datos

De forma predeterminada, AWS DataSync [verifica la integridad](#) de los datos al final de una transferencia. Usa la siguiente información para ayudarte a diagnosticar los errores y advertencias de verificación más comunes, como la modificación o eliminación de archivos antes de DataSync terminar de verificar los datos.

En el caso de los problemas de verificación, muchas veces resulta útil revisar [CloudWatch los registros](#) (o [informes de tareas](#)) además del error de ejecución de la tarea que se esté detectando.

DataSync proporciona registros estructurados en JSON para las tareas del modo mejorado, mientras que las tareas del modo básico tienen registros no estructurados.

Hay discrepancias entre el contenido de un archivo

Cuando finalice la ejecución de la tarea, aparecerá el siguiente error:

```
Transfer and verification completed. Verification detected mismatches. Files with mismatches are listed in Cloud Watch Logs
```

En tus CloudWatch registros, es posible que veas errores en las verificaciones de los contenidos que difieren entre las ubicaciones de origen y destino. Esto puede ocurrir si los archivos se modifican durante la transferencia.

Por ejemplo, los siguientes registros muestran que `file1.txt` tiene `dstHash` valores y diferentes `mtime`: `srcHash`

Ejemplo de registro de 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
```

En DataSync, `mtime` representa la última vez que se escribió un archivo antes de su [preparación](#). Al verificar las transferencias, DataSync compara `mtime` los valores entre las ubicaciones de origen y destino. Se produce un error de verificación como este si el archivo `mtime` de un archivo no es el mismo en ambas ubicaciones. Las diferencias entre el contenido del archivo `srcHash` y lo `dstHash` indican no coincide en ambas ubicaciones.

Acciones que ejecutar

Haga lo siguiente:

1. Utilice un conversor de época y hora para determinar si el archivo u objeto de origen o destino se modificó más recientemente. Esto puede ayudar a identificar qué versión es la actual.
2. Para evitar que vuelva a producirse este error, [programa la tarea](#) para que se ejecute durante un período de mantenimiento, cuando no haya actividad en el origen ni en el destino.

Hay una discrepancia entre los metadatos SMB de un archivo

Cuando finalice la ejecución de la tarea, aparecerá el siguiente error:

```
Transfer and verification completed. Verification detected mismatches. Files with mismatches are listed in Cloud Watch Logs
```

Al realizar transferencias entre sistemas de almacenamiento que admiten el protocolo del bloque de mensajes del servidor (SMB), es posible que aparezca este error cuando los atributos SMB extendidos de un archivo no coinciden entre el origen y el destino.

Por ejemplo, los siguientes registros muestran que `file1.txt` tiene un `extAttrsHash` valor diferente entre las ubicaciones, lo que indica que el contenido del archivo es idéntico, pero los atributos extendidos no se establecieron en el destino:

Ejemplo de registro en 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
extAttrsHash=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
extAttrsHash=3051150340
[NOTICE]   dstHash: 38571d42b646ac8f4034b7518636b37dd0899c6fc03cdaa8369be6e81a1a2bb5
```

Es posible que también veas un mensaje de error relacionado con los atributos extendidos:

```
[ERROR] Deferred error: WriteFileExtAttr2 failed to setextattrlist(filename="/
directory1/directory2/file1.txt"): Input/output error
```

Acción que debe ejecutarse

Este error suele producirse cuando no hay permisos suficientes para copiar las listas de control de acceso (ACLs) al destino. Para resolver este problema, consulte las siguientes guías de configuración según el tipo de destino:

- [Permisos necesarios](#) FSx para los sistemas de archivos del servidor de archivos de Windows
- [Permisos necesarios](#) FSx para los sistemas de archivos ONTAP que utilizan SMB

Los archivos que se van a transferir ya no se encuentran en la ubicación de origen

Cuando finalice la ejecución de la tarea, aparecerá el siguiente error:

```
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.
```

En los registros, es posible que veas errores que indican que los archivos no están en la ubicación de origen. Esto puede ocurrir si los archivos (como file1.dll y file2.dll) se eliminan después de [prepararlos](#), pero antes de DataSync transferirlos:

Ejemplo de registro del 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
```

Acción que debe ejecutarse

Para evitar estas situaciones, [programa la tarea para](#) que se ejecute cuando no haya actividad en la ubicación de origen.

Por ejemplo, puede ejecutar la tarea durante un período de mantenimiento cuando los usuarios y las aplicaciones no estén trabajando activamente en esa ubicación.

En algunos casos, es posible que no veas los registros asociados a este error. Si eso ocurre, póngase en contacto con [AWS Support el Centro](#).

DataSync no puede verificar los datos de destino

Cuando finalice la ejecución de la tarea, aparecerá el siguiente error:

Transfer and verification completed. Verification detected mismatches. Files with mismatches are listed in Cloud Watch Logs

En tus registros, es posible que notes que no DataSync se pueden verificar determinadas carpetas o archivos de la ubicación de destino. Estos errores pueden tener este aspecto:

Ejemplo de registro en modo básico

```
[ERROR] Failed to read metadata for destination file /directory1/directory2/
file1.txt: No such file or directory
```

En el caso de los archivos, es posible que veas errores de verificación como los siguientes:

Ejemplo de registro en modo básico

[illegible]

Acción que debe ejecutarse

Estos registros indican que los datos de destino se eliminaron después de la transferencia, pero antes de la verificación. (Los registros tienen un aspecto similar cuando los datos se cargan en una ubicación de origen durante el mismo período de tiempo).

Para evitar estas situaciones, [programa la tarea para](#) que se ejecute cuando no haya actividad en la ubicación de destino.

Por ejemplo, puede ejecutar la tarea durante un período de mantenimiento cuando los usuarios y las aplicaciones no estén trabajando activamente en esa ubicación.

DataSync no puede leer los metadatos del objeto

Quando finalice la ejecución de la tarea, aparecerá el siguiente error:

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.

En sus registros, es posible que observe que no DataSync se puede leer `file1.png` debido a una `HeadObject` solicitud de Amazon S3 fallida. [DataSync realiza HeadObject solicitudes](#) a las ubicaciones de S3 durante la preparación y verificación de las tareas.

Ejemplo de registro en modo básico

```
[WARN] Failed to read metadata for file /file1.png: S3 Head Object Failed
```

Acciones que ejecutar

Para solucionar este problema, compruebe si DataSync tiene el nivel de permisos adecuado para trabajar con su bucket de S3:

- Asegúrese de que el rol de IAM que DataSync utiliza para acceder a sus ubicaciones de Amazon S3 permita el `s3:GetObject` permiso. Para obtener más información, consulte [Permisos necesarios](#).
- Si su bucket de S3 utiliza cifrado del lado del servidor, asegúrese de que DataSync tiene permiso para acceder a los objetos de ese bucket. Para obtener más información, consulte [Acceso a buckets de S3 mediante el cifrado del servidor](#).

Hay una discrepancia en los metadatos de un objeto definidos por el sistema

Cuando finalice la ejecución de la tarea en modo mejorado entre los buckets de S3, aparecerá el siguiente error:

```
Verification failed due to a difference in metadata
```

Es posible que observe en sus registros una discrepancia en los metadatos definidos por el [sistema](#) Amazon S3 de un objeto. En este ejemplo concreto, el objeto de origen no tiene `Content-Type` metadatos, pero el objeto de destino sí. Esto se debió a que el depósito S3 de destino aplicaba automáticamente `"ContentType": "application/octet-stream"` los metadatos al objeto cuando lo DataSync transfería allí.

Ejemplo de registro de modo mejorado

```
{
  "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"
}
```

Acción que debe ejecutarse

Para evitar este error, actualice los objetos de ubicación de origen para incluir la propiedad de Content-Type metadatos.

Comprenda la duración de la verificación de datos

DataSync La verificación incluye una SHA256 suma de verificación del contenido de los archivos y una comparación exacta de los metadatos de los archivos entre las distintas ubicaciones. La duración de la verificación depende de varios factores, como la cantidad de archivos u objetos involucrados, el tamaño de los datos de los sistemas de almacenamiento y el rendimiento de estos sistemas.

Acción que debe ejecutarse

Dados los factores que pueden afectar al tiempo de verificación, no debería tener que hacer nada. Sin embargo, si la ejecución de su tarea parece estar atascada con un estado de [verificación](#), póngase en contacto con el [AWS Support Centro](#).

Solución de problemas con costes de almacenamiento en S3 superiores a los esperados con DataSync

Si sus costos de almacenamiento en Amazon S3 son más altos de lo que pensaba tras una transferencia de AWS DataSync , es posible que se deba a uno o varios de los siguientes motivos:

- Al realizar transferencias hacia o desde los depósitos de S3, se incurre en costes relacionados con las solicitudes de API de S3 realizadas por DataSync
- DataSync utiliza la función de carga multiparte de Amazon S3 para cargar objetos en buckets de S3. Este método puede dar lugar a cargos de almacenamiento inesperados para las cargas que no se completan correctamente.
- El control de versiones de objetos puede estar habilitado en el bucket de S3. El control de versiones da lugar a que Amazon S3 almacene varias copias de objetos que tienen el mismo nombre.

Acciones que ejecutar

En estos casos, puede seguir estos pasos:

- Asegúrese de entender cómo DataSync utiliza las solicitudes de S3 y cómo pueden afectar a sus costes de almacenamiento. Para obtener más información, consulte [Evaluar los costos de las solicitudes de S3 al usar DataSync](#).
- Si el problema está relacionado con las cargas multiparte, configure una política de cargas multiparte para el bucket de S3 con el fin de depurar las cargas multiparte incompletas y reducir el costo de almacenamiento. Para obtener más información, consulte la entrada del AWS blog [S3 Lifecycle Management Update: Support for Multipart Uploads and Delete Markers](#).
- Si el problema está relacionado con el control de versiones de objetos, desactive el control de versiones de objetos en su bucket S3.
- [Si necesita más ayuda, póngase en contacto con el Centro de AWS Support](#).

AWS DataSync tutoriales

Estos tutoriales le guían a través de algunos escenarios del mundo real con AWS DataSync.

Temas

- [Tutorial: Transferencia de datos del almacenamiento local a Amazon S3 a través de Cuentas de AWS](#)
- [Tutorial: Transferencia de datos entre depósitos de Amazon S3 Cuentas de AWS](#)

Tutorial: Transferencia de datos del almacenamiento local a Amazon S3 a través de Cuentas de AWS

Cuando se usa AWS DataSync con almacenamiento local, normalmente se transfieren datos a un servicio AWS de almacenamiento que pertenece al Cuenta de AWS mismo que su agente. DataSync Sin embargo, hay situaciones en las que es posible que necesite transferir datos a un bucket de Amazon S3 asociado a una cuenta diferente.

Important

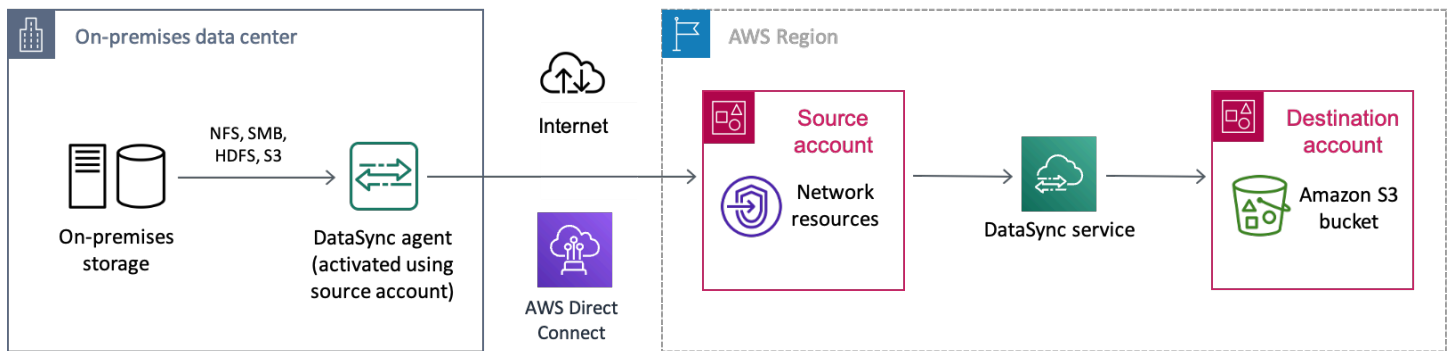
La transferencia de datos Cuentas de AWS mediante los métodos de este tutorial solo funciona cuando Amazon S3 es una de las ubicaciones de DataSync transferencia.

Descripción general

No es raro tener que transferir datos entre diferentes equipos Cuentas de AWS, especialmente si tiene equipos independientes que administran los recursos de su organización. Así es como DataSync puede ser una transferencia entre cuentas mediante el uso de:

- Cuenta de origen: la que se utiliza Cuenta de AWS para administrar los recursos de la red. Esta es la cuenta con la que activas a tu DataSync agente.
- Cuenta de destino: la que se utiliza Cuenta de AWS para administrar el depósito de S3 al que necesita transferir los datos.

En el siguiente diagrama se ilustra este tipo de escenario.



Requisito previo: permisos de cuenta de origen necesarios

Para su fuente Cuenta de AWS, hay dos conjuntos de permisos que debe tener en cuenta en este tipo de transferencia entre cuentas:

- Permisos de usuario que permiten a un usuario trabajar con ellos DataSync (puede ser usted o su administrador de almacenamiento). Estos permisos le permiten crear DataSync ubicaciones y tareas.
- DataSync permisos de servicio que permiten DataSync transferir datos al depósito de cuentas de destino.

User permissions

En su cuenta de origen, añada al menos los siguientes permisos a un rol de IAM para crear sus DataSync ubicaciones y tareas. Para obtener información sobre cómo añadir permisos a un rol, consulte [creación](#) o [modificación](#) de un rol de 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 los permisos de usuario, considere [AWSDataSyncFullAccess](#) utilizarlos. Se trata de una política AWS gestionada que proporciona al usuario un acceso total DataSync y mínimo a sus dependencias.

DataSync service permissions

El DataSync servicio necesita los siguientes permisos en la cuenta de origen para transferir los datos al depósito de cuentas de destino.

Más adelante en este tutorial, añadirá estos permisos al [crear un rol de IAM](#) para DataSync. También debe especificar este rol (*source-datasync-role*) en su [política de segmentos de destino](#) y al [crear su ubicación 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/*"
    }
  ]
}
```

Requisito previo: permisos de cuenta de destino obligatorios

En tu cuenta de destino, tus permisos de usuario deben permitirte actualizar la política del depósito de destino e inhabilitar sus listas de control de acceso (ACLs). Para obtener más información sobre estos permisos específicos, consulte la [Guía del usuario de Amazon S3](#).

Paso 1: En tu cuenta de origen, crea un DataSync agente

Para empezar, debe crear un DataSync agente que pueda leer el contenido de su sistema de almacenamiento local y comunicarse con el DataSync servicio. Este proceso incluye la implementación de un agente en su entorno de almacenamiento en las instalaciones y la activación del agente en su origen Cuenta de AWS.

Note

Los pasos de este tutorial se aplican a cualquier tipo de agente y punto de conexión de servicio que utilice.

Para crear un agente DataSync

1. [Implemente un DataSync agente](#) en su entorno de almacenamiento local.
2. [Elija un punto final de servicio](#) con AWS el que el agente se comunicará.
3. [Active su agente](#) en su cuenta de origen.

Paso 2: En su cuenta de origen, cree un rol de DataSync IAM para acceder al bucket de destino

En tu cuenta de origen, necesitas un rol de IAM que te dé DataSync los permisos para transferir datos al depósito de tu cuenta de destino.

Como vas a realizar transferencias entre cuentas, debes crear el rol manualmente. (DataSync puede crear este rol en la consola si lo transfieres a la misma cuenta).

Cree el rol DataSync de IAM

Cree un rol de IAM DataSync como entidad de confianza.

Creación del rol de IAM

1. Inicie sesión en el AWS Management Console con su cuenta de origen.
2. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
3. En el panel de navegación situado a la izquierda, en Administración de acceso, elija Roles y luego Crear rol.

4. En la página Seleccionar entidad de confianza, en Tipo de entidad de confianza, elija Servicio de AWS.
5. En Caso de uso, elige una opción DataSync en la lista desplegable y selecciona DataSync. Elija Siguiente.
6. En la página Agregar permisos, elija Siguiente.
7. Introduzca un nombre de rol y elija Crear rol.

Para obtener más información, consulte [Crear un rol para un Servicio de AWS \(consola\)](#) en la Guía del usuario de IAM.

Añada permisos al rol de DataSync IAM

El rol de IAM que acaba de crear necesita los permisos que permiten transferir datos DataSync al bucket de S3 de su cuenta de destino.

Para añadir permisos a su rol de IAM

1. En la página Roles de la consola de IAM, busque el rol que acaba de crear y seleccione el nombre.
2. En la página de detalles del rol, elija la pestaña Permisos. Elija Agregar permisos y luego Crear política insertada.
3. Elija la pestaña JSON y haga lo siguiente:
 - a. Pegue el siguiente JSON en el editor de políticas:

Note

El valor de `aws:ResourceAccount` debe ser el ID de cuenta propietario del bucket de Amazon S3 especificado en la 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. Reemplace cada instancia de *amzn-s3-demo-destination-bucket* por el nombre del bucket de S3 de su cuenta de destino.
4. Elija Siguiente. Escriba un nombre para la política y elija Crear política.

Paso 3: en su cuenta de destino, actualice su política de buckets de S3

En su cuenta de destino, modifique la política de buckets de S3 de destino para incluir el [rol de DataSync IAM](#) que creó en su cuenta de origen.

Antes de empezar: asegúrese de tener los [permisos necesarios para su cuenta de destino](#).

Cómo actualizar la política de bucket de S3 de destino

1. En el AWS Management Console, cambia a tu cuenta de destino.
2. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
3. En el panel de navegación situado a la izquierda, elija Buckets.
4. En la lista Buckets, elija el bucket de S3 al que va a transferir los datos.
5. En la página de detalles del bucket, elija la pestaña Permisos.
6. En Política de buckets, seleccione Editar y haga lo siguiente para modificar su política de bucket de S3:
 - a. Actualice lo que hay en el editor para incluir las siguientes declaraciones 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. Sustituya cada instancia de *source-account* por el ID de Cuenta de AWS de su cuenta de origen.
 - c. *source-datasync-role* Sustitúyala por la [función de IAM para la que creaste DataSync en tu cuenta de origen](#).
 - d. Reemplace cada instancia de *amzn-s3-demo-destination-bucket* por el nombre del bucket de S3 de su cuenta de destino.
7. Seleccione Save changes (Guardar cambios).

Paso 4: En tu cuenta de destino, inhabilita tu bucket ACLs de S3

Es importante que todos los datos que copie en el bucket de S3 pertenezcan a su cuenta de destino. Para asegurarte de que esta cuenta es la propietaria de los datos, desactiva las listas de control de acceso del bucket (ACLs). Para obtener más información, consulte [Controlar la propiedad de los objetos y deshabilitar ACLs su bucket](#) en la Guía del usuario de Amazon S3.

ACLs Para inhabilitarlo en su bucket de destino

1. Mientras esté conectado en la consola de S3 con su cuenta de destino, elija el bucket de S3 al que va a transferir los datos.
2. En la página de detalles del bucket, elija la pestaña Permisos.
3. En Propiedad de objeto, elija Editar.
4. Si aún no está seleccionada, elige la opción ACLs deshabilitada (recomendada).
5. Seleccione Save changes (Guardar cambios).

Paso 5: En tu cuenta de origen, crea una ubicación de DataSync origen para tu almacenamiento local

En tu cuenta de origen, crea una [ubicación de DataSync origen](#) para el sistema de almacenamiento local desde el que vas a transferir los datos. Esta ubicación usa el [agente que acaba de activar](#) en su cuenta de origen.

Paso 6: En tu cuenta de origen, crea una ubicación de DataSync destino para tu bucket de S3

Aún en su cuenta de origen, cree una ubicación para el bucket de S3 al que transfiere los datos.

Antes de empezar: asegúrese de tener los [permisos necesarios para su cuenta de origen](#).

Como no puede crear ubicaciones entre cuentas mediante la interfaz de la DataSync consola, estas instrucciones requieren que ejecute un `create-location-s3` comando para crear la ubicación de destino. Recomendamos ejecutar el comando mediante AWS CloudShell un shell preautenticado y basado en un navegador que se inicie directamente desde la consola. CloudShell permite ejecutar AWS CLI comandos `create-location-s3` sin necesidad de descargar ni instalar herramientas de línea de comandos.

Note

Para completar los siguientes pasos con una herramienta de línea de comandos que no sea CloudShell, asegúrese de que su [AWS CLI perfil](#) utilice la misma función de IAM que incluye los [permisos de usuario necesarios](#) para utilizarla DataSync en su cuenta de origen.

Para crear una ubicación de DataSync destino mediante CloudShell

1. Mientras estés en tu cuenta de origen, realiza una de las siguientes acciones para CloudShell iniciarla desde la consola:
 - Selecciona el CloudShell icono de la barra de navegación de la consola. Se encuentra a la derecha del cuadro de búsqueda.
 - Utilice el cuadro de búsqueda de la barra de navegación de la consola para buscar CloudShelly, a continuación, seleccionar la CloudShellopción.
2. Copie el siguiente 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. Sustituya *amzn-s3-demo-destination-bucket* por el nombre del bucket de S3 en su cuenta de destino.
4. Sustituya *source-user-account* por el ID de Cuenta de AWS de su cuenta de origen.
5. *source-datasync-role* Sustitúyala por la [función de DataSync IAM](#) que creaste en tu cuenta de origen.
6. Ejecute el comando en CloudShell.

Si el comando devuelve un ARN de DataSync ubicación similar a este, la ubicación se ha creado correctamente:

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
abcdef01234567890"
}
```

7. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones.

En su cuenta de origen, puede ver la ubicación de S3 que acaba de crear para el bucket de la cuenta de destino.

Paso 7: En su cuenta de origen, cree e inicie DataSync la tarea

Antes de iniciar una DataSync tarea para transferir tus datos, recapitulemos lo que has hecho hasta ahora:

- En tu cuenta de origen, creaste tu DataSync agente. El agente puede leer el contenido de su sistema de almacenamiento local y comunicarse con el DataSync servicio.
- En su cuenta de origen, creó un rol de IAM que permite transferir datos DataSync al depósito de S3 de su cuenta de destino.
- En su cuenta de destino, configuró su bucket de S3 para DataSync poder transferirle datos.
- En su cuenta de origen, creó las ubicaciones de DataSync origen y destino de la transferencia.

Para crear e iniciar la DataSync tarea

1. Mientras sigues usando la DataSync consola de tu cuenta de origen, expande Transferencia de datos en el panel de navegación izquierdo y, a continuación, selecciona Tareas y Crear tarea.

2. En la página Configurar ubicación de origen elija Elegir una ubicación existente. Elija la ubicación de origen desde la que va a copiar los datos (su almacenamiento en las instalaciones) y, luego, Siguiente.
3. En la página Configurar la ubicación de destino, seleccione Elegir una ubicación existente. Elija la ubicación de destino a la que va a copiar los datos (el bucket de S3 de su cuenta de destino) y, a continuación, Siguiente.
4. En la página Configurar los ajustes, asigne un nombre a la tarea. Según sea necesario, configure ajustes adicionales, como especificar un grupo de CloudWatch registros de Amazon. Elija Siguiente.
5. En la página Revisar, revise los ajustes y seleccione Crear tarea.
6. En la página de detalles de la tarea, elija Iniciar y, a continuación, elija una de las siguientes acciones:
 - Para ejecutar la tarea sin modificarla, seleccione Comenzar con los valores predeterminados.
 - Para modificar la tarea antes de ejecutarla, elija Comenzar con las opciones principales.

Cuando finalice la tarea, compruebe el bucket de S3 en su cuenta de destino. Debería ver los datos que se movieron desde la ubicación de origen.

Recursos relacionados

Para obtener más información sobre lo que hizo en este tutorial, consulte los siguientes temas:

- [Crear un rol para un Servicio de AWS \(consola\)](#)
- [Modificación de una política de confianza de rol \(consola\)](#)
- [Incorporación de una política de bucket mediante la consola de Amazon S3](#)
- [Cree una ubicación de S3 con AWS CLI](#)

Tutorial: Transferencia de datos entre depósitos de Amazon S3 Cuentas de AWS

Con AWS DataSync, puede transferir datos entre depósitos de Amazon S3 que pertenezcan a diferentes Cuentas de AWS.

⚠ Important

La transferencia de datos Cuentas de AWS mediante los métodos de este tutorial solo funciona con Amazon S3. Además, este tutorial puede ayudarlo a transferir datos entre buckets de S3 que también se encuentran en diferentes Regiones de AWS.

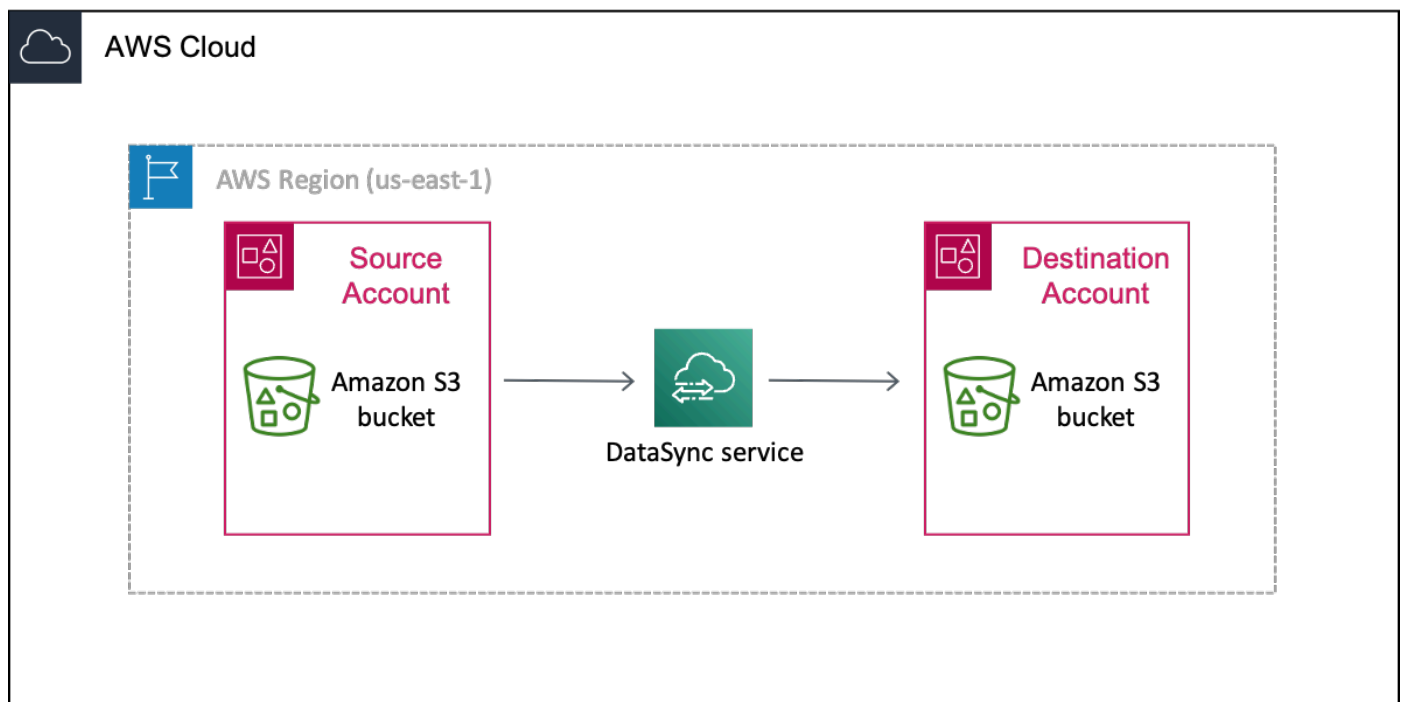
Descripción general

No es raro que se transfieran datos de un lugar a otro Cuentas de AWS, especialmente si tiene equipos independientes que administran los recursos de su organización. Así es como DataSync puede ser una transferencia entre cuentas mediante:

- Cuenta de origen: la que se utiliza Cuenta de AWS para gestionar el depósito de S3 desde el que se deben transferir los datos.
- Cuenta de destino: la que se utiliza Cuenta de AWS para administrar el depósito de S3 al que necesita transferir los datos.

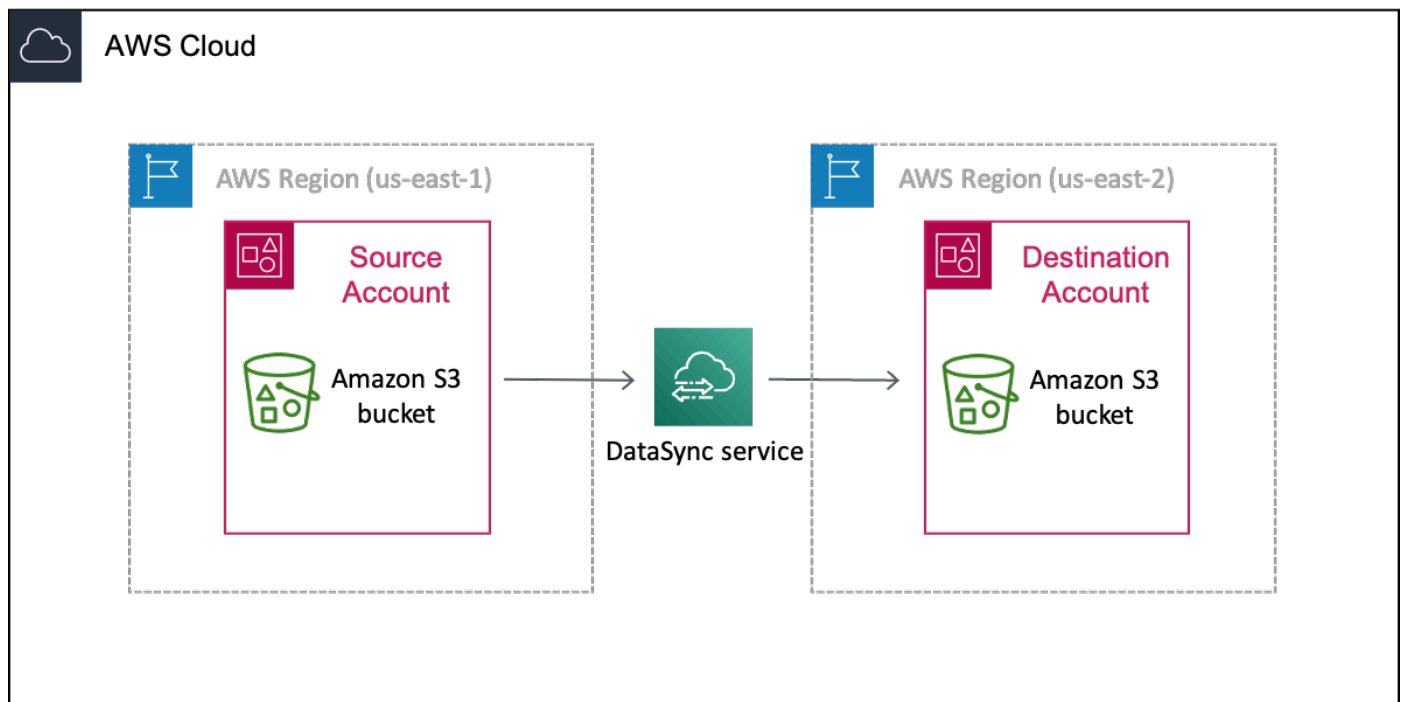
Transfers across accounts

El siguiente diagrama muestra un escenario en el que se transfieren datos de un bucket de S3 a otro bucket de S3 que se encuentra en una Cuenta de AWS diferente.



Transfers across accounts and Regions

El siguiente diagrama ilustra un escenario en el que se transfieren datos de un depósito de S3 a otro depósito de S3 que se encuentra en una región Cuenta de AWS AND diferente.



Requisito previo: permisos de cuenta de origen necesarios

Para tu fuente Cuenta de AWS, hay dos conjuntos de permisos que debes tener en cuenta a la hora de realizar este tipo de transferencia entre cuentas:

- Permisos de usuario que permiten a un usuario trabajar con ellos DataSync (puede ser usted o su administrador de almacenamiento). Estos permisos le permiten crear DataSync ubicaciones y tareas.
- DataSync permisos de servicio que permiten DataSync transferir datos al depósito de cuentas de destino.

Permisos de usuario para su cuenta de origen

En su cuenta de origen, añada al menos los siguientes permisos a un rol de IAM para crear sus DataSync ubicaciones y tareas. Para obtener información sobre cómo añadir permisos a un rol, consulte [creación](#) o [modificación](#) de un rol de 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"
          ]
        }
      }
    }
  ]
}
```

```
}
```

Tip

Para configurar los permisos de usuario, considere [AWSDataSyncFullAccess](#) utilizarlos. Se trata de una política AWS gestionada que proporciona al usuario un acceso total DataSync y mínimo a sus dependencias.

DataSync permisos de servicio para su cuenta de origen

El DataSync servicio necesita los siguientes permisos en tu cuenta de origen para transferir datos al depósito de cuentas de destino.

Más adelante en este tutorial, añadirá estos permisos al [crear un rol de IAM](#) para DataSync. También debe especificar este rol (*source-datasync-role*) en su [política de segmentos de destino](#) y al [crear su ubicación 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/*"
    }
  ]
}
```

Requisito previo: permisos de cuenta de destino obligatorios

En tu cuenta de destino, tus permisos de usuario deben permitirte actualizar la política del depósito de destino e inhabilitar sus listas de control de acceso (ACLs). Para obtener más información sobre estos permisos específicos, consulte la [Guía del usuario de Amazon S3](#).

Paso 1: En tu cuenta de origen, crea un rol de DataSync IAM para el acceso al bucket de destino

En tu fuente Cuenta de AWS, necesitas un rol de IAM que te dé DataSync los permisos para transferir datos al depósito de tu cuenta de destino.

Como vas a realizar transferencias entre cuentas, debes crear la función manualmente. (DataSync puede crearte este rol en la consola al transferirlo a la misma cuenta).

Cree el rol DataSync de IAM

Cree un rol de IAM DataSync como entidad de confianza.

1. Inicie sesión en el AWS Management Console con su cuenta de origen.
2. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
3. En el panel de navegación situado a la izquierda, en Administración de acceso, elija Roles y luego Crear rol.
4. En la página Seleccionar entidad de confianza, en Tipo de entidad de confianza, elija Servicio de AWS.
5. En Caso de uso, elige una opción DataSync en la lista desplegable y selecciona DataSync. Elija Siguiente.
6. En la página Agregar permisos, elija Siguiente.
7. Introduzca un nombre de rol y elija Crear rol.

Para obtener más información, consulte [Crear un rol para una Servicio de AWS \(consola\)](#) en la Guía del usuario de IAM.

Añada permisos al rol de DataSync IAM

El rol de IAM que acaba de crear necesita los permisos que permiten transferir datos DataSync al bucket de S3 de su cuenta de destino.

1. En la página Roles de la consola de IAM, busque el rol que acaba de crear y seleccione el nombre.
2. En la página de detalles del rol, elija la pestaña Permisos. Elija Agregar permisos y luego Crear política insertada.
3. Elija la pestaña JSON y haga lo siguiente:
 - a. Pegue el siguiente JSON en el editor de políticas:

Note

El valor de `aws:ResourceAccount` debe ser el ID de cuenta propietario del bucket de Amazon S3 especificado en la 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. Reemplace cada instancia de *amzn-s3-demo-destination-bucket* por el nombre del bucket de S3 de su cuenta de destino.
4. Elija Siguiente. Escriba un nombre para la política y elija Crear política.

Paso 2: en su cuenta de destino, actualice su política de buckets de S3

En su cuenta de destino, modifique la política de buckets de S3 de destino para incluir el [rol de DataSync IAM](#) que creó en su cuenta de origen.

Antes de empezar: asegúrese de tener los [permisos necesarios para su cuenta de destino](#).

actualizar la política de bucket de S3 de destino

1. En el AWS Management Console, cambia a tu cuenta de destino.
2. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
3. En el panel de navegación situado a la izquierda, elija Buckets.
4. En la lista Buckets, elija el bucket de S3 al que va a transferir los datos.

5. En la página de detalles del bucket, elija la pestaña Permisos.
6. En Política de buckets, seleccione Editar y haga lo siguiente para modificar su política de bucket de S3:
 - a. Actualice lo que hay en el editor para incluir las siguientes declaraciones 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. Sustituya cada instancia *source-account* de por el Cuenta de AWS ID de su cuenta de origen.
- c. *source-datasync-role* Sustitúyala por la [función de IAM para la que creaste DataSync en tu cuenta de origen](#).
- d. Reemplace cada instancia de *amzn-s3-demo-destination-bucket* por el nombre del bucket de S3 de su cuenta de destino.

7. Seleccione Save changes (Guardar cambios).

Paso 3: En tu cuenta de destino, inhabilita tu bucket ACLs de S3

Es importante que todos los datos que transfiera al bucket de S3 pertenezcan a su cuenta de destino. Para asegurarte de que esta cuenta es la propietaria de los datos, desactiva las listas de control de acceso del bucket (ACLs). Para obtener más información, consulte [Controlar la propiedad de los objetos y deshabilitar ACLs su bucket](#) en la Guía del usuario de Amazon S3.

Antes de empezar: asegúrese de tener los [permisos necesarios para su cuenta de destino](#).

Inhabilite el bucket de S3 de destino ACLs

1. Mientras esté conectado en la consola de S3 con su cuenta de destino, elija el bucket de S3 al que va a transferir los datos.
2. En la página de detalles del bucket, elija la pestaña Permisos.
3. En Propiedad de objeto, elija Editar.
4. Si aún no está seleccionada, elige la opción ACLs deshabilitada (recomendada).
5. Seleccione Save changes (Guardar cambios).

Paso 4: En tu cuenta de origen, crea tus DataSync ubicaciones

En su cuenta de origen, cree las DataSync ubicaciones para los buckets S3 de origen y destino.

Antes de empezar: asegúrese de tener los [permisos necesarios para su cuenta de origen](#).

Cree su ubicación DataSync de origen

- En su cuenta de origen, cree una [ubicación](#) para el bucket de S3 desde el que transfiere los datos.

Crea tu ubicación de DataSync destino

Aún en su cuenta de origen, cree una ubicación para el bucket de S3 al que transfiere los datos.

Como no puede crear ubicaciones entre cuentas mediante la interfaz de la DataSync consola, estas instrucciones requieren que ejecute un `create-location-s3` comando para crear la ubicación de destino. Recomendamos ejecutar el comando mediante AWS CloudShell un shell preautenticado y basado en un navegador que se inicie directamente desde la consola. CloudShell permite ejecutar

AWS CLI comandos `create-location-s3` sin necesidad de descargar ni instalar herramientas de línea de comandos.

 Note

Para completar los siguientes pasos con una herramienta de línea de comandos que no sea CloudShell, asegúrese de que su [AWS CLI perfil](#) utilice la misma función de IAM que incluye los [permisos de usuario necesarios](#) para utilizarla DataSync en su cuenta de origen.

Para crear una ubicación de DataSync destino mediante CloudShell

1. Mientras estés en tu cuenta de origen, realiza una de las siguientes acciones para CloudShell iniciarla desde la consola:
 - Selecciona el CloudShell icono de la barra de navegación de la consola. Se encuentra a la derecha del cuadro de búsqueda.
 - Utilice el cuadro de búsqueda de la barra de navegación de la consola para buscar CloudShelly, a continuación, seleccionar la CloudShellopción.
2. Copie el siguiente 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. Sustituya *amzn-s3-demo-destination-bucket* por el nombre del bucket de S3 en su cuenta de destino.
4. Si el bucket de destino se encuentra en una región diferente a la del bucket de origen, reemplace *amzn-s3-demo-destination-bucket-region* por la región en la que reside el bucket de destino (por ejemplo, *us-east-2*). Elimine esta opción si los buckets están en la misma región.
5. *source-account-id* Sustitúyala por la Cuenta de AWS ID de origen.
6. *source-datasync-role* Sustitúyalo por el [rol de DataSync IAM](#) que creaste en tu cuenta de origen.

7. Ejecute el comando en CloudShell.

Si el comando devuelve un ARN de DataSync ubicación similar a este, la ubicación se ha creado correctamente:

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:123456789012:location/loc-
abcdef01234567890"
}
```

8. En el panel de navegación situado a la izquierda, expanda Transferencia de datos y, a continuación, seleccione Ubicaciones.
9. Si creó la ubicación en una región diferente, elija esa región en el panel de navegación.

En su cuenta de origen, puede ver la ubicación de S3 que acaba de crear para el bucket de la cuenta de destino.

Paso 5: En su cuenta de origen, cree e inicie DataSync la tarea

Antes de iniciar una DataSync tarea para transferir tus datos, recapitulemos lo que has hecho hasta ahora:

- En su cuenta de origen, creó un rol de IAM que permite transferir datos DataSync al bucket de S3 de su cuenta de destino.
- En su cuenta de destino, configuró su bucket de S3 para DataSync poder transferirle datos.
- En su cuenta de origen, creó las ubicaciones de DataSync origen y destino de la transferencia.

Crea e inicia tu DataSync tarea

1. Mientras sigues usando la DataSync consola de tu cuenta de origen, expande Transferencia de datos en el panel de navegación izquierdo y, a continuación, selecciona Tareas y Crear tarea.
2. Si el bucket de su cuenta de destino se encuentra en una región diferente a la del bucket de su cuenta de origen, seleccione la región del bucket de destino en el panel de navegación superior.

 Important

Para evitar un error de conexión a la red, debes crear la DataSync tarea en la misma región que la ubicación de destino.

3. En la página Configurar ubicación de origen, haga lo siguiente:
 - a. Seleccione Elegir una ubicación existente.
 - b. (Para transferencias entre regiones) En el menú desplegable Región, seleccione la región en la que reside el bucket de origen.
 - c. En Ubicaciones existentes, elija la ubicación de origen del bucket de S3 desde el que está transfiriendo los datos y, a continuación, seleccione Siguiente.
4. En la página Configurar ubicación de destino, haga lo siguiente:
 - a. Seleccione Elegir una ubicación existente.
 - b. En Ubicaciones existentes, elija la ubicación de destino del bucket de S3 al que está transfiriendo los datos y, a continuación, seleccione Siguiente.
5. En la página Configurar ajustes, elija un modo de tarea.

 Tip

Se recomienda utilizar el modo mejorado. Para obtener más información, consulte [Elegir un modo de tarea para la transferencia de datos](#).

6. Asigne un nombre a la tarea y configure ajustes adicionales, como especificar un grupo de CloudWatch registros de Amazon. Elija Siguiente.
7. En la página Revisar, revise los ajustes y seleccione Crear tarea.
8. En la página de detalles de la tarea, elija Iniciar y, a continuación, elija una de las siguientes acciones:
 - Para ejecutar la tarea sin modificarla, seleccione Comenzar con los valores predeterminados.
 - Para modificar la tarea antes de ejecutarla, elija Comenzar con las opciones principales.

Cuando finalice la tarea, compruebe el bucket de S3 en su cuenta de destino. Debería ver los datos que se movieron desde el bucket de su cuenta de origen.

Solución de problemas

Consulta la siguiente información si tienes problemas al intentar completar la transferencia entre cuentas.

Errores de conexión

Al realizar transferencias entre depósitos de S3 en tareas distintas Cuentas de AWS o de regiones con el modo Básico, es posible que se produzca un error de conexión de red al iniciar la DataSync tarea. Para solucionar este problema, usa una tarea en modo mejorado. Como alternativa, cree una tarea en modo básico en la misma región que su ubicación de destino e intente ejecutar esa tarea.

Relacionado: Transferencias entre cuentas con buckets de S3 mediante el cifrado del servidor

Si intenta realizar esta transferencia con buckets de S3 mediante el cifrado del lado del servidor, consulta el [blog sobre almacenamiento de AWS](#) para obtener instrucciones.

Realizar una migración de datos de gran tamaño con AWS DataSync

Las migraciones de datos a gran escala pueden implicar la transferencia de volúmenes importantes de datos que abarcan millones de archivos u objetos en varios formatos. AWS DataSync simplifica estas transferencias complejas al gestionar la programación, la supervisión, el cifrado y la verificación de los datos.

¿Qué es una migración de datos de gran tamaño?

Por lo general, una migración de datos de gran tamaño implica la transferencia de terabytes o más de datos distribuidos en varias fuentes a un nuevo entorno de almacenamiento de destino (en este caso, AWS). Estas migraciones requieren una planificación y una coordinación cuidadosas dentro de la organización para transferir los datos con éxito y, al mismo tiempo, minimizar las interrupciones del negocio.

DataSync puede simplificar estas migraciones, que suelen ser de naturaleza compleja. Algunas de las ventajas de utilizarlas DataSync para la migración son las siguientes:

- Administración automatizada de los procesos de transferencia de datos y de la infraestructura necesaria para una transferencia de datos segura y de alto rendimiento.
- End-to-end seguridad, que incluye el cifrado y la validación de la integridad de los datos, para garantizar que sus datos lleguen de forma segura, intacta y lista para su uso.
- Un protocolo de red diseñado específicamente y una arquitectura paralela de subprocesos múltiples para acelerar las migraciones.

Etapas clave de una migración de datos de gran tamaño

Por lo general, puede dividir una migración grande en las siguientes etapas:

- (Etapas 1) Planear la migración de datos: en esta etapa, está intentando entender por qué está migrando y con qué tipo de datos está trabajando. Las actividades de planificación incluyen:
 - Entender por qué quiere migrar
 - Reunir un equipo que le ayude con todos los aspectos de la migración.

- Identificar las ubicaciones, los formatos y los patrones de uso de los datos
- Evaluar los recursos de hardware disponibles y los requisitos de red (si va a migrar desde un centro de datos local)
- Realice pruebas de concepto (POC) DataSync para estimar los plazos de migración, planificar los plazos de transición y hacerse una idea de cómo debe configurarse DataSync
- (Etapa 2) Implementación de la migración de datos de gran tamaño: en este punto, está validando su plan e iniciando la migración. Las actividades de implementación incluyen:
 - Validar el plan de migración
 - Ejecutar transiciones escalonadas que incluyan la supervisión y la verificación de las transferencias de datos según lo previsto
 - Optimizar y ajustar según sea necesario entre cada transición
 - Limpiar los recursos no utilizados una vez que haya terminado

Recursos adicionales

AWS Prescriptive Guidance cuenta con los siguientes recursos que pueden ayudarle a planificar e implementar una migración de gran envergadura. Utilice esta guía para comprender cómo DataSync puede funcionar en el contexto de procesos y actividades de migración comunes.

- [Grandes migraciones a la nube AWS](#)
- [Estrategia y mejores prácticas para AWS grandes migraciones](#)
- [Migre sistemas de archivos compartidos en una migración AWS grande](#): este recurso incluye un libro de trabajo de SFS-Discovery que puede descargar y usar para planificar una migración a nivel de recurso compartido de archivos.

Etapa 1: Planificar la migración de datos de gran tamaño

La planificación es esencial a la hora de migrar un conjunto de datos grande. Debe comprender los datos que va a migrar, sus motivaciones para la migración y cómo AWS DataSync puede ayudarlo a llevar sus datos a donde los desea.

Temas

- [Recopilación de los requisitos para la migración](#)
- [Realización de una DataSync prueba de concepto](#)

- [Estimación de los plazos de migración](#)

Recopilación de los requisitos para la migración

El primer paso de una migración de datos de gran tamaño requiere recopilar una variedad de información en toda la organización.

Esta información le ayuda a crear un [proceso](#) de migración, que, en el caso de migraciones grandes, puede incluir múltiples transferencias y procedimientos para transferir las operaciones (realizadas en [oleadas](#)) del almacenamiento de origen al de destino.

Comprenda por qué quiere migrar

Antes de poder empezar a migrar a AWS, debe comprender claramente por qué está migrando sus datos. Esto ayuda a abordar los desafíos de migración más comunes, como el cumplimiento de los plazos, la gestión de los recursos y la coordinación entre los equipos.

Si necesitas ayuda para determinar tus motivaciones para la migración, responde a estas preguntas:

- ¿Está liberando espacio de almacenamiento local?
- ¿Cumple con los plazos de los contratos de soporte de hardware?
- ¿Es para la salida de un centro de datos?
- ¿Cuál es su cronograma de migración?
- ¿Está transfiriendo datos desde otro almacenamiento en la nube?
- ¿Está migrando conjuntos de datos parciales o completos?
- ¿Es para archivar datos?
- ¿Necesitan las aplicaciones o los usuarios un acceso regular a estos datos?

Descubriendo la logística

Aborde algunos aspectos de la logística básica relacionados con su entorno de almacenamiento, la migración y su organización:

1. Obtenga una comprensión básica de su infraestructura de almacenamiento de datos actual.
2. Compruebe si necesita un [DataSync agente](#). Por ejemplo, necesitas un agente si vas a realizar la transferencia desde un almacenamiento local.

3. Si necesitas un agente, asegúrate de entender los [requisitos del agente](#):
 - Un agente puede ejecutarse como una máquina virtual (VM) en hipervisores Microsoft Hyper-V VMware ESXi, una máquina virtual basada en el núcleo de Linux (KVM) y una máquina virtual basada en el núcleo de Linux. También puede implementar un agente como una EC2 instancia de Amazon en AWS.
 - Las migraciones grandes suelen consumir mucha memoria. Asegúrese de que su agente tenga suficiente RAM.
4. Identifique a las principales partes interesadas de sus departamentos de liderazgo, redes, almacenamiento y TI que deben participar en la migración. Esto puede incluir:
 - Encuentre un [líder de un solo hilo](#) que se dedique al proyecto y a sus resultados.
 - Determine quién es responsable de la propiedad y la clasificación de los datos que va a migrar.
 - Identifique quién administra su fuente y quién, en última instancia, administrará el servicio de AWS almacenamiento al que está migrando.
 - Descubra quién creará y administrará cualquier otro proceso para sus datos una vez que estén disponibles. AWS
5. Establezca canales de comunicación entre departamentos.
6. Cree un plan de reducción de contingencias.
7. Documente todo el proceso de migración, incluidos los procedimientos de oleada, validación y transición. Utilícelo como manual para toda la migración. Actualizará este proceso a medida que planifique e implemente la migración.

Revisar los datos que va a migrar

Trabaje con sus equipos de almacenamiento y aplicaciones para analizar las características de los datos que va a migrar. Esta información le ayuda a determinar una estrategia de migración con DataSync la que pueda ejecutar.

Contenido

- [Determinar los patrones de uso de datos](#)
- [Identificar la estructura y el diseño de los datos](#)
- [Documentar los recursos compartidos y las carpetas](#)
- [Analizar los tamaños de los archivos](#)

Determinar los patrones de uso de datos

- En el caso de los datos que se utilizan de forma activa y que se modifican con frecuencia, planifique múltiples oleadas de transferencias incrementales para evitar interrumpir las operaciones comerciales.
- En el caso de los datos de solo lectura que puedan considerarse archivados, es posible que no necesite planificar las oleadas.
- Si tiene una combinación de patrones de uso de datos, planifique oleadas que migren estos distintos conjuntos de datos por separado. Por ejemplo, puede tener una oleada para archivar datos y dedicar el resto a la migración de datos activos.

Identificar la estructura y el diseño de los datos

- Determine si los datos están organizados por períodos de tiempo (año, mes, día) u otros patrones.
- Utilice esta estructura organizativa para planificar sus oleadas de migración. Por ejemplo, puede migrar los datos archivados correspondientes a un año de una sola oleada.

Documentar los recursos compartidos y las carpetas

- Cree un inventario de los recursos compartidos y las carpetas (incluidos los recuentos de archivos u objetos de cada uno).
- Identifique los recursos compartidos y las carpetas con conjuntos de datos activos. Es posible que requieran transferencias incrementales durante la migración.
- Revise las [DataSync cuotas](#). Esto puede ayudarle a planificar cómo particionar el conjunto de datos durante la configuración DataSync.

Analizar los tamaños de los archivos

- Espere un mayor rendimiento de datos para las transferencias con archivos más grandes (MB o GB) en comparación con archivos más pequeños (KB).
- Si trabaja con muchos archivos más pequeños, espere más operaciones de metadatos en su sistema de almacenamiento y un menor rendimiento de datos. DataSync realiza estas operaciones al comparar y verificar las ubicaciones de origen y destino.

Identificar los requisitos de almacenamiento

Para elegir un servicio AWS de almacenamiento compatible para migrar sus datos, debe evaluar las características y el rendimiento del sistema de almacenamiento de origen.

Esta información también puede ayudarlo a [programar sus transferencias](#) para minimizar el impacto en las operaciones comerciales durante la migración.

Contenido

- [Determinar el soporte de almacenamiento de origen](#)
- [Revisión de los requisitos de conservación de los metadatos](#)
- [Recopilación de métricas de rendimiento del almacenamiento de origen](#)
- [Elegir un servicio de AWS almacenamiento de destino](#)

Determinar el soporte de almacenamiento de origen

DataSync puede funcionar con una variedad de sistemas de almacenamiento que permiten el acceso a través de clientes de almacenamiento de objetos compatibles con NFS, SMB, HDFS y S3.

Si vas a migrar desde otro almacenamiento en la nube, comprueba que funcione con ese DataSync proveedor. Para obtener una lista de las ubicaciones de origen compatibles, consulta [¿Dónde puedo transferir mis datos con AWS DataSync?](#)

Revisión de los requisitos de conservación de los metadatos

DataSync puede conservar los metadatos del archivo u objeto durante una transferencia. La forma en que se conservan los metadatos depende de las ubicaciones de transferencia y de si esas ubicaciones utilizan tipos de metadatos similares.

DataSync en algunos casos, necesita permisos adicionales para conservar los metadatos de los archivos, como las listas de acceso discrecional de NTFS (DACLs).

Para obtener más información, consulte [Comprenda cómo DataSync gestiona los metadatos de archivos y objetos](#).

Recopilación de métricas de rendimiento del almacenamiento de origen

Mida las IOPS de referencia y el rendimiento del disco durante las cargas de trabajo medias y máximas del almacenamiento de origen. La transferencia de datos añade una sobrecarga de E/S a los sistemas de almacenamiento de origen y destino.

Compare estos datos de rendimiento con las especificaciones de su sistema de almacenamiento para determinar los recursos de rendimiento disponibles.

Elegir un servicio de AWS almacenamiento de destino

En este punto, es posible que tenga una idea de qué servicio de AWS almacenamiento es adecuado para sus datos. Si no es así, los patrones de uso de datos y el rendimiento del almacenamiento son un par de aspectos a tener en cuenta a la hora de tomar una decisión. Por ejemplo, podría considerar Amazon S3 si tiene datos archivados y Amazon FSx o Amazon EFS para los datos activos.

Para ayudarle a decidir cuál es el almacenamiento basado en objetos o archivos adecuado para sus datos, consulte [Elegir un servicio AWS de almacenamiento](#).

Determinar los requisitos de la red

Para migrar sus datos DataSync, debe establecer conexiones de red entre el almacenamiento de origen, el agente y AWS. También debe planificar una infraestructura y un ancho de banda de red suficientes.

Trabaje con sus ingenieros de redes y administradores de almacenamiento para reunir los siguientes requisitos de red.

Contenido

- [Evaluar el ancho de banda de red disponible](#)
- [¿Está considerando las opciones para conectar su red a AWS](#)
- [Elegir un punto final de servicio para la comunicación entre los agentes](#)
- [Planificar una infraestructura de red suficiente](#)

Evaluar el ancho de banda de red disponible

El ancho de banda de red disponible tiene en cuenta las velocidades de transferencia y el tiempo total de migración. Si realizas la transferencia desde un sistema de almacenamiento local, haz lo siguiente:

- Trabaje con su equipo de red para determinar la utilización media y máxima del ancho de banda.
- Identifique los momentos en los que puede transferir datos y evite interrumpir las operaciones diarias. Esto le permitirá saber cuándo se produzcan las oleadas migratorias y las transiciones.

Puede controlar cuánto ancho de banda DataSync utiliza. Para obtener más información, consulte [Configuración de los límites de ancho de banda para la tarea de AWS DataSync](#).

Dado que las transferencias desde otro almacenamiento en la nube suelen realizarse a través de la Internet pública, estas transferencias suelen tener menos restricciones y consideraciones de ancho de banda.

¿Está considerando las opciones para conectar su red a AWS

Ten en cuenta las siguientes opciones para establecer la conectividad de red para tu DataSync transferencia:

- AWS Direct Connect- Revise los [ejemplos de arquitectura y enrutamiento](#) para usar Direct Connect with DataSync. Puedes monitorizar la actividad de Direct Connect a través de [Amazon CloudWatch](#).
- VPN: [AWS Site-to-Site VPN](#) ofrece un rendimiento de hasta 1,25 Gbps por túnel.
- Internet pública: póngase en contacto con su proveedor de servicios de Internet para obtener datos de uso de la red.

Elegir un punto final de servicio para la comunicación entre los agentes

DataSync los agentes utilizan los [puntos finales del servicio](#) para comunicarse con el DataSync servicio. El tipo de punto final que utilice depende de la forma a la que se conecte a AWS la red.

Planificar una infraestructura de red suficiente

Para cada tarea de transferencia que cree, genera y administra DataSync automáticamente la infraestructura de red para sus transferencias de datos. Esta infraestructura se conoce como interfaces de red o interfaces de red elásticas, que son componentes de red lógicos en una nube privada virtual (VPC) de Amazon que representan tarjetas de red virtuales. Para obtener más información, consulta la [Guía del EC2 usuario de Amazon](#).

Cada interfaz de red utiliza una única dirección IP en la subred de VPC de destino. Para asegurarte de que tienes suficiente infraestructura de red para la migración, haz lo siguiente:

- Anote la cantidad de [interfaces de red](#) que DataSync se crearán para su ubicación de DataSync destino.

- Asegúrese de que la subred tenga suficientes direcciones IP para sus DataSync tareas. Por ejemplo, una tarea que utiliza un agente requiere cuatro direcciones IP. Si crea cuatro tareas para la migración, significa que necesita 16 direcciones IP disponibles en la subred.

Realización de una DataSync prueba de concepto

La ejecución de una prueba de concepto (POC) le AWS DataSync ayuda a validar los siguientes aspectos de la planificación de la migración de datos:

- Verifique la conectividad de red entre las ubicaciones de origen y destino.
- Valide la configuración inicial de la DataSync tarea.
- Mida el rendimiento de la transferencia de datos.
- Calcule los plazos de migración.
- Defina los criterios de éxito con las principales partes interesadas que trabajan en la migración.

Cómo empezar con su prueba de concepto

1. Crea tu DataSync agente:

1. [Despliega a tu agente.](#)
2. [Elija un punto final de servicio](#) para su agente.
3. [Activación del agente.](#)
4. [Verifica las conexiones de red de tu agente.](#)

2. Seleccione un subconjunto pequeño de datos que represente los datos que va a migrar.

Por ejemplo, si el almacenamiento de origen tiene una combinación de archivos grandes y pequeños, el subconjunto de datos que transfiera a su POC debería reflejarlo. Esto le proporciona una comprensión preliminar del rendimiento de los sistemas de almacenamiento, su red y DataSync

3. Cree una ubicación DataSync de origen para su sistema de almacenamiento [local](#) u [otro sistema de almacenamiento en la nube](#).
4. Cree una ubicación de DataSync destino para su [servicio AWS de almacenamiento](#).
5. [Cree una tarea DataSync de transferencia](#) con un [filtro](#) que solo transfiera su subconjunto de datos.
6. [Comience su DataSync tarea.](#)

7. Recopile las métricas del rendimiento de las transferencias supervisando lo siguiente:
 - El rendimiento de los archivos y los datos de la ejecución de sus tareas. Puede hacerlo a través de la DataSync consola o de la [DescribeTaskExecution](#) operación. Si las usas `DescribeTaskExecution`, estas métricas se calculan de la siguiente manera:
 - Rendimiento de datos: divida entre `BytesWritten` `TransferDuration`
 - Rendimiento de archivos: dividir por `FilesTransferred` `TransferDuration`
 - Utilización del almacenamiento de origen y destino. Trabaje en estrecha colaboración con sus administradores de almacenamiento de información para obtener esta información.
 - Uso de la red.
8. Verifique los datos transferidos en su ubicación de destino:
 - Revise sus CloudWatch registros para ver si hay errores en la ejecución de las tareas.
 - Compruebe que los permisos y los metadatos se conservan en la ubicación de destino.
 - Confirme que las aplicaciones y los usuarios puedan acceder a los datos de destino según lo previsto.
 - Solucione cualquier problema que pueda surgir. Para obtener más información, consulte [Solución de AWS DataSync problemas](#).
9. Ejecute la tarea unas cuantas veces más para hacerse una idea del tiempo que lleva DataSync preparar, transferir y verificar los datos. (Para obtener más información, consulte [Estados de ejecución de las tareas](#)).

Si ejecutas una tarea más de una vez, de forma DataSync predeterminada, realiza una transferencia incremental y copia solo los datos que han cambiado con respecto a la ejecución anterior de la tarea.

Si bien es probable que el tiempo de transferencia sea más corto en el caso de las transferencias incrementales, siempre DataSync preparará la transferencia de la misma manera escaneando y comparando las ubicaciones para identificar qué desea transferir. Puedes usar estos tiempos de preparación para [estimar los plazos de transición de](#) tu migración.
10. Si es necesario, actualice su plan de migración en función de lo que haya aprendido durante la POC.

Estimación de los plazos de migración

Con la información que ha recopilado hasta ahora, puede estimar cuánto tiempo llevará la migración.

AWS DataSync

Estimación de los plazos de transferencia de datos

Puede estimar el tiempo que se tarda en DataSync transferir sus datos en función de la siguiente información que recopiló durante la recopilación de los requisitos de migración y de su DataSync prueba de concepto (POC):

- El ancho de banda de [red disponible](#)
- Métricas de utilización del almacenamiento de origen y destino
- Métricas de rendimiento de su [DataSync POC](#)

Para estimar un cronograma de transferencia de datos

1. Compare el rendimiento de datos y archivos de su POC con el ancho de banda de red disponible.
2. Si su rendimiento es inferior al ancho de banda disponible (por ejemplo, 300 MiB/s para un rendimiento con 10 Gbps de ancho de banda de red), considere la posibilidad de dividir el conjunto de datos en varias tareas para maximizar el uso del ancho de banda.

DataSync tiene algunas opciones para particionar el conjunto de datos. Para obtener más información, consulte [Acelera la migración con el particionamiento de datos](#).

3. Calcula el número de días que tarda una transferencia mediante la siguiente fórmula, que proporciona un tiempo de transferencia mínimo teórico:

```
(DATA_SIZE * 8 bits per byte)/(CIRCUIT * NETWORK_UTILIZATION percentage * 3600  
seconds per hour * AVAILABLE_HOURS) = Number of days
```

Cuando utilices esta fórmula, sustituye lo siguiente por tus propios valores:

- DATA_SIZE: la cantidad de datos que está migrando (expresada en bytes).
- CIRCUIT: el ancho de banda de red disponible (expresado en bits por segundo).
- NETWORK_UTILIZATION: Qué porcentaje de la red se está utilizando.
- AVAILABLE_HOURS: El número de horas de funcionamiento disponibles en cada día.

Por ejemplo, calcularía una migración con 100 TB de datos, una conexión a Internet de 1 Gbps, un 80 por ciento de utilización de la red y una disponibilidad de 24 horas al día de la siguiente manera:

$$(100,000,000,000,000 \text{ bytes} * 8) / (1,000,000,000 \text{ bps} * 0.80 * 3600 * 24) = 11.57 \text{ days}$$

En este caso, la migración tardaría casi 12 días en tener en cuenta las condiciones reales.

4. Ajusta la duración de la transferencia calculada para tener en cuenta las condiciones del mundo real:
 - Fluctuaciones del rendimiento de la
 - Variaciones en el rendimiento del almacenamiento
 - Tiempo de inactividad entre oleadas de migración

Estimación de los plazos de transición

Si está migrando conjuntos de datos activos, es probable que necesite transiciones para no interrumpir las operaciones comerciales.

No subestime el tiempo que tardan las transiciones. En el caso de migraciones grandes, no es raro que las actividades de transición ocupen hasta un 30 por ciento del tiempo total de migración.

1. Evalúe si necesita realizar transiciones en oleadas para reducir la cantidad de datos escaneados en busca de cambios incrementales.

Una estrategia para hacerlo consiste en dividir los conjuntos de datos que se particionan en función de recursos compartidos, carpetas o sistemas de almacenamiento.

2. Revisa cuánto tiempo se tarda normalmente en DataSync preparar, transferir y verificar los datos durante la POC.

Tenga en cuenta, en particular, la duración de la preparación de las ejecuciones de sus tareas. Para obtener esta información, ejecute la [DescribeTaskExecution](#) operación y, a continuación, compruebe el valor del [PrepareDuration](#) tiempo de duración (en milisegundos).

3. Calcule cuánto tiempo podría tardar una transición midiendo el delta de tiempo entre tareas paralelas.

Para obtener más información sobre las tareas paralelas, consulte [Acelera la migración con el particionamiento de datos](#).

4. Utilice su estimación de transición para programar las transiciones. Básicamente, se trata de períodos de mantenimiento en los que los datos de origen no se pueden modificar.

Pasos a seguir a continuación

Tras estimar los plazos, estará listo para empezar a implementar la migración.

Etapa 2: Implementación de la migración de datos de gran tamaño

Con la información que recopiló durante la planificación, puede empezar AWS DataSync a utilizarla para migrar a su nuevo sistema de almacenamiento. Si aún no lo ha hecho, le recomendamos que consulte los [recursos de orientación AWS prescriptiva para migraciones grandes](#).

Temas

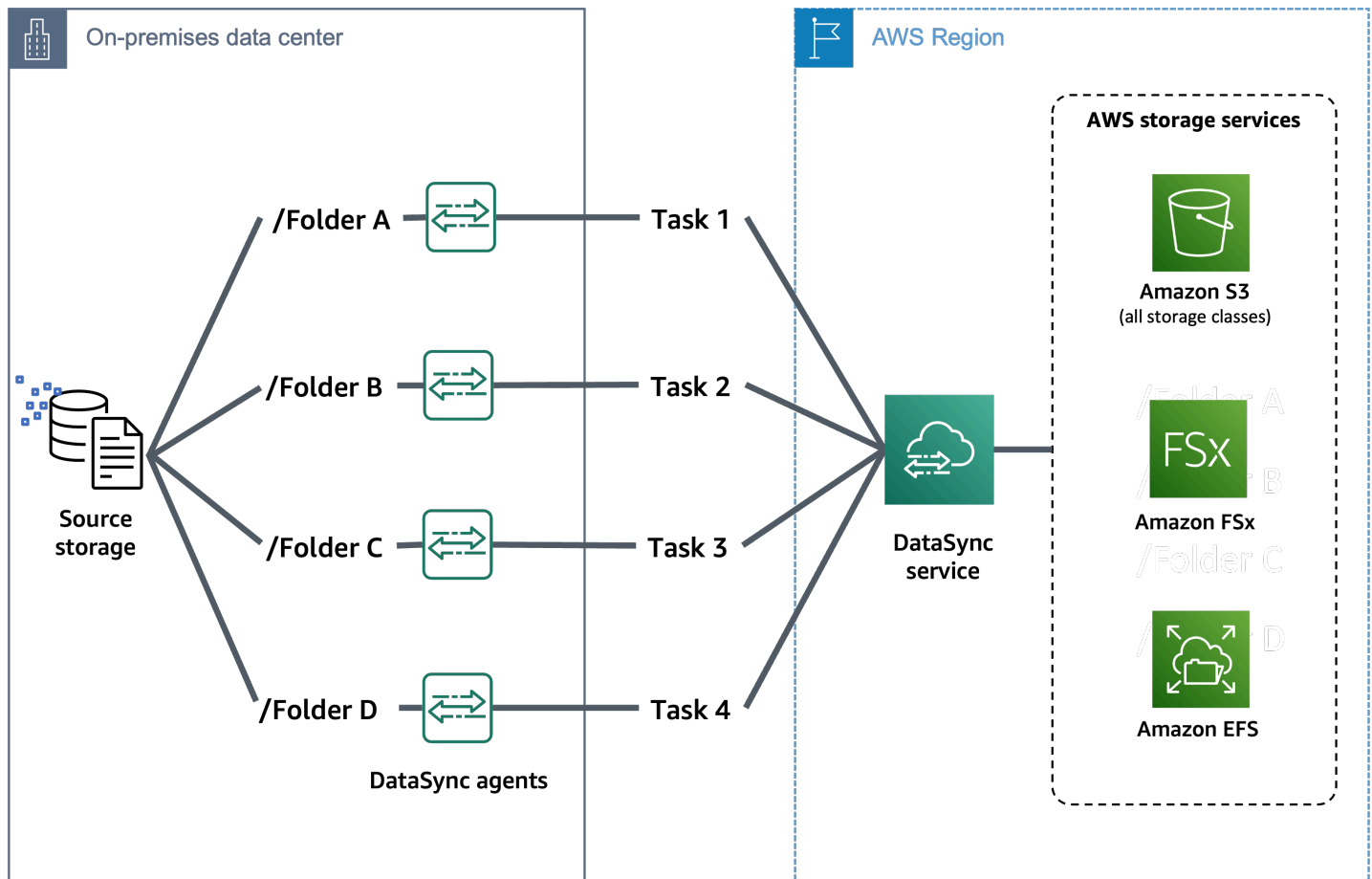
- [Acelera la migración con el particionamiento de datos](#)
- [Ejecutar las tareas DataSync de transferencia](#)
- [Supervisar sus transferencias](#)

Acelera la migración con el particionamiento de datos

En el caso de una migración a gran escala, recomendamos particionar el conjunto de datos con varias DataSync tareas. Dividir los datos de origen en varias tareas (y, posiblemente, en varios agentes) permite paralelizar las transferencias y reducir el tiempo de migración.

La partición también le ayuda a mantenerse dentro de DataSync [las cuotas](#) y simplifica la supervisión y la depuración de sus tareas.

El siguiente diagrama muestra cómo puede utilizar varias DataSync tareas y agentes para transferir datos desde la misma ubicación de almacenamiento de origen. En este escenario, cada tarea se centra en una carpeta específica de la ubicación de origen. Para obtener más información y ejemplos sobre estos enfoques, consulte [Cómo acelerar las transferencias de datos con arquitecturas AWS DataSync escalables](#).



Particionar el conjunto de datos por carpeta o prefijo

Al crear la ubicación DataSync de origen, puedes especificar una carpeta, un directorio o un prefijo desde el que DataSync leer. Por ejemplo, si vas a migrar un recurso compartido de archivos con directorios de nivel superior, puedes crear varias ubicaciones que especifiquen una ruta de directorio diferente. A continuación, puede utilizar estas ubicaciones para ejecutar varias DataSync tareas durante la migración.

Particionar el conjunto de datos con filtros

Puedes aplicar [filtros](#) para incluir o excluir datos de tu ubicación de origen en una transferencia. En el contexto de una migración a gran escala, los filtros pueden ayudarte a limitar las tareas a partes específicas de tu conjunto de datos.

Por ejemplo, si vas a migrar datos archivados organizados por año, puedes crear un filtro de inclusión que se ajuste a un año específico o a varios años. También puedes modificar el filtro cada vez que ejecutes la tarea para que coincida con un año diferente.

Particionar el conjunto de datos con manifiestos

Un [manifiesto](#) es una lista de archivos u objetos que deseas DataSync transferir. Con un manifiesto, DataSync no es necesario leer todo lo que hay en la ubicación de origen para determinar qué se va a transferir.

Puede crear manifiestos a partir de los inventarios de su almacenamiento de origen o mediante enfoques basados en eventos (por ejemplo, consulte [Implementación AWS DataSync con cientos de millones de objetos](#)). También puede usar un manifiesto diferente cada vez que inicie una tarea, lo que le permitirá transferir diferentes conjuntos de datos con la misma tarea.

Ejecutar las tareas DataSync de transferencia

Durante cada oleada de migración, la transferencia de datos suele seguir el mismo proceso general:

1. Realice una transferencia inicial completa de sus datos.
2. Compruebe los datos en el destino.
3. Realice transferencias incrementales para cualquier dato que pueda haber cambiado desde la transferencia inicial.
4. Traslade las operaciones a su ubicación de destino.
5. Revise los resultados de la transición.

Ejecutando tus tareas

Es probable que tengas que ejecutar las tareas de DataSync transferencia durante el horario laboral para minimizar el tiempo total de migración. En estas situaciones, es habitual ejecutar una transferencia inicial completa seguida de transferencias incrementales que tengan en cuenta los cambios en la ubicación de origen por parte de los usuarios y las aplicaciones.

Para evitar problemas relacionados con la red durante el horario laboral, puedes limitar la cantidad de ancho de banda que utilizan tus tareas. Para obtener más información, consulte [Configuración de los límites de ancho de banda para la tarea de AWS DataSync](#).

1. Realiza una transferencia completa inicial:
 - a. [Comienza tu DataSync tarea](#) (o tareas si las ejecutas en paralelo).
 - b. Supervisa el progreso y el rendimiento de la ejecución de tus tareas.

- c. Compruebe que los datos se hayan transferido de la forma esperada (por ejemplo, se conservan los metadatos de los archivos).
2. Ejecute transferencias incrementales:
 - a. [Programa tus tareas](#) para que se ejecuten periódicamente.
 - b. Supervisa la ejecución de tus tareas y corrige los errores si los encuentras.

Realizando una transición

Tras las transferencias iniciales e incrementales, puede iniciar el proceso de traslado de las operaciones a su ubicación de destino.

1. Inicie el período de mantenimiento programado.
2. Actualice su sistema de almacenamiento de origen para que sea de solo lectura para aplicaciones y usuarios.
3. Realice las transferencias incrementales finales para copiar los deltas restantes entre las ubicaciones de origen y destino.
4. Realice una validación exhaustiva de los datos (por ejemplo, revisando CloudWatch los registros y los [informes de tareas](#)).
5. Cambie sus aplicaciones y usuarios al nuevo entorno de su ubicación de destino.
6. Pruebe la funcionalidad de la aplicación y asegúrese de que los usuarios puedan acceder a los datos de su ubicación de destino.
7. Programa una reunión retrospectiva para revisar la transferencia con los equipos de migración. Haga los siguientes ejemplos de preguntas de sondeo:
 - ¿Se realizó correctamente la transición? Si no, ¿cuál era el problema?
 - ¿Usamos todo el ancho de banda disponible?
 - ¿Se utilizaron por completo el almacenamiento de origen y destino?
 - ¿Podemos obtener un mayor rendimiento de datos con tareas adicionales?
 - ¿Debemos planificar un período de mantenimiento más largo?
8. Si es necesario, actualice su plan de migración antes de iniciar la siguiente oleada.

Supervisar sus transferencias

AWS DataSync proporciona varias opciones de supervisión para ayudarte a validar y depurar tu transferencia.

Monitoriza tus transferencias con métricas CloudWatch

Puedes crear CloudWatch paneles personalizados con métricas de la ejecución de tus DataSync tareas. Para obtener más información, consulte [Supervisión de las transferencias de datos con CloudWatch las métricas de Amazon](#).

Supervisión de transferencias de con informes de tareas

Si va a transferir millones de archivos u objetos, considere la posibilidad de utilizar informes de tareas. Los informes de tareas proporcionan información detallada sobre lo que se DataSync intenta transferir, omitir, verificar y eliminar durante la ejecución de una tarea. Para obtener más información, consulte [Supervise sus transferencias de datos con informes de tareas](#).

También puede visualizar sus informes de tareas mediante AWS servicios como AWS Glue Amazon Athena y Amazon. QuickSight Para obtener más información, consulte el [blog sobre AWS almacenamiento](#).

Supervise sus transferencias con CloudWatch registros

Como mínimo, le recomendamos que configure su tarea para registrar la información básica y los errores de transferencia. Para obtener más información, consulte [Supervisión de las transferencias de datos con Amazon CloudWatch Logs](#).

AWS DataSync API

Además de la AWS Management Console y AWS CLI, puede usar la AWS DataSync API para configurar y administrar DataSync con [AWS SDKs](#).

Temas

- [Acciones](#)
- [Data Types](#)
- [Errores comunes](#)
- [Parámetros comunes](#)

Acciones

Se admiten las siguientes acciones:

- [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

Detiene la ejecución de una AWS DataSync tarea en curso. La transferencia de algunos archivos se interrumpe bruscamente. El contenido de los archivos que se transfiere al destino puede estar incompleto o no ser coherente con los archivos de origen.

Sin embargo, si inicia la ejecución de una nueva tarea con la misma tarea y deja que finalice, el contenido del archivo de destino estará completo y será coherente. Esto se aplica a otros errores inesperados que interrumpan la ejecución de una tarea. En todos estos casos, la transferencia se completa DataSync correctamente al iniciar la siguiente ejecución de la tarea.

Sintaxis de la solicitud

```
{  
  "TaskExecutionArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[TaskExecutionArn](#)

Nombre de recurso de Amazon (ARN) de la ejecución de la tarea para que se detenga.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Activa un AWS DataSync agente que se implementa en el entorno de almacenamiento. El proceso de activación asocia el agente con el suyo Cuenta de AWS.

Si aún no ha desplegado un agente, consulte [¿Necesito un DataSync agente?](#)

Sintaxis de la solicitud

```
{
  "ActivationKey": "string",
  "AgentName": "string",
  "SecurityGroupArns": [ "string" ],
  "SubnetArns": [ "string" ],
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "VpcEndpointId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[ActivationKey](#)

Especifica la clave de activación de su DataSync agente. Si no tiene una clave de activación, consulte [Activar el agente](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 29 caracteres.

Patrón: [A-Z0-9]{5}(-[A-Z0-9]{5}){4}

Obligatorio: sí

AgentName

Especifica un nombre para el agente. Le recomendamos que especifique un nombre que pueda recordar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Obligatorio: no

SecurityGroupArns

Especifica el nombre de recurso de Amazon (ARN) del grupo de seguridad que permite el tráfico entre su agente y el punto de conexión del servicio de VPC. Solo puede especificar un ARN.

Tipo: matriz de cadenas

Miembros de la matriz: número fijo de 1 elemento.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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]+$`

Obligatorio: no

SubnetArns

Especifica el ARN de la subred en la que se encuentra el punto de conexión del servicio de VPC. Solo puede especificar un ARN.

Tipo: matriz de cadenas

Miembros de la matriz: número fijo de 1 elemento.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:subnet/.*$`

Obligatorio: no

Tags

Especifica las etiquetas que le ayudan a clasificar, filtrar y buscar AWS los recursos. Le recomendamos que cree al menos una etiqueta para el agente.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

VpcEndpointId

Especifica el ID del [punto de conexión del servicio de VPC](#) que está utilizando. Por ejemplo, un ID de punto de conexión de VPC se parece a `vpce-01234d5aff67890e1`.

Important

El punto final del servicio de VPC que utilice debe incluir el nombre del DataSync servicio (por ejemplo, `com.amazonaws.us-east-2.datasync`).

Tipo: cadena

Patrón: `^vpce-[0-9a-f]{17}$`

Obligatorio: no

Sintaxis de la respuesta

```
{
  "AgentArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AgentArn](#)

Estos comandos devuelven el ARN del agente que acaba de activar. Utilice la [ListAgents](#) operación para devolver una lista de los agentes que tiene en su mano Cuenta de AWS . Región de AWS

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Solicitud de ejemplo

El siguiente ejemplo activa un DataSync agente.

```
{
  "ActivationKey": "AAAAA-1AAAA-BB1CC-33333-EEEE",
  "AgentName": "MyAgent",
  "Tags": [{
    "Key": "Job",
    "Value": "TransferJob-1"
```

```
}]  
}
```

Respuesta de ejemplo

La respuesta devuelve el ARN del agente activado.

```
{  
  "AgentArn": "arn:aws:datasync:us-east-2:111222333444:agent/agent-0b0addbeef44baca3"  
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un contenedor de Microsoft Azure Blob Storage. AWS DataSync puede usar esta ubicación como origen o destino de la transferencia. Puede realizar transferencias con o sin un [DataSync agente](#) que se conecte a su contenedor.

Antes de empezar, asegúrese de saber [cómo se DataSync accede a Azure Blob Storage](#) y cómo funciona con los [niveles de acceso](#) y los tipos de [blob](#).

Sintaxis de la solicitud

```
{
  "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"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

AccessTier

Especifica el nivel de acceso al que desea transferir sus objetos o archivos. Esto solo se aplica cuando se utiliza la ubicación como destino de transferencia. Para obtener más información, consulte [Niveles de acceso](#).

Tipo: cadena

Valores válidos: HOT | COOL | ARCHIVE

Obligatorio: no

AgentArns

(Opcional) Especifica el nombre de recurso de Amazon (ARN) del DataSync agente que se puede conectar con el contenedor de Azure Blob Storage. Si va a configurar una transferencia entre nubes sin agente, no necesita especificar un valor para este parámetro.

Puede especificar más de un agente. Para obtener más información, consulte [Using multiple agents for your transfer](#).

Note

Asegúrese de configurar este parámetro correctamente la primera vez que cree su ubicación de almacenamiento. No puede añadir ni eliminar agentes de una ubicación de almacenamiento después de crearla.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

AuthenticationType

Especifica el método de autenticación que se DataSync utiliza para acceder a Azure Blob Storage. DataSync puede acceder al almacenamiento de blobs mediante una firma de acceso compartido (SAS).

Tipo: cadena

Valores válidos: SAS | NONE

Obligatorio: sí

BlobType

Especifica el tipo de blob que desea que tengan sus objetos o archivos al transferirlos a Azure Blob Storage. Actualmente, DataSync solo admite el traslado de datos a Azure Blob Storage como bloques blobs. Para obtener más información sobre los tipos de blobs, consulte la [Documentación de Azure Blob Storage](#).

Tipo: cadena

Valores válidos: BLOCK

Obligatorio: no

CmkSecretConfig

Especifica la información de configuración de un secreto DataSync administrado, que incluye el token de autenticación que se DataSync utiliza para acceder a una ubicación de AzureBlob almacenamiento específica, con una ubicación administrada por el cliente. AWS KMS key

Cuando incluye este parámetro como parte de una `CreateLocationAzureBlob` solicitud, solo proporciona la clave KMS ARN. DataSync utiliza esta clave de KMS junto con el token de autenticación que especifique `SasConfiguration` para crear un secreto DataSync administrado que almacene las credenciales de acceso a la ubicación.

Asegúrese de que DataSync tiene permiso para acceder a la clave de KMS que especifique.

Note

Puede usar `CmkSecretConfig (conSasConfiguration)` o `CustomSecretConfig (sinSasConfiguration)` para proporcionar las credenciales para una

CreateLocationAzureBlob solicitud. No proporciones ambos parámetros para la misma solicitud.

Tipo: objeto [CmkSecretConfig](#)

Obligatorio: no

[ContainerUrl](#)

Especifica la URL del contenedor de Azure Blob Storage implicado en la transferencia.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 325 caracteres.

Patrón: `^https:\\\\[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}\\[a-z0-9](-?[a-z0-9]){2,62}$`

Obligatorio: sí

[CustomSecretConfig](#)

Especifica la información de configuración de un secreto de Secrets Manager administrado por el cliente en el que el token de autenticación de una ubicación AzureBlob de almacenamiento se almacena en texto plano. Esta configuración incluye el ARN secreto y el ARN de un rol de IAM que proporciona acceso al secreto.

Note

Puede utilizar CmkSecretConfig (conSasConfiguration) o CustomSecretConfig (sinSasConfiguration) para proporcionar las credenciales a una solicitud.

CreateLocationAzureBlob No proporciones ambos parámetros para la misma solicitud.

Tipo: objeto [CustomSecretConfig](#)

Obligatorio: no

[SasConfiguration](#)

Especifica la configuración de SAS que permite acceder DataSync a su Azure Blob Storage.

Note

Si proporciona un token de autenticación utilizando `SasConfiguration`, pero no proporciona detalles de configuración secretos utilizando `CmkSecretConfig` o `CustomSecretConfig`, entonces DataSync almacena el token utilizando el secreto del administrador de secretos de su AWS cuenta.

Tipo: objeto [AzureBlobSasConfiguration](#)

Obligatorio: no

Subdirectory

Especifica los segmentos de ruta si desea limitar su transferencia a un directorio virtual del contenedor (por ejemplo, `/my/images`).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 1024 caracteres.

Patrón: `^[\\p{L}\\p{M}\\p{Z}\\p{S}\\p{N}\\p{P}\\p{C}]*$`

Obligatorio: no

Tags

Especifica las etiquetas que le ayudan a clasificar, filtrar y buscar sus recursos de AWS . Le recomendamos crear al menos una etiqueta de nombre para su ubicación de transferencia.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{
  "LocationArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[LocationArn](#)

ARN de la ubicación de transferencia de Azure Blob Storage que creó.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un sistema de archivos Amazon EFS. AWS DataSync puede usar esta ubicación como origen o destino para transferir datos.

Antes de empezar, asegúrese de entender cómo DataSync [accede a los sistemas de archivos de Amazon EFS](#).

Sintaxis de la solicitud

```
{
  "AccessPointArn": "string",
  "Ec2Config": {
    "SecurityGroupArns": [ "string" ],
    "SubnetArn": "string"
  },
  "EfsFileSystemArn": "string",
  "FileSystemAccessRoleArn": "string",
  "InTransitEncryption": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[AccessPointArn](#)

Especifica el nombre de recurso de Amazon (ARN) del punto de acceso que se DataSync utiliza para montar el sistema de archivos Amazon EFS.

Para obtener más información, consulte [Acceso a sistemas de archivos restringidos](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

[Ec2Config](#)

Especifica la subred y los grupos de seguridad que se DataSync utilizan para conectarse a uno de los [destinos de montaje](#) del sistema de archivos Amazon EFS.

Tipo: objeto [Ec2Config](#)

Obligatorio: sí

[EfsFileSystemArn](#)

Especifica el ARN del sistema de archivos de Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):elasticfilesystem:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

Obligatorio: sí

[FileSystemAccessRoleArn](#)

Especifica un rol AWS Identity and Access Management (IAM) que permite acceder DataSync al sistema de archivos Amazon EFS.

Para obtener información sobre la creación de esta función, consulte [Creación de una función de DataSync IAM para el acceso al sistema de archivos](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam:[0-9]{12}:role/.*$`

Obligatorio: no

[InTransitEncryption](#)

Especifica si desea DataSync utilizar el cifrado Transport Layer Security (TLS) 1.2 cuando transfiera datos hacia o desde su sistema de archivos Amazon EFS.

Si especifica un punto de acceso mediante `AccessPointArn` o un rol de IAM con `FileSystemAccessRoleArn`, debe establecer este parámetro en `TLS1_2`.

Tipo: cadena

Valores válidos: NONE | TLS1_2

Obligatorio: no

[Subdirectory](#)

Especifica una ruta de montaje para el sistema de archivos de Amazon EFS. Aquí es donde DataSync lee o escribe los datos en su sistema de archivos (dependiendo de si se trata de una ubicación de origen o de destino).

De forma predeterminada, DataSync usa el directorio raíz (o [el punto de acceso](#) si lo proporciona `AccessPointArn`). También puede incluir subdirectorios usando barras diagonales (por ejemplo, `/path/to/folder`).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obligatorio: no

[Tags](#)

Especifica el par clave-valor que representa una etiqueta que desea agregar al recurso. El valor puede ser una cadena vacía. Este valor le ayuda a administrar, filtrar y buscar sus recursos. Le recomendamos que cree una etiqueta de nombre para su ubicación.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{
  "LocationArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

LocationArn

Nombre de recurso de Amazon (ARN) de la ubicación del sistema de archivos de Amazon EFS que cree.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Solicitud de ejemplo

En el siguiente ejemplo, se crea una ubicación para un sistema de archivos de 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"
  }]
}
```

Solicitud de muestra: creación de una ubicación para un sistema de archivos de Amazon EFS restringido

En el siguiente ejemplo, se crea una ubicación para un sistema de archivos de Amazon EFS configurado para acceso restringido. En este tipo de escenario, es posible que deba especificar valores para `AccessPointArn`, `FileSystemAccessRoleArn` y `InTransitEncryption` en su solicitud.

```
{
  "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"
  }]
}
```

Respuesta de ejemplo

Una respuesta arroja el ARN de ubicación del sistema de archivos de Amazon EFS.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
  loc-12abcdef012345678"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un sistema de archivos de Amazon FSx for Lustre. AWS DataSync puede usar esta ubicación como origen o destino para transferir datos.

Antes de empezar, asegúrese de entender cómo se DataSync [accede a los sistemas de archivos FSx de Lustre](#).

Sintaxis de la solicitud

```
{
  "FsxFilesystemArn": "string",
  "SecurityGroupArns": [ "string" ],
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[FsxFilesystemArn](#)

Especifica el nombre de recurso de Amazon (ARN) del sistema de archivos de FSx for Lustre.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

Obligatorio: sí

SecurityGroupArns

Especifica los nombres de recursos de Amazon (ARNs) de hasta cinco grupos de seguridad que proporcionan acceso a su sistema de archivos FSx for Lustre.

Los grupos de seguridad deben poder acceder a los puertos del sistema de archivos. El sistema de archivos también debe permitir el acceso desde los grupos de seguridad. Para obtener información sobre el acceso al sistema de archivos, consulte la [Guía del usuario de Amazon FSx for Lustre](#).

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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]+$`

Obligatorio: sí

Subdirectory

Especifica una ruta de montaje para su sistema FSx de archivos para Lustre. La ruta puede incluir subdirectorios.

Cuando la ubicación se utiliza como fuente, DataSync lee los datos de la ruta de montaje. Cuando la ubicación se utiliza como destino, DataSync escribe los datos en la ruta de montaje. Si no incluye este parámetro, DataSync utiliza el directorio raíz del sistema de archivos (/).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\+\.\/(\\)\$\\p{Zs}]+$`

Obligatorio: no

Tags

Especifica las etiquetas que le ayudan a clasificar, filtrar y buscar sus recursos de AWS . Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{  
  "LocationArn": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[LocationArn](#)

El nombre del recurso de Amazon (ARN) de la ubicación del sistema de archivos de FSx for Lustre que ha creado.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un sistema de archivos Amazon FSx for NetApp ONTAP. AWS DataSync puede usar esta ubicación como origen o destino para transferir datos.

Antes de empezar, asegúrese de entender cómo se DataSync [accede a los sistemas de archivos FSx de ONTAP](#).

Sintaxis de la solicitud

```
{
  "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"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

Protocol

Especifica el protocolo de transferencia de datos que se AWS DataSync utiliza para acceder al sistema de FSx archivos de Amazon.

Tipo: objeto [FsxProtocol](#)

Obligatorio: sí

SecurityGroupArns

Especifica los grupos EC2 de seguridad de Amazon que proporcionan acceso a la subred preferida del sistema de archivos.

Los grupos de seguridad deben permitir el tráfico saliente en los siguientes puertos (según el protocolo que utilice):

- Sistema de archivos de red (NFS): puertos TCP 111, 635 y 2049
- Server Message Block (SMB): puerto TCP 445

Los grupos de seguridad del sistema de archivos también deben permitir el tráfico entrante en los mismos puertos.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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]+$`

Obligatorio: sí

StorageVirtualMachineArn

Especifica el ARN de la máquina virtual de almacenamiento (SVM) del sistema de archivos en el que quiere copiar datos o desde el que quiere copiar datos.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 162 caracteres.

Patrón: `^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,}$`

Obligatorio: sí

Subdirectory

Especifica una ruta al recurso compartido de archivos del SVM al que desea transferir los datos o desde el que desea transferirlos.

Puede especificar una ruta de unión (también conocida como punto de montaje), una ruta de qtree (para recursos compartidos de archivos NFS) o un nombre de recurso compartido (para recursos compartidos de archivos SMB). Por ejemplo, la ruta de montaje podría ser /vol1, /vol1/tree1 o /share1.

Note

No especifique una ruta de cruce en el volumen raíz del SVM. Para obtener más información, consulte [Administración FSx de máquinas virtuales de almacenamiento de ONTAP](#) en la Guía del usuario de Amazon FSx for NetApp ONTAP.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^[^\u0000\u0085\u2028\u2029\r\n]{1,255}$`

Obligatorio: no

Tags

Especifica las etiquetas que le ayudan a clasificar, filtrar y buscar sus recursos de AWS . Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{  
  "LocationArn": "string"
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

LocationArn

Especifica el ARN de la ubicación del sistema FSx de archivos ONTAP que cree.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)

- [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

Crea una ubicación de transferencia para un sistema de archivos Amazon FSx for OpenZFS. AWS DataSync puede usar esta ubicación como origen o destino para transferir datos.

Antes de empezar, asegúrese de entender cómo se DataSync [accede a los sistemas FSx de archivos OpenZFS](#).

Note

Los parámetros de solicitud relacionados con SMB no se admiten con la operación CreateLocationFsxOpenZfs.

Sintaxis de la solicitud

```
{
  "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"
    }
  ]
}
```



```
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[FsxFilesystemArn](#)

El nombre de recurso de Amazon (ARN) del sistema de archivos FSx OpenZFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

Obligatorio: sí

[Protocol](#)

El tipo de protocolo que se AWS DataSync utiliza para acceder al sistema de archivos.

Tipo: objeto [FsxProtocol](#)

Obligatorio: sí

[SecurityGroupArns](#)

Los grupos ARNs de seguridad que se utilizan para configurar el sistema de FSx archivos OpenZFS.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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]+$`

Obligatorio: sí

Subdirectory

Un subdirectorio en la ruta de la ubicación que debe empezar por. /fsx DataSync utiliza este subdirectorio para leer o escribir datos (dependiendo de si el sistema de archivos es una ubicación de origen o de destino).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[^\\u0000\\u0085\\u2028\\u2029\\r\\n]{1,4096}$`

Obligatorio: no

Tags

El par clave-valor que representa una etiqueta que desea agregar al recurso. El valor puede ser una cadena vacía. Este valor le ayuda a administrar, filtrar y buscar sus recursos. Le recomendamos que cree una etiqueta de nombre para su ubicación.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{
  "LocationArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

LocationArn

El ARN de la ubicación del sistema FSx de archivos OpenZFS que creó.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un sistema de archivos de Amazon FSx para Windows File Server. AWS DataSync puede usar esta ubicación como origen o destino para transferir datos.

Antes de empezar, asegúrese de entender cómo se DataSync [accede FSx a los sistemas de archivos del servidor de archivos de Windows](#).

Sintaxis de la solicitud

```
{
  "Domain": "string",
  "FsxFilesystemArn": "string",
  "Password": "string",
  "SecurityGroupArns": [ "string" ],
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "User": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

Domain

Especifica el nombre del dominio de Windows al que pertenece el sistema FSx de archivos del servidor de archivos de Windows.

Si tiene varios dominios de Active Directory en su entorno, la configuración de este parámetro garantiza que DataSync se conecte al sistema de archivos correcto.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 253 caracteres.

Patrón: `^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}$`

Obligatorio: no

FsxFilesystemArn

Especifica el nombre de recurso de Amazon (ARN) FSx para el sistema de archivos del servidor de archivos de Windows.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

Obligatorio: sí

Password

Especifica la contraseña del usuario con los permisos para montar y acceder a los archivos, las carpetas y los metadatos de los archivos del sistema de archivos FSx del servidor de archivos de Windows.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^.{0,104}$`

Obligatorio: sí

SecurityGroupArns

Especifica los grupos ARNs de EC2 seguridad de Amazon que proporcionan acceso a la subred preferida del sistema de archivos.

Los grupos de seguridad que especifique deben poder comunicarse con los grupos de seguridad del sistema de archivos. Para obtener información sobre la configuración de grupos de seguridad para el acceso al sistema de archivos, consulte la [Guía del usuario de Amazon FSx for Windows File Server](#).

Note

Si elige un grupo de seguridad que no permite conexiones desde dentro de sí mismo, haga una de estas cosas:

- Configure el grupo de seguridad para permitir que se comunique dentro de sí mismo.
- Elija un grupo de seguridad diferente que pueda comunicarse con el grupo de seguridad del destino de montaje.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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]+$`

Obligatorio: sí

Subdirectory

Especifica una ruta de montaje para el sistema de archivos mediante barras inclinadas. Aquí es donde DataSync lee o escribe los datos (dependiendo de si se trata de una ubicación de origen o de destino).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\+\.\/(\\)\$\\p{Zs}]+$`

Obligatorio: no

Tags

Especifica las etiquetas que le ayudan a clasificar, filtrar y buscar sus recursos de AWS . Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

User

Especifica el usuario con los permisos para montar y acceder a los archivos, las carpetas y los metadatos de los archivos del sistema FSx de archivos del servidor de archivos de Windows.

Para obtener información sobre cómo elegir un usuario con el nivel de acceso adecuado para la transferencia, consulte [los permisos necesarios](#) FSx para las ubicaciones de los servidores de archivos de Windows.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^[^\\x22\\x5B\\x5D\\/\\:;|,+=*?\\x3C\\x3E]{1,104}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "LocationArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[LocationArn](#)

El ARN de la ubicación del sistema FSx de archivos del servidor de archivos de Windows que creó.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un sistema de archivos distribuido Hadoop (HDFS). AWS DataSync puede utilizar esta ubicación como origen o destino para transferir datos.

Antes de empezar, asegúrese de entender cómo se DataSync [accede a los clústeres de HDFS](#).

Sintaxis de la solicitud

```
{
  "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"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[AgentArns](#)

Los nombres de recursos de Amazon (ARNs) de los DataSync agentes que se pueden conectar al clúster de HDFS.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

[AuthenticationType](#)

El tipo de autenticación utilizado para determinar la identidad del usuario.

Tipo: cadena

Valores válidos: SIMPLE | KERBEROS

Obligatorio: sí

[BlockSize](#)

El tamaño de los bloques de datos que se escribirán en el clúster HDFS. El tamaño del bloque debe ser un múltiplo de 512 bytes. El tamaño de bloque predeterminado es de 128 mebibytes (MiB).

Tipo: entero

Rango válido: valor mínimo de 1 048 576. Valor máximo de 1 073 741 824.

Obligatorio: no

[KerberosKeytab](#)

La tabla de claves de Kerberos (keytab) que contiene asignaciones entre el Kerberos principal definido y las claves cifradas. Puede cargar el keytab desde un archivo proporcionando la dirección del archivo.

 Note

Este parámetro es obligatorio si se especifica KERBEROS para AuthenticationType.

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 65 536 caracteres.

Obligatorio: no

KerberosKrb5Conf

El archivo `krb5.conf` que contiene la información de configuración de Kerberos. Puede cargar el archivo `krb5.conf` proporcionando la dirección del archivo. Si utiliza la AWS CLI, esta realizará la codificación base64 por usted. De lo contrario, proporcione texto codificado en base64.

 Note

Este parámetro es obligatorio si se especifica KERBEROS para AuthenticationType.

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 131 072 caracteres.

Obligatorio: no

KerberosPrincipal

La entidad principal de Kerberos con acceso a los archivos y carpetas del clúster de HDFS.

 Note

Este parámetro es obligatorio si se especifica KERBEROS para AuthenticationType.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^.+`

Obligatorio: no

[KmsKeyProviderUri](#)

El URI de Key Management Server (KMS) del clúster HDFS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `^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$`

Obligatorio: no

[NameNodes](#)

El NameNode que administra el espacio de nombres HDFS. NameNode Realiza operaciones como abrir, cerrar y cambiar el nombre de archivos y directorios. NameNode Contiene la información necesaria para asignar bloques de datos al DataNodes. Puede usar solo uno NameNode.

Tipo: matriz de objetos [HdfsNameNode](#)

Miembros de la matriz: número mínimo de 1 artículo.

Obligatorio: sí

[QopConfiguration](#)

La configuración de calidad de protección (QOP) especifica la llamada a procedimiento remoto (RPC) y los ajustes de protección de transferencia de datos configurados en el clúster del sistema de archivos distribuido de Hadoop (HDFS). Si no se especifica `QopConfiguration`, el valor predeterminado de `RpcProtection` y `DataTransferProtection` es `PRIVACY`. Si configura `RpcProtection` o `DataTransferProtection`, el otro parámetro asume el mismo valor.

Tipo: objeto [QopConfiguration](#)

Obligatorio: no

[ReplicationFactor](#)

El número en el DataNodes que se van a replicar los datos al escribir en el clúster HDFS. De forma predeterminada, los datos se replican en tres. DataNodes

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 512.

Obligatorio: no

[SimpleUser](#)

El nombre de usuario utilizado para identificar al cliente en el sistema operativo host.

Note

Este parámetro es obligatorio si se especifica SIMPLE para AuthenticationType.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^[_ .A-Za-z0-9][_ .A-Za-z0-9]*$`

Obligatorio: no

[Subdirectory](#)

Un subdirectorio del clúster de HDFS. Este subdirectorio se utiliza para leer o escribir datos en el clúster de HDFS. Si no se especifica el subdirectorio, el valor predeterminado será `/`.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\/\(\)\$\p{Zs}]+$`

Obligatorio: no

[Tags](#)

El par clave-valor que representa la etiqueta que desea agregar a la ubicación. El valor puede ser una cadena vacía. Le recomendamos que utilice etiquetas para asignar nombres a sus recursos.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{  
  "LocationArn": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[LocationArn](#)

El ARN de la ubicación del clúster de HDFS de origen que usted crea.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un servidor de archivos de Network File System (NFS). AWS DataSync puede usar esta ubicación como origen o destino para transferir datos.

Antes de empezar, asegúrese de entender cómo se DataSync [accede a los servidores de archivos NFS](#).

Sintaxis de la solicitud

```
{
  "MountOptions": {
    "Version": "string"
  },
  "OnPremConfig": {
    "AgentArns": [ "string" ]
  },
  "ServerHostname": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[MountOptions](#)

Especifica las opciones que se DataSync pueden utilizar para montar el servidor de archivos NFS.

Tipo: objeto [NfsMountOptions](#)

Obligatorio: no

OnPremConfig

Especifica el nombre de recurso de Amazon (ARN) del DataSync agente que se puede conectar al servidor de archivos NFS.

Puede especificar más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

Tipo: objeto [OnPremConfig](#)

Obligatorio: sí

ServerHostname

Especifica el nombre DNS o la dirección IP versión 4 del servidor de archivos NFS al que se conecta el DataSync agente.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(([a-zA-Z0-9\-.]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-.:]*[A-Za-z0-9])$`

Obligatorio: sí

Subdirectory

Especifica la ruta de exportación del servidor de archivos NFS que desea DataSync montar.

Esta ruta (o un subdirectorio de la ruta) es DataSync desde donde se transfieren los datos hacia o desde ella. Para obtener información sobre cómo configurar una exportación DataSync, consulte [Acceso a los servidores de archivos NFS](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]+$`

Obligatorio: sí

Tags

Especifica etiquetas que le ayudan a clasificar, filtrar y buscar los recursos. AWS Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{  
  "LocationArn": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[LocationArn](#)

El ARN de la ubicación de transferencia que creó para el servidor de archivos NFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Ejemplo

El siguiente ejemplo crea una ubicación de DataSync transferencia para un servidor de archivos NFS.

Solicitud de muestra

```
{
  "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"
    }
  ]
}
```

Ejemplo

La respuesta devuelve el ARN de la ubicación NFS.

Respuesta de ejemplo

```
{
```

```
"LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-07db7abfc326c50aa"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un sistema de almacenamiento de objetos. AWS DataSync puede usar esta ubicación como origen o destino para transferir datos. Puede realizar transferencias con o sin un [DataSyncagente](#).

Antes de empezar, asegúrese de entender los [requisitos previos](#) DataSync para trabajar con sistemas de almacenamiento de objetos.

Sintaxis de la solicitud

```
{
  "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"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

AccessKey

Especifica la clave de acceso (por ejemplo, un nombre de usuario) si se requieren credenciales para autenticarse en el servidor de almacenamiento de objetos.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 200 caracteres.

Patrón: `^\.*$`

Obligatorio: no

AgentArns

(Opcional) Especifica los nombres de recursos de Amazon (ARNs) de los DataSync agentes que se pueden conectar al sistema de almacenamiento de objetos. Si está configurando una transferencia entre nubes sin agentes, no necesita especificar un valor para este parámetro.

Note

Asegúrese de configurar este parámetro correctamente la primera vez que cree su ubicación de almacenamiento. No puede añadir ni eliminar agentes de una ubicación de almacenamiento después de crearla.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

BucketName

Especifica el nombre del bucket de almacenamiento de objetos implicado en la transferencia.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 63 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\\(\)\$\p{Zs}]+$`

Obligatorio: sí

[CmkSecretConfig](#)

Especifica la información de configuración de un secreto DataSync administrado, que incluye el `SecretKey` que se DataSync utiliza para acceder a una ubicación de almacenamiento de objetos específica, con un secreto administrado por el cliente AWS KMS key.

Cuando incluye este parámetro como parte de una `CreateLocationObjectStorage` solicitud, solo proporciona la clave KMS ARN. DataSync utiliza esta clave de KMS junto con el valor que especifique para el `SecretKey` parámetro a fin de crear un secreto DataSync administrado para almacenar las credenciales de acceso a la ubicación.

Asegúrese de que DataSync tiene permiso para acceder a la clave de KMS que especifique.

Note

Puede usar `CmkSecretConfig` (`conSecretKey`) o `CustomSecretConfig` (`sinSecretKey`) para proporcionar las credenciales para una `CreateLocationObjectStorage` solicitud. No proporcione ambos parámetros para la misma solicitud.

Tipo: objeto [CmkSecretConfig](#)

Obligatorio: no

[CustomSecretConfig](#)

Especifica la información de configuración de un secreto de Secrets Manager administrado por el cliente, donde la clave secreta de una ubicación de almacenamiento de objetos específica se almacena en texto sin formato. Esta configuración incluye el ARN secreto y el ARN de un rol de IAM que proporciona acceso al secreto.

Note

Puede utilizar `CmkSecretConfig` (`conSecretKey`) o `CustomSecretConfig` (`sinSecretKey`) para proporcionar las credenciales a una solicitud.

CreateLocationObjectStorage No proporciona ambos parámetros para la misma solicitud.

Tipo: objeto [CustomSecretConfig](#)

Obligatorio: no

[SecretKey](#)

Especifica la clave secreta (por ejemplo, una contraseña) si se requieren credenciales para autenticarse en el servidor de almacenamiento de objetos.

Note

Si proporciona un secreto utilizando `SecretKey`, pero no proporciona los detalles de configuración del secreto, utilizando `CmkSecretConfig` o `CustomSecretConfig`, entonces DataSync almacena el token con el secreto de Secrets Manager de su AWS cuenta.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 200 caracteres.

Patrón: `^.*$`

Obligatorio: no

[ServerCertificate](#)

Especifica una cadena de certificados DataSync para autenticarse en el sistema de almacenamiento de objetos si el sistema utiliza una entidad de certificación (CA) privada o autofirmada. Debe especificar un único archivo `.pem` con una cadena de certificados completa (por ejemplo, `file:///home/user/.ssh/object_storage_certificates.pem`).

La cadena de certificados puede incluir:

- El certificado del sistema de almacenamiento de objetos
- Todos los certificados intermedios (si los hay)
- El certificado raíz de la CA firmante

Puede concatenar sus certificados en un archivo .pem (que puede tener un máximo de 32 768 bytes antes de la codificación base64). El siguiente comando cat de ejemplo crea un archivo `object_storage_certificates.pem` que incluye tres certificados:

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

Para usar este parámetro, configure el `ServerProtocol` para HTTPS.

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 32 768 caracteres.

Obligatorio: no

ServerHostname

Especifica el nombre de dominio o la dirección IP de versión 4 (IPv4) del servidor de almacenamiento de objetos al que se conecta el DataSync agente.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(([a-zA-Z0-9\-\.]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-\:]*[A-Za-z0-9])$`

Obligatorio: sí

ServerPort

Especifica el puerto en el que el servidor de almacenamiento de objetos acepta el tráfico de red entrante (por ejemplo, el puerto 443).

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 65 536.

Obligatorio: no

ServerProtocol

Especifica el protocolo que usa el servidor de almacenamiento de objetos para comunicarse. Si no se especifica, el valor predeterminado es HTTPS.

Tipo: cadena

Valores válidos: HTTPS | HTTP

Obligatorio: no

[Subdirectory](#)

Especifica el prefijo de objeto del servidor de almacenamiento de objetos. Si se trata de una ubicación de origen, DataSync solo copia los objetos con este prefijo. Si se trata de una ubicación de destino, DataSync escribe todos los objetos con este prefijo.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\+\.\/\(\)\p{Zs}]*$`

Obligatorio: no

[Tags](#)

Especifica el par clave-valor que representa una etiqueta que desea agregar al recurso. Las etiquetas le ayudan a administrar, filtrar y buscar sus recursos. Le recomendamos crear una etiqueta de nombre para su ubicación.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{
  "LocationArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

LocationArn

Especifique el ARN de la ubicación del sistema de almacenamiento de objetos que creó.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un bucket de Amazon S3. AWS DataSync puede usar esta ubicación como origen o destino para transferir datos.

Important

Antes de comenzar, asegúrese de haber leído los siguientes temas:

- [Consideraciones sobre las clases de almacenamiento en las ubicaciones de Amazon S3](#)
- [Evaluación de los costos de las solicitudes de S3 al usar DataSync](#)

Para obtener más información, consulte [Configuring transfers with Amazon S3](#).

Sintaxis de la solicitud

```
{
  "AgentArns": [ "string" ],
  "S3BucketArn": "string",
  "S3Config": {
    "BucketAccessRoleArn": "string"
  },
  "S3StorageClass": "string",
  "Subdirectory": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

AgentArns

(Amazon S3 solo en Outposts) Especifica el nombre de recurso de Amazon (ARN) del DataSync agente de su Outpost.

Para obtener más información, consulte [Implementar su agente en. DataSync AWS Outposts](#)

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

S3BucketArn

Especifica el ARN del bucket de S3 que desea usar como ubicación. (Al crear la DataSync tarea más adelante, especifique si esta ubicación es un origen o un destino de transferencia).

Si su bucket de S3 se encuentra en un AWS Outposts recurso, debe especificar un punto de acceso de Amazon S3. Para obtener más información, consulte [Administración del acceso a datos con puntos de acceso de Amazon S3](#) en la Guía del usuario de Amazon S3.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 268.

Patrón: `^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}$`

Obligatorio: sí

S3Config

Especifica el nombre de recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que se DataSync utiliza para acceder al bucket de S3.

Para obtener más información, consulte [Proporcionar DataSync acceso a los buckets de S3](#).

Tipo: objeto [S3Config](#)

Obligatorio: sí

[S3StorageClass](#)

Especifica la clase de almacenamiento que desea que utilicen los objetos cuando Amazon S3 sea un destino de transferencia.

Para los depósitos incluidos Regiones de AWS, la clase de almacenamiento se establece de forma predeterminada en. STANDARD Para los depósitos activados AWS Outposts, la clase de almacenamiento se establece de forma predeterminada en. OUTPOSTS

Para obtener más información, consulte [Storage class considerations with Amazon S3 transfers](#).

Tipo: cadena

Valores válidos: STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL

Obligatorio: no

[Subdirectory](#)

Especifica un prefijo en el depósito de S3 que DataSync lee o escribe en él (en función de si el depósito es una ubicación de origen o de destino).

Note

DataSync no puede transferir objetos con un prefijo que comience con una barra (/) o que incluya ///./, o patrones. /./ Por ejemplo:

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

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\+\.\/\(\)\p{Zs}]*$`

Obligatorio: no

Tags

Especifica etiquetas que ayudan a clasificar, filtrar y buscar los recursos. AWS Le recomendamos crear al menos una etiqueta de nombre para su ubicación de transferencia.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{
  "LocationArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[LocationArn](#)

El ARN de la ubicación de S3 que creó.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Paso 1. Permiso para que se asuma el rol de IAM necesario para escribir en el bucket

El siguiente ejemplo muestra la política más sencilla que concede los permisos necesarios para acceder AWS DataSync a un bucket de Amazon S3 de destino, seguida de una función de IAM a la que se ha asociado la `create-location-s3-iam-role` política.

```
{
  "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"
}
```

Paso 2. Permiso para que el rol de IAM creado escriba en el bucket.

Asocie una política que disponga de permisos suficientes para acceder el bucket al rol. Un ejemplo de esta política es la política administrada `AWSDDataSyncFullAccess`.

Para obtener más información, consulte [AWSDDataSyncFullAccess](#) en la consola de IAM.

No es necesario que usted cree esta política. Está administrado por AWS, por lo que todo lo que necesita hacer es especificar su ARN en el `attach-role-policy` comando.

```
IAM_POLICY_ARN='arn:aws:iam::aws:policy/AWSDDataSyncFullAccess'
```

Paso 3. Creación de un punto de conexión para un bucket de Amazon S3.

El ejemplo a continuación crea un punto de conexión para un bucket de Amazon S3.

Cuando se crea el punto de conexión S3, una respuesta similar a la del segundo ejemplo siguiente devuelve el nombre de recurso de Amazon (ARN) de la nueva ubicación de Amazon S3.

Solicitud de muestra

```
{
  "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"
}
```

Respuesta de ejemplo

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Crea una ubicación de transferencia para un servidor de archivos de bloque de mensajes del servidor (SMB). AWS DataSync puede usar esta ubicación como origen o destino para transferir datos.

Antes de empezar, asegúrese de entender cómo se DataSync accede a los servidores de archivos SMB. Para obtener más información, consulte [Proporcionar DataSync acceso a los servidores de archivos SMB](#).

Sintaxis de la solicitud

```
{
  "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"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

AgentArns

Especifica el DataSync agente (o los agentes) que se pueden conectar al servidor de archivos SMB. Puede especificar un agente mediante un nombre de recurso de Amazon (ARN).

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

AuthenticationType

Especifica el protocolo de autenticación que se DataSync utiliza para conectarse al servidor de archivos SMB. DataSync admite NTLM (predeterminado) y KERBEROS autenticación.

Para obtener más información, consulte [Proporcionar DataSync acceso a servidores de archivos SMB](#).

Tipo: cadena

Valores válidos: NTLM | KERBEROS

Obligatorio: no

DnsIpAddresses

Especifica las IPv4 direcciones de los servidores DNS a los que pertenece el servidor de archivos SMB. Este parámetro solo se aplica si AuthenticationType está establecido en. KERBEROS

Si tiene varios dominios en su entorno, la configuración de este parámetro garantiza que DataSync se conecte al servidor de archivos SMB correcto.

Tipo: matriz de cadenas

Miembros de la matriz: número máximo de 2 elementos.

Limitaciones de longitud: longitud mínima de 7. Longitud máxima de 39.

Patrón: \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

Obligatorio: no

[Domain](#)

Especifica el nombre de dominio de Windows al que pertenece el servidor de archivos SMB. Este parámetro solo se aplica si `AuthenticationType` está establecido en `NTLM`.

Si tiene varios dominios en su entorno, la configuración de este parámetro garantiza que DataSync se conecte al servidor de archivos correcto.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 253 caracteres.

Patrón: ^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}\$

Obligatorio: no

[KerberosKeytab](#)

Especifica el archivo de tabla de claves de Kerberos (keytab), que incluye las asignaciones entre las claves principales y de cifrado de Kerberos.

Para evitar errores de ejecución de tareas, asegúrese de que el principal de Kerberos que utiliza para crear el archivo keytab coincide exactamente con lo que ha especificado.

`KerberosPrincipal`

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 65 536 caracteres.

Obligatorio: no

[KerberosKrb5Conf](#)

Especifica un archivo de configuración de Kerberos (`krb5.conf`) que define la configuración del dominio de Kerberos.

El archivo debe estar codificado en base64. Si está utilizando el AWS CLI, la codificación está hecha por usted.

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 131 072 caracteres.

Obligatorio: no

KerberosPrincipal

Especifica un director de Kerberos, que es una identidad de su dominio de Kerberos que tiene permiso para acceder a los archivos, las carpetas y los metadatos de los archivos de su servidor de archivos SMB.

Un principal de Kerberos podría tener este aspecto. HOST/kerberosuser@MYDOMAIN.ORG

Los nombres principales distinguen entre mayúsculas y minúsculas. La ejecución de la DataSync tarea fallará si el principal que especifique para este parámetro no coincide exactamente con el principal que utilizó para crear el archivo keytab.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: ^.+\$

Obligatorio: no

MountOptions

Especifica la versión del protocolo SMB que se DataSync utiliza para acceder al servidor de archivos SMB.

Tipo: objeto [SmbMountOptions](#)

Obligatorio: no

Password

Especifica la contraseña del usuario que puede montar su servidor de archivos SMB y que tiene permiso para acceder a los archivos y las carpetas involucrados en la transferencia. Este parámetro solo se aplica si AuthenticationType está establecido en. NTLM

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^\{0,104\}$`

Obligatorio: no

ServerHostname

Especifica el nombre de dominio o la dirección IP del servidor de archivos SMB al que se conecta el DataSync agente.

Recuerde lo siguiente al configurar este parámetro:

- No puede especificar una dirección IP de versión 6 (IPv6).
- Si utiliza la autenticación Kerberos, debe especificar un nombre de dominio.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(([a-zA-Z0-9\-\_]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-\_]*[A-Za-z0-9])$`

Obligatorio: sí

Subdirectory

Especifica el nombre del recurso compartido exportado por el servidor de archivos SMB donde se DataSync leerán o escribirán los datos. Puede incluir un subdirectorio en la ruta del recurso compartido (por ejemplo, `/path/to/subdirectory`). Asegúrese de que otros clientes de SMB de la red también puedan montar esta ruta.

Para copiar todos los datos del subdirectorio, DataSync debe poder montar el recurso compartido SMB y acceder a todos sus datos. Para obtener más información, consulte [Proporcionar DataSync acceso a los servidores de archivos SMB](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\+\.\/(\\)\$\\p{Zs}]+$`

Obligatorio: sí

Tags

Especifica las etiquetas que le ayudan a clasificar, filtrar y buscar sus recursos de AWS . Le recomendamos crear al menos una etiqueta de nombre para su ubicación.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

User

Especifica el usuario que puede montar y acceder a los archivos, carpetas y metadatos del servidor de archivos de SMB. Este parámetro solo se aplica si `AuthenticationType` está establecido en. NTLM

Para obtener información sobre cómo elegir un usuario con el nivel de acceso adecuado para la transferencia, consulte [Proporcionar DataSync acceso a los servidores de archivos SMB](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^[^\\x22\\x5B\\x5D\\/\\:;|=, +*?\\x3C\\x3E]{1,104}$`

Obligatorio: no

Sintaxis de la respuesta

```
{
  "LocationArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[LocationArn](#)

El ARN de la ubicación de SMB que creó.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Solicitud de ejemplo

En el siguiente ejemplo, se crea una ubicación para un sistema de archivos 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"
}
```

Respuesta de ejemplo

Una respuesta devuelve el ARN de ubicación de su servidor de archivos SMB.

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

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 una tarea, que define dónde y cómo AWS DataSync transfiere los datos.

Una tarea incluye una ubicación de origen, una ubicación de destino y opciones de transferencia (como límites de ancho de banda, la programación, entre otras opciones).

Important

Si planea transferir datos a o desde una ubicación de Amazon S3, consulte [cómo DataSync pueden afectar los cargos por solicitud de S3](#) y la [página de DataSync precios](#) antes de empezar.

Sintaxis de la solicitud

```
{
  "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"
}

```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[CloudWatchLogGroupArn](#)

Especifica el nombre de recurso de Amazon (ARN) de un grupo de CloudWatch registros de Amazon para supervisar la tarea.

Para las tareas del modo mejorado, no necesita especificar nada. DataSync envía automáticamente los registros a un grupo de CloudWatch registros denominado `/aws/datasync`.

Para obtener más información, consulte [Supervisar las transferencias de datos con CloudWatch registros](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 562 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-\0-9]+:[0-9]{12}:log-group:([^\:]*)(:\:*)?.$`

Obligatorio: no

DestinationLocationArn

Especifica el ARN de la ubicación de destino de la transferencia.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Excludes

Especifica los filtros de exclusión que definen los archivos, objetos y carpetas de la ubicación de origen que no se DataSync desean transferir. Para obtener más información y ejemplos, consulte [Especificar qué se DataSync transfiere mediante filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Obligatorio: no

Includes

Especifica incluir filtros que definan los archivos, objetos y carpetas de la ubicación de origen que DataSync desea transferir. Para obtener más información y ejemplos, consulte [Especificar lo que se DataSync transfiere mediante filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Obligatorio: no

ManifestConfig

Configura un manifiesto, que es una lista de archivos u objetos que se desean DataSync transferir. Para obtener más información y ejemplos de configuración, consulte [Especificar lo que se DataSync transfiere mediante un manifiesto](#).

Al usar este parámetro, la identidad de la persona que llama (el rol DataSync con el que estás usando) debe tener el `iam:PassRole` permiso. La [AWSDataSyncFullAccess](#) política incluye este permiso.

Tipo: objeto [ManifestConfig](#)

Obligatorio: no

[Name](#)

Especifica el nombre de la tarea.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Obligatorio: no

[Options](#)

Especifica la configuración de la tarea, como la conservación de los metadatos de los archivos y la verificación de la integridad de los datos, entre otras opciones.

Tipo: objeto [Options](#)

Obligatorio: no

[Schedule](#)

Especifica el momento en que quiere que la tarea se ejecute. Para obtener más información, consulte [Scheduling your task](#) (Programación de tareas).

Tipo: objeto [TaskSchedule](#)

Obligatorio: no

[SourceLocationArn](#)

Especifica el ARN de la ubicación de origen de la transferencia.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Tags

Las etiquetas que desea aplicar a la tarea.

Las etiquetas son pares clave-valor que ayudan a administrar, filtrar y buscar los recursos. DataSync

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

TaskMode

Especifica uno de los siguientes modos de tarea para la transferencia de datos:

- **ENHANCED**- Transfiere un número prácticamente ilimitado de objetos con un rendimiento superior al del modo Básico. Las tareas del modo mejorado optimizan el proceso de transferencia de datos al enumerar, preparar, transferir y verificar los datos en paralelo. El modo mejorado está disponible actualmente para las transferencias entre ubicaciones de Amazon S3, las transferencias entre Azure Blob y Amazon S3 sin un agente y las transferencias entre otras nubes y Amazon S3 sin un agente.



Note

Para crear una tarea en modo mejorado, el rol de IAM que utilice para llamar a la `CreateTask` operación debe tener el `iam:CreateServiceLinkedRole` permiso.

- **BASIC**(predeterminado): transfiere archivos u objetos entre el AWS almacenamiento y todas las demás DataSync ubicaciones compatibles. Las tareas del modo básico están sujetas a [cuotas](#) en cuanto al número de archivos, objetos y directorios de un conjunto de datos. El modo básico prepara, transfiere y verifica los datos de forma secuencial, lo que lo hace más lento que el modo mejorado para la mayoría de las cargas de trabajo.

Para obtener más información, consulte [Comprender las diferencias entre los modos de tarea.](#)

Tipo: cadena

Valores válidos: BASIC | ENHANCED

Obligatorio: no

[TaskReportConfig](#)

Especifica cómo desea configurar un informe de tareas, que proporciona información detallada sobre la DataSync transferencia. Para obtener más información, consulte [Supervisar DataSync las transferencias con informes de tareas](#).

Al usar este parámetro, la identidad de la persona que llama (el rol que utilizas DataSync) debe tener el `iam:PassRole` permiso. La [AWSDataSyncFullAccess](#) política incluye este permiso.

Tipo: objeto [TaskReportConfig](#)

Obligatorio: no

Sintaxis de la respuesta

```
{
  "TaskArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[TaskArn](#)

El nombre de recurso de Amazon (ARN) de la tarea.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Ejemplo de solicitud para una tarea en modo mejorado

En el siguiente ejemplo, se crea una DataSync tarea que utiliza el modo mejorado.

A diferencia de cuando se crean tareas en modo Básico, no es necesario especificar un grupo de CloudWatch registros de Amazon. Con las tareas del modo mejorado, envía DataSync automáticamente los registros de tareas a un grupo de registros denominado `/aws/datasync`. Si ese grupo de registros no existe en su cuenta Región de AWS, DataSync crea el grupo de registros en su nombre al crear la tarea.

```
{
  "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"
  }
}
```

Ejemplo de solicitud para una tarea en modo básico

En el siguiente ejemplo, se crea una DataSync tarea que utiliza el 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"
    }
  ]
}
```

Respuesta de ejemplo

La siguiente respuesta incluye el ARN de una tarea creada.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Elimina un recurso de AWS DataSync agente de su Cuenta de AWS.

Tenga en cuenta que esta operación (que no se puede deshacer) no elimina la máquina virtual (VM) del agente ni la EC2 instancia de Amazon de su entorno de almacenamiento. Para los siguientes pasos, puede eliminar la máquina virtual o la instancia de su entorno de almacenamiento o reutilizarla para [activar un nuevo agente](#).

Sintaxis de la solicitud

```
{
  "AgentArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[AgentArn](#)

El nombre de recurso de Amazon (ARN) del agente que se va a eliminar. Utilice la `ListAgents` operación para devolver una lista de agentes para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Elimina un recurso de ubicación de transferencia de AWS DataSync.

Sintaxis de la solicitud

```
{
  "LocationArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

LocationArn

El nombre de recurso de Amazon (ARN) de la ubicación que se va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Elimina un recurso de tarea de transferencia de AWS DataSync.

Sintaxis de la solicitud

```
{
  "TaskArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

TaskArn

Especifique las etiquetas que desea aplicar al nombre de recurso de Amazon (ARN) de la tarea que desea eliminar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Devuelve información sobre un AWS DataSync agente, como su nombre, tipo de punto final del servicio y estado.

Sintaxis de la solicitud

```
{  
  "AgentArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[AgentArn](#)

Especifica el nombre de recurso de Amazon (ARN) del DataSync agente sobre el que desea obtener información.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "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 respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AgentArn

El ARN del agente.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

La hora a la que se [activó](#) el agente.

Tipo: marca temporal

EndpointType

El tipo de [punto de conexión del servicio](#) al que está conectado el agente.

Tipo: cadena

Valores válidos: PUBLIC | PRIVATE_LINK | FIPS

LastConnectionTime

La última vez que el agente se comunicó con el DataSync servicio.

Tipo: marca temporal

Name

El nombre del agente.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Platform

Los detalles relacionados con la plataforma sobre el agente, como el número de versión.

Tipo: objeto [Platform](#)

PrivateLinkConfig

La configuración de red que usa el agente cuando se conecta a un [punto de conexión del servicio de VPC](#).

Tipo: objeto [PrivateLinkConfig](#)

Status

El estado del agente.

- Si el estado es ONLINE, el agente está configurado correctamente y listo para usarse.
- Si el estado es OFFLINE, el agente no ha estado en contacto con el DataSync durante cinco minutos o más. Esto puede suceder por varias razones. Para obtener más información, consulte [What do I do if my agent is offline?](#)

Tipo: cadena

Valores válidos: ONLINE | OFFLINE

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Solicitud de ejemplo

En el siguiente ejemplo, se arroja información sobre un agente especificado en una solicitud.

```
{
  "AgentArn": "arn:aws:datasync:us-east-2:111122223333:agent/agent-1234567890abcdef0"
}
```

Respuesta de ejemplo

El siguiente ejemplo de respuesta describe un agente que usa un punto de conexión de servicio 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"
  }
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)

- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para Microsoft Azure Blob Storage.

Sintaxis de la solicitud

```
{  
  "LocationArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[LocationArn](#)

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de transferencia de Azure Blob Storage.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "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 respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AccessTier](#)

El nivel de acceso al que desea transferir sus objetos o archivos. Esto solo se aplica cuando se utiliza la ubicación como destino de transferencia. Para obtener más información, consulte [Niveles de acceso](#).

Tipo: cadena

Valores válidos: HOT | COOL | ARCHIVE

[AgentArns](#)

Uno ARNs de los DataSync agentes que se pueden conectar con su contenedor de Azure Blob Storage.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

El método de autenticación que se DataSync utiliza para acceder a su Azure Blob Storage. DataSync puede acceder al almacenamiento de blobs mediante una firma de acceso compartido (SAS).

Tipo: cadena

Valores válidos: SAS | NONE

BlobType

El tipo de blob que desea que tengan sus objetos o archivos al transferirlos a Azure Blob Storage. Actualmente, DataSync solo admite el traslado de datos a Azure Blob Storage como bloques blobs. Para obtener más información sobre los tipos de blobs, consulte la [Documentación de Azure Blob Storage](#).

Tipo: cadena

Valores válidos: BLOCK

CmkSecretConfig

Describe la información de configuración de un secreto DataSync administrado, como un token de autenticación que se DataSync utiliza para acceder a una ubicación de almacenamiento específica, con una ubicación administrada por el cliente. AWS KMS key

Tipo: objeto [CmkSecretConfig](#)

CreationTime

La hora en que se creó la ubicación de transferencia de Azure Blob Storage.

Tipo: marca temporal

CustomSecretConfig

Describe la información de configuración de un secreto administrado por el cliente, como un token de autenticación que se DataSync utiliza para acceder a una ubicación de almacenamiento específica, con una ubicación administrada por el cliente. AWS KMS key

Tipo: objeto [CustomSecretConfig](#)

LocationArn

El ARN de la ubicación de transferencia de Azure Blob Storage.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

La URL del contenedor de Azure Blob Storage implicado en la transferencia.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\\-]+$`

[ManagedSecretConfig](#)

Describe la información de configuración de un secreto DataSync administrado, como un token de autenticación que se DataSync utiliza para acceder a una ubicación de almacenamiento específica. DataSync utiliza la clave KMS AWS administrada por defecto para cifrar este secreto. AWS Secrets Manager

Tipo: objeto [ManagedSecretConfig](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un sistema de archivos Amazon EFS.

Sintaxis de la solicitud

```
{  
  "LocationArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[LocationArn](#)

El nombre de recurso de Amazon (ARN) de la ubicación del sistema de archivos de Amazon EFS sobre el que desea obtener información.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "AccessPointArn": "string",  
  "CreationTime": number,  
  "Ec2Config": {  
    "SecurityGroupArns": [ "string" ],  
    "SubnetArn": "string"  
  }  
}
```

```
},  
"FileSystemAccessRoleArn": "string",  
"InTransitEncryption": "string",  
"LocationArn": "string",  
"LocationUri": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AccessPointArn

El ARN del punto de acceso que se DataSync utiliza para acceder al sistema de archivos Amazon EFS.

Para obtener más información, consulte [Acceso a sistemas de archivos restringidos](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: ^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

La hora en que se creó el registro.

Tipo: marca temporal

Ec2Config

La subred y los grupos de seguridad que se AWS DataSync utilizan para conectarse a uno de los [destinos de montaje](#) del sistema de archivos Amazon EFS.

Tipo: objeto [Ec2Config](#)

FileSystemAccessRoleArn

El rol AWS Identity and Access Management (IAM) que permite acceder DataSync al sistema de archivos Amazon EFS.

Para obtener más información, consulte [Crear un rol de DataSync IAM para el acceso al sistema de archivos.](#)

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam:[0-9]{12}:role/.*$`

[InTransitEncryption](#)

Indica si DataSync utiliza el cifrado Transport Layer Security (TLS) al transferir datos hacia o desde el sistema de archivos Amazon EFS.

Tipo: cadena

Valores válidos: NONE | TLS1_2

[LocationArn](#)

El ARN de la ubicación del sistema de archivos de Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

La URL de la ubicación del sistema de archivos de Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-\-]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes.](#)

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Solicitud de ejemplo

El siguiente ejemplo muestra cómo obtener información sobre una ubicación específica del sistema de archivos de Amazon EFS.

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/loc-12abcdef012345678"
}
```

Respuesta de ejemplo

El siguiente ejemplo devuelve detalles de ubicación sobre un sistema de archivos de 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/"
}
```

Respuesta de ejemplo: descripción de una ubicación para un sistema de archivos de Amazon EFS restringido

El siguiente ejemplo devuelve los detalles de ubicación de un sistema de archivos de Amazon EFS con acceso restringido, incluidos los elementos `AccessPointArn`, `FileSystemAccessRoleArn` y `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"
  }]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un sistema de archivos de Amazon FSx for Lustre.

Sintaxis de la solicitud

```
{  
  "LocationArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[LocationArn](#)

El nombre del recurso de Amazon (ARN) de la ubicación de FSx for Lustre que se va a describir.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "CreationTime": number,  
  "LocationArn": "string",  
  "LocationUri": "string",  
  "SecurityGroupArns": [ "string" ]  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La hora en que se creó la ubicación FSx de for Lustre.

Tipo: marca temporal

LocationArn

El nombre del recurso de Amazon (ARN) de la ubicación de FSx for Lustre que se describió.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

El URI de la ubicación de FSx for Lustre que se describió.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\\-]+$`

SecurityGroupArns

Los nombres de recursos de Amazon (ARNs) de los grupos de seguridad que están configurados FSx para el sistema de archivos de Lustre.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un sistema de archivos de Amazon FSx for NetApp ONTAP.

Note

Si su ubicación utiliza SMB, la operación `DescribeLocationFsxOntap` en realidad no devuelve un `Password`.

Sintaxis de la solicitud

```
{  
  "LocationArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

LocationArn

Especifica el nombre de recurso de Amazon (ARN) de la ubicación del sistema de archivos ONTAP sobre la que desea FSx obtener información.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
```



```

"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 respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La hora en que se creó el registro.

Tipo: marca temporal

FsxFilesystemArn

El ARN del sistema de archivos ONTAP. FSx

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):fsx:[a-z\-\0-9]*:[0-9]{12}:file-system/fs-.*$`

[LocationArn](#)

El ARN de la ubicación del sistema de archivos FSx de ONTAP.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

El identificador uniforme de recursos (URI) de la ubicación del sistema de archivos FSx de ONTAP.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\\-]+$`

[Protocol](#)

Especifica el protocolo de transferencia de datos que se AWS DataSync utiliza para acceder al sistema de FSx archivos de Amazon.

Tipo: objeto [FsxProtocol](#)

[SecurityGroupArns](#)

Los grupos de seguridad que se DataSync utilizan para acceder al sistema de archivos de ONTAP. FSx

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

El ARN de la máquina virtual de almacenamiento (SVM) del sistema de archivos de ONTAP en el que se copian los datos FSx hacia o desde donde se copian los datos.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 162 caracteres.

Patrón: `^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,}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un sistema de archivos Amazon FSx for OpenZFS.

Note

Los elementos de respuesta relacionados con SMB no son compatibles con la operación DescribeLocationFsxOpenZfs.

Sintaxis de la solicitud

```
{
  "LocationArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

LocationArn

El nombre del recurso de Amazon (ARN) de la FSx ubicación de OpenZFS que se va a describir.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
```

```

"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 respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La hora en que se creó la ubicación FSx de OpenZFS.

Tipo: marca temporal

LocationArn

El ARN de la FSx ubicación de OpenZFS que se describió.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):datasync:[a-z\n-0-9]+:[0-9]{12}:location/loc-[0-9a-z]{17}$`

[LocationUri](#)

El identificador uniforme de recursos (URI) de la FSx ubicación de OpenZFS que se describió.

Ejemplo: `fsxz://us-west-2.fs-1234567890abcdef02/fsx/folderA/folder`

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[Protocol](#)

El tipo de protocolo que se AWS DataSync utiliza para acceder al sistema de archivos.

Tipo: objeto [FsxProtocol](#)

[SecurityGroupArns](#)

El ARNs de los grupos de seguridad que están configurados FSx para el sistema de archivos OpenZFS.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un sistema de archivos de Amazon FSx para Windows File Server.

Sintaxis de la solicitud

```
{  
  "LocationArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[LocationArn](#)

Especifica el nombre de recurso de Amazon (ARN) de la ubicación del servidor FSx de archivos de Windows.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{  
  "CreationTime": number,  
  "Domain": "string",  
  "LocationArn": "string",  
  "LocationUri": "string",  
  "SecurityGroupArns": [ "string" ],  
  "User": "string"  
}
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

Hora en que se creó FSx la ubicación del servidor de archivos de Windows.

Tipo: marca temporal

[Domain](#)

El nombre del dominio de Microsoft Active Directory al que pertenece el sistema FSx de archivos del servidor de archivos de Windows.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 253 caracteres.

Patrón: `^[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}$`

[LocationArn](#)

El ARN de la ubicación del servidor FSx de archivos de Windows.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

El identificador uniforme de recursos (URI) de la ubicación del servidor FSx de archivos de Windows.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

SecurityGroupArns

Los grupos ARNs de EC2 seguridad de Amazon que proporcionan acceso a la subred preferida de su sistema de archivos.

Para obtener información sobre la configuración de grupos de seguridad para el acceso al sistema de archivos, consulte la [Guía del usuario de Amazon FSx for Windows File Server](#).

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

El usuario con los permisos para montar y acceder al sistema de archivos del servidor de archivos de Windows. FSx

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^[^\\x22\\x5B\\x5D\\/\\:;|=, +*?\\x3C\\x3E]{1,104}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un sistema de archivos distribuido Hadoop (HDFS).

Sintaxis de la solicitud

```
{
  "LocationArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

LocationArn

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de HDFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "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 respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AgentArns

Los ARNs DataSync agentes que se pueden conectar con su clúster de HDFS.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

El tipo de autenticación utilizado para determinar la identidad del usuario.

Tipo: cadena

Valores válidos: SIMPLE | KERBEROS

BlockSize

El tamaño de los bloques de datos que se escribirán en el clúster de HDFS.

Tipo: entero

Rango válido: valor mínimo de 1 048 576. Valor máximo de 1 073 741 824.

[CreationTime](#)

Es la hora en que se creó la ubicación del HDFS.

Tipo: marca temporal

[KerberosPrincipal](#)

La entidad principal de Kerberos con acceso a los archivos y carpetas del clúster de HDFS. Este parámetro se utiliza si `AuthenticationType` se define como `KERBEROS`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^.+`

[KmsKeyProviderUri](#)

El URI de Key Management Server (KMS) del clúster HDFS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `^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](#)

El ARN de la ubicación de HDFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

El URI de la ubicación de HDFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[NameNodes](#)

El NameNode que administra el espacio de nombres HDFS.

Tipo: matriz de objetos [HdfsNameNode](#)

Miembros de la matriz: número mínimo de 1 artículo.

[QopConfiguration](#)

La configuración de calidad de protección (QOP), que especifica la llamada a procedimiento remoto (RPC) y los ajustes de protección de transferencia de datos configurados en el clúster del sistema de archivos distribuido de Hadoop (HDFS).

Tipo: objeto [QopConfiguration](#)

[ReplicationFactor](#)

El número en el DataNodes que se van a replicar los datos al escribir en el clúster HDFS.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 512.

[SimpleUser](#)

El nombre de usuario utilizado para identificar al cliente en el sistema operativo host. Este parámetro se utiliza si `AuthenticationType` se define como `SIMPLE`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^[_A-Za-z0-9][_A-Za-z0-9]*$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un servidor de archivos de Network File System (NFS).

Sintaxis de la solicitud

```
{
  "LocationArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

LocationArn

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de NFS sobre la que desea obtener información.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "CreationTime": number,
  "LocationArn": "string",
  "LocationUri": "string",
  "MountOptions": {
    "Version": "string"
  }
}
```

```
},  
  "OnPremConfig": {  
    "AgentArns": [ "string" ]  
  }  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CreationTime](#)

Es la hora en que se creó la ubicación de NFS.

Tipo: marca temporal

[LocationArn](#)

El ARN de la ubicación de NFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

El URI de la ubicación de NFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\\-]+$`

[MountOptions](#)

Las opciones de montaje que se DataSync utilizan para montar el servidor de archivos NFS.

Tipo: objeto [NfsMountOptions](#)

[OnPremConfig](#)

Los AWS DataSync agentes que se pueden conectar al servidor de archivos del Network File System (NFS).

Tipo: objeto [OnPremConfig](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo, se arroja información sobre la ubicación de NFS especificada en el ejemplo de solicitud.

Solicitud de muestra

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50aa"
}
```

Ejemplo

Este ejemplo ilustra un uso de DescribeLocationNfs.

Respuesta de ejemplo

```
{
  "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" ]
  }
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un sistema de almacenamiento de objetos.

Sintaxis de la solicitud

```
{
  "LocationArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[LocationArn](#)

Especifica el nombre de recurso de Amazon (ARN) de la ubicación del sistema de almacenamiento de objetos.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "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 respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AccessKey](#)

La clave de acceso (por ejemplo, un nombre de usuario) requerida para autenticarse en el sistema de almacenamiento de objetos.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 200 caracteres.

Patrón: `^.*$`

[AgentArns](#)

Los ARNs DataSync agentes que se pueden conectar con el sistema de almacenamiento de objetos.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

Describe la información de configuración de un secreto DataSync administrado, como un token de autenticación o un conjunto de credenciales que se DataSync utiliza para acceder a una ubicación de transferencia específica, y de un secreto administrado por el cliente AWS KMS key.

Tipo: objeto [CmkSecretConfig](#)

[CreationTime](#)

La hora en que se creó el registro.

Tipo: marca temporal

[CustomSecretConfig](#)

Describe la información de configuración de un secreto administrado por el cliente, como un token de autenticación o un conjunto de credenciales que se DataSync utiliza para acceder a una ubicación de transferencia específica, y una administrada por el cliente. AWS KMS key

Tipo: objeto [CustomSecretConfig](#)

[LocationArn](#)

El ARN de la ubicación del sistema de almacenamiento de objetos.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

El URI de la ubicación del sistema de almacenamiento de objetos.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[ManagedSecretConfig](#)

Describe la información de configuración de un secreto DataSync administrado, como un token de autenticación o un conjunto de credenciales que se DataSync utiliza para acceder a una ubicación de transferencia específica. DataSync utiliza la clave KMS AWS administrada por defecto para cifrar este secreto. AWS Secrets Manager

Tipo: objeto [ManagedSecretConfig](#)

[ServerCertificate](#)

La cadena de certificados DataSync para autenticarse en el sistema de almacenamiento de objetos si el sistema utiliza una entidad de certificación (CA) privada o autofirmada.

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 32 768 caracteres.

[ServerPort](#)

El puerto en el que el servidor de almacenamiento de objetos acepta el tráfico de red entrante (por ejemplo, el puerto 443).

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 65 536.

[ServerProtocol](#)

El protocolo que utiliza su sistema de almacenamiento de objetos para comunicarse.

Tipo: cadena

Valores válidos: HTTPS | HTTP

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un bucket de S3.

Sintaxis de la solicitud

```
{
  "LocationArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

LocationArn

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de Amazon S3.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "AgentArns": [ "string" ],
  "CreationTime": number,
  "LocationArn": "string",
  "LocationUri": "string",
  "S3Config": {
    "BucketAccessRoleArn": "string"
  },
}
```

```
"S3StorageClass": "string"  
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AgentArns

Los DataSync agentes desplegados en su Outpost cuando trabajaba con Amazon S3 en Outposts. ARNs

Para obtener más información, consulte [Implementar su DataSync agente en](#). AWS Outposts

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

La hora en que se creó la ubicación de Amazon S3.

Tipo: marca temporal

LocationArn

El ARN de la ubicación de Amazon S3.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

Es la dirección URL de la ubicación de Amazon S3 que se describió.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[S3Config](#)

Especifica el nombre de recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que se DataSync utiliza para acceder al bucket de S3.

Para obtener más información, consulte [Proporcionar DataSync acceso a los buckets de S3](#).

Tipo: objeto [S3Config](#)

[S3StorageClass](#)

Cuando Amazon S3 es una ubicación de destino, esta es la clase de almacenamiento que ha elegido para sus objetos.

Algunas clases de almacenamiento tienen comportamientos que pueden afectar los costos de almacenamiento de Amazon S3. Para obtener más información, consulte [Storage class considerations with Amazon S3 transfers](#).

Tipo: cadena

Valores válidos: STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo, se arroja información sobre la ubicación de Amazon S3 especificada en el ejemplo de solicitud.

Solicitud de muestra

```
{
  "LocationArn": "arn:aws:datasync:us-east-2:111222333444:location/
loc-07db7abfc326c50s3"
}
```

Ejemplo

Este ejemplo ilustra un uso de DescribeLocation S3.

Respuesta de ejemplo

```
{
  "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"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona detalles sobre cómo se configura una ubicación de AWS DataSync transferencia para un servidor de archivos de bloque de mensajes del servidor (SMB).

Sintaxis de la solicitud

```
{
  "LocationArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[LocationArn](#)

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de SMB sobre la que desea obtener información.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "AgentArns": [ "string" ],
  "AuthenticationType": "string",
  "CreationTime": number,
  "DnsIpAddresses": [ "string" ],
  "Domain": "string",
  "KerberosPrincipal": "string",
```



```
"LocationArn": "string",
"LocationUri": "string",
"MountOptions": {
  "Version": "string"
},
"User": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[AgentArns](#)

Los ARNs DataSync agentes que se pueden conectar con el servidor de archivos SMB.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

El protocolo de autenticación que se DataSync utiliza para conectarse al servidor de archivos SMB.

Tipo: cadena

Valores válidos: NTLM | KERBEROS

[CreationTime](#)

Es la hora en que se creó la ubicación SMB.

Tipo: marca temporal

[DnsIpAddresses](#)

Las IPv4 direcciones de los servidores DNS a los que pertenece el servidor de archivos SMB. Este elemento solo se aplica si `AuthenticationType` está establecido en. KERBEROS

Tipo: matriz de cadenas

Miembros de la matriz: número máximo de 2 elementos.

Limitaciones de longitud: longitud mínima de 7. Longitud máxima de 39.

Patrón: `\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]{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](#)

El nombre del dominio de Windows al que pertenece el servidor de archivos SMB. Este elemento solo se aplica si `AuthenticationType` está establecido en. NTLM

Tipo: cadena

Limitaciones de longitud: longitud máxima de 253 caracteres.

Patrón: `^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}$`

[KerberosPrincipal](#)

El principal de Kerberos que tiene permiso para acceder a los archivos, las carpetas y los metadatos de los archivos del servidor de archivos SMB.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^\.+`

[LocationArn](#)

El ARN de la ubicación de SMB.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

El URI de la ubicación de SMB.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

[MountOptions](#)

La versión del protocolo SMB que se DataSync utiliza para acceder al servidor de archivos SMB.

Tipo: objeto [SmbMountOptions](#)

[User](#)

El usuario que puede montar y acceder a los archivos, carpetas y metadatos del servidor de archivos de SMB. Este elemento solo se aplica si `AuthenticationType` está establecido en NTLM

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^[^\\x22\\x5B\\x5D\\/\\:;|, +*?\\x3C\\x3E]{1,104}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Ejemplo

Este ejemplo ilustra un uso de DescribeLocationSmb.

Solicitud de muestra

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

Ejemplo

Este ejemplo ilustra un uso de DescribeLocationSmb.

Respuesta de ejemplo

```
{
  "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"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)

- [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

Proporciona información sobre una tarea, que define dónde y cómo AWS DataSync transfiere los datos.

Sintaxis de la solicitud

```
{
  "TaskArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

TaskArn

Especifique el nombre de recurso de Amazon (ARN) de la tarea de transferencia sobre la que desea obtener información.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "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 respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[CloudWatchLogGroupArn](#)

El nombre de recurso de Amazon (ARN) de un grupo de CloudWatch registros de Amazon para supervisar la tarea.

Para obtener más información, consulte [Supervisión de las transferencias de datos con CloudWatch registros](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 562 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-\0-9]+:[0-9]{12}:log-group:([^\:]*)(:\:)*$`

[CreationTime](#)

La hora en que se creó la tarea.

Tipo: marca temporal

[CurrentTaskExecutionArn](#)

El ARN de la ejecución de tarea más reciente.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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](#)

El ARN de la ubicación de destino de la transferencia.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

Las [interfaces ARNs de red](#) que se DataSync crearon para su ubicación de destino.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:aws[\-a-z]{0,}:ec2:[a-z\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

ErrorCode

Si hay algún problema con la tarea, puede usar el código de error como ayuda para solucionar el problema. Para obtener más información, consulta [Solución de problemas relacionados con DataSync las transferencias](#).

Tipo: cadena

ErrorDetail

Si hay algún problema con la tarea, puede usar los detalles del error como ayuda para solucionar el problema. Para obtener más información, consulta [Solución de problemas relacionados con DataSync las transferencias](#).

Tipo: cadena

Excludes

Los filtros de exclusión que definen los archivos, objetos y carpetas de la ubicación de origen que no DataSync desea transferir. Para obtener más información y ejemplos, consulte [Especificar qué se DataSync transfiere mediante filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Includes

Incluyen filtros que definen los archivos, objetos y carpetas de la ubicación de origen que DataSync desea transferir. Para obtener más información y ejemplos, consulte [Especificar qué se DataSync transfiere mediante filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

ManifestConfig

La configuración del manifiesto que enumera los archivos u objetos que DataSync desea transferir. Para obtener más información, consulta [Especificar qué se DataSync transfiere mediante un manifiesto](#).

Tipo: objeto [ManifestConfig](#)

Name

El nombre de la tarea.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Options

La configuración de la tarea. Por ejemplo, qué metadatos del archivo se conservan, cómo se verifica la integridad de los datos al final de la transferencia, límites de ancho de banda, entre otras opciones.

Tipo: objeto [Options](#)

Schedule

El momento en que quiere que la tarea se ejecute. Para obtener más información, consulte [Scheduling your task](#) (Programación de tareas).

Tipo: objeto [TaskSchedule](#)

ScheduleDetails

Los detalles de su [programa de tareas](#).

Tipo: objeto [TaskScheduleDetails](#)

SourceLocationArn

El ARN de la ubicación de origen de la transferencia.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

Las [interfaces ARNs de red](#) que se DataSync crearon para su ubicación de origen.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:aws[\\-a-z]{0,}:ec2:[a-z\\-0-9]*:[0-9]{12}:network-interface/eni-[0-9a-f]+$`

Status

El estado de la tarea. Para obtener información sobre el significado de cada estado, consulte [Estados de las tareas](#).

Tipo: cadena

Valores válidos: AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE

TaskArn

El ARN de la tarea.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

El modo de tarea que está utilizando. Para obtener más información, consulte [Elegir un modo de tarea para la transferencia de datos](#).

Tipo: cadena

Valores válidos: BASIC | ENHANCED

[TaskReportConfig](#)

La configuración del informe de tareas, que proporciona información detallada sobre la DataSync transferencia. Para obtener más información, consulta [Supervisar tus DataSync transferencias con informes de tareas](#).

Tipo: objeto [TaskReportConfig](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Solicitud de ejemplo

En el siguiente ejemplo se especifica el ARN de una DataSync tarea sobre la que se va a obtener información.

```
{
  "TaskArn": "arn:aws:datasync:us-east-2:111222333444:task/task-08de6e6697796f026"
}
```

Respuesta de ejemplo

En el siguiente ejemplo, se muestra una DescribeTask respuesta.

```
{
```

```
"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:*"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Proporciona información sobre la ejecución de la AWS DataSync tarea. Puede utilizar esta operación para ayudar a supervisar el progreso de una transferencia de datos en curso o comprobar los resultados de la transferencia.

Note

Algunos elementos de `DescribeTaskExecution` respuesta solo son relevantes para un modo de tarea específico. Para obtener más información, consulte [Comprender las diferencias entre los modos de tarea](#) y [Comprender los contadores de rendimiento de la transferencia de datos](#).

Sintaxis de la solicitud

```
{  
  "TaskExecutionArn": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[TaskExecutionArn](#)

Especifique el nombre de recurso de Amazon (ARN) de la tarea de ejecución sobre la que desea obtener información.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "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 respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BytesCompressed

El número de bytes físicos que se DataSync transfieren a través de la red después de la compresión (si la compresión es posible). Este número suele ser inferior a, [BytesTransferred](#) a menos que los datos no se puedan comprimir.

Tipo: largo

[BytesTransferred](#)

El número de bytes que se DataSync envían a la red antes de la compresión (si la compresión es posible). Para conocer el número de bytes transferidos a través de la red, consulte [BytesCompressed](#).

Tipo: largo

[BytesWritten](#)

El número de bytes lógicos que DataSync realmente se escriben en la ubicación de destino.

Tipo: largo

[EndTime](#)

Hora a la que finaliza la tarea de transferencia.

Tipo: marca temporal

[EstimatedBytesToTransfer](#)

El número de bytes lógicos que se DataSync espera escribir en la ubicación de destino.

Tipo: largo

[EstimatedFilesToDelete](#)

El número de archivos, objetos y directorios que se DataSync espera eliminar en la ubicación de destino. Si no [configura la tarea](#) para eliminar datos del destino que no estén en el origen, el valor siempre será 0.

Tipo: largo

[EstimatedFilesToTransfer](#)

La cantidad de archivos, objetos y directorios que se DataSync espera transferir a través de la red. Este valor se calcula mientras DataSync [se prepara](#) la transferencia.

La forma en que se calcula depende principalmente de la configuración del [modo de transferencia](#) de la tarea:

- Si TransferMode está configurado como CHANGED: el cálculo se basa en comparar el contenido de las ubicaciones de origen y destino, y en determinar la diferencia que debe transferirse. La diferencia puede incluir:
 - Todo lo que se añada o modifique en la ubicación de origen.

- Todo lo que se encuentre en ambas ubicaciones y que se haya modificado en el destino después de una transferencia inicial (a menos que [OverwriteMode](#) esté configurado en NEVER).
- (Solo en el modo de tarea básica) El número de elementos que se DataSync espera eliminar (si [PreserveDeletedFiles](#) está configurado en REMOVE).
- Si TranseMode está establecido en ALL: el cálculo se basa únicamente en los elementos que DataSync se encuentran en la ubicación de origen.

Tipo: largo

[Excludes](#)

Una lista de reglas de filtrado que excluyen datos específicos durante la transferencia. Para obtener más información y ejemplos, consulte [Filtrar los datos transferidos por DataSync](#).

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

[FilesDeleted](#)

El número de archivos, objetos y directorios que DataSync realmente se eliminan en la ubicación de destino. Si no [configura la tarea](#) para eliminar datos del destino que no estén en el origen, el valor siempre será 0.

Tipo: largo

[FilesFailed](#)

El número de objetos que DataSync no se pueden preparar, transferir, verificar ni eliminar durante la ejecución de la tarea.

Note

Se aplica únicamente a las [tareas del modo mejorado](#).

Tipo: objeto [TaskExecutionFilesFailedDetail](#)

[FilesListed](#)

El número de objetos que DataSync se encuentran en sus ubicaciones.

 Note

Se aplica solo a las [tareas del modo mejorado](#).

Tipo: objeto [TaskExecutionFilesListedDetail](#)

[FilesPrepared](#)

El número de objetos que DataSync se intentarán transferir tras comparar las ubicaciones de origen y destino.

 Note

Se aplica solo a las [tareas del modo mejorado](#).

Este contador no se aplica si configura la tarea para [transferir todos los datos](#). En ese escenario, DataSync copia todo desde el origen hasta el destino sin comparar las diferencias entre las ubicaciones.

Tipo: largo

[FilesSkipped](#)

El número de archivos, objetos y directorios que se DataSync omiten durante la transferencia.

Tipo: largo

[FilesTransferred](#)

El número de archivos, objetos y directorios que DataSync realmente se transfieren a través de la red. Este valor se actualiza periódicamente durante la ejecución de la tarea cuando se lee algo del origen y se envía a través de la red.

Si DataSync no se puede transferir algo, este valor puede ser inferior a `aEstimatedFilesToTransfer`. Este valor también puede ser mayor que `EstimatedFilesToTransfer` en algunos casos. Este elemento es específico de la implementación para algunos tipos de ubicaciones, así que no lo utilices como una indicación exacta de lo que se está transfiriendo ni para supervisar la ejecución de la tarea.

Tipo: largo

FilesVerified

El número de archivos, objetos y directorios que se DataSync verifica durante la transferencia.

Note

Al configurar la tarea para [comprobar únicamente los datos que se transfieren](#), DataSync no comprueba los directorios en algunas situaciones ni los archivos que no se transfieren.

Tipo: largo

Includes

Una lista de reglas de filtrado que incluyen datos específicos durante la transferencia. Para obtener más información y ejemplos, consulte [Filtrar los datos transferidos por DataSync](#).

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

LaunchTime

La hora a la que realmente comienza la ejecución de la tarea. Para las tareas que no están en cola, LaunchTime y StartTime suelen ser las mismas. En el caso de las tareas en cola, LaunchTime suele ser más tarde que StartTime porque las tareas previamente puestas en cola deben terminar de ejecutarse antes de que puedan comenzar las tareas más nuevas.

Tipo: marca temporal

ManifestConfig

La configuración del manifiesto que enumere los archivos y los objetos a transferir. Para obtener más información, consulte [Especificar qué se DataSync transfiere mediante un manifiesto](#).

Tipo: objeto [ManifestConfig](#)

Options

Indica cómo está configurada la tarea de transferencia. Estas opciones incluyen la forma en que DataSync gestiona los archivos, los objetos y sus metadatos asociados durante la transferencia. También puede especificar cómo verificar la integridad de los datos y establecer límites de ancho de banda para su tarea, entre otras opciones.

Cada opción tiene un valor predeterminado. A menos que lo necesites, no tienes que configurar ninguna opción antes de llamar [StartTaskExecution](#).

También puede anular sus opciones de tarea para cada ejecución de tareas. Por ejemplo, es posible que desee ajustar el `LogLevel` para una ejecución individual.

Tipo: objeto [Options](#)

[ReportResult](#)

Indica si DataSync se ha generado un [informe de tareas](#) completo para tu transferencia.

Tipo: objeto [ReportResult](#)

[Result](#)

El resultado de la ejecución de la tarea.

Tipo: objeto [TaskExecutionResultDetail](#)

[StartTime](#)

La hora a la que se DataSync envía la solicitud para iniciar la ejecución de la tarea. Para las tareas que no están en cola, `LaunchTime` y `StartTime` suelen ser las mismas. En el caso de las tareas en cola, `LaunchTime` suele ser más tarde que `StartTime` porque las tareas previamente puestas en cola deben terminar de ejecutarse antes de que puedan comenzar las tareas más nuevas.

Tipo: marca temporal

[Status](#)

El estado de la ejecución de la tarea.

Para obtener información detallada sobre los estados de ejecución de las tareas, consulte [Task execution statuses](#).

Tipo: cadena

Valores válidos: QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR

[TaskExecutionArn](#)

El ARN de ejecución de la tarea sobre la que quería información. `TaskExecutionArn` es jerárquico e incluye `TaskArn` para la tarea que se ejecutó.

Por ejemplo, un valor de `TaskExecution` con el ARN `arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2/execution/exec-08ef1e88ec491019b` ejecutó la tarea con el ARN `arn:aws:datasync:us-east-1:111222333444:task/task-0208075f79cedf4a2`.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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

El modo de tareas que estás utilizando. Para obtener más información, consulte [Elegir un modo de tarea para la transferencia de datos](#).

Tipo: cadena

Valores válidos: BASIC | ENHANCED

TaskReportConfig

La configuración del informe de tareas, que proporciona información detallada sobre la DataSync transferencia. Para obtener más información, consulte [Creating a task report](#).

Tipo: objeto [TaskReportConfig](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Solicitud de ejemplo

En este ejemplo se ilustra una solicitud de `DescribeTaskExecution`.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/execution/exec-1234abcd1234abcd1"
}
```

Ejemplo de respuesta 1 para la ejecución de una tarea en modo mejorado

El siguiente ejemplo describe la ejecución de una DataSync tarea que utiliza el modo mejorado. La ejecución también transfiere datos específicos mediante los filtros de exclusión e inclusión.

```
{
  "TaskExecutionArn": "arn:aws:datasync:us-east-1:111222333444:task/task-
aaaabbbbccccddddf/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
    }
}

```

Ejemplo de respuesta 2 para la ejecución de una tarea en modo mejorado

El siguiente ejemplo describe la ejecución de otra DataSync tarea que utiliza el modo mejorado. En esta situación, la ejecución transfiere datos específicos mediante un manifiesto en lugar 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
    }
}

```

```
}
```

Ejemplo de respuesta para la ejecución de una tarea en modo básico

El siguiente ejemplo describe la ejecución de una DataSync tarea que utiliza el 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"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Devuelve una lista de AWS DataSync agentes que pertenecen a una Cuenta de AWS de las Región de AWS especificadas en la solicitud.

Con la paginación, puede reducir la cantidad de agentes devueltos en una respuesta. Si obtiene una lista truncada de agentes en una respuesta, la respuesta contiene un marcador que puede especificar en su próxima solicitud para obtener la siguiente página de agentes.

ListAgents acaba siendo coherente. Esto significa que es posible que el resultado de ejecutar la operación no refleje que acaba de crear o eliminar un agente. Por ejemplo, si crea un agente con [CreateAgenty](#) lo ejecuta inmediatamenteListAgents, es posible que ese agente no aparezca inmediatamente en la lista. En situaciones como esta, siempre puede confirmar si un agente se ha creado (o eliminado) mediante [DescribeAgent](#).

Sintaxis de la solicitud

```
{
  "MaxResults": number,
  "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[MaxResults](#)

Especifica el número máximo de DataSync agentes que se deben incluir en una respuesta. De forma predeterminada, una respuesta muestra un máximo de 100 agentes.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 100.

Obligatorio: no

[NextToken](#)

Especifica una cadena opaca que indica la posición en la que debe comenzar la siguiente lista de resultados de la respuesta.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: [a-zA-Z0-9=_-]+

Obligatorio: no

Sintaxis de la respuesta

```
{
  "Agents": [
    {
      "AgentArn": "string",
      "Name": "string",
      "Platform": {
        "Version": "string"
      },
      "Status": "string"
    }
  ],
  "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[Agents](#)

Una lista de sus DataSync agentes Cuenta de AWS en los Región de AWS especificados en la solicitud. La lista está ordenada por los nombres de los recursos de Amazon (ARNs) de los agentes.

Tipo: matriz de objetos [AgentListEntry](#)

NextToken

Es la cadena opaca que indica la posición en la que debe comenzar la siguiente lista de resultados de la respuesta.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: [a-zA-Z0-9=_-]+

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Devuelve una lista de ubicaciones de origen y destino.

Si tiene más ubicaciones de las que se muestran en una respuesta (es decir, la respuesta devuelve solo una lista truncada de sus agentes), la respuesta incluye un token que puede especificar en su próxima solicitud para buscar la siguiente página de ubicaciones.

Sintaxis de la solicitud

```
{
  "Filters": [
    {
      "Name": "string",
      "Operator": "string",
      "Values": [ "string" ]
    }
  ],
  "MaxResults": number,
  "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[Filters](#)

Puede utilizar filtros de API para acotar la lista de recursos devueltos por ListLocations. Por ejemplo, para recuperar todas las tareas en una ubicación de origen específica, puede utilizar ListLocations con el nombre del filtro LocationType S3 y Operator Equals.

Tipo: matriz de objetos [LocationFilter](#)

Obligatorio: no

[MaxResults](#)

Número máximo de ubicaciones que se devolverán.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 100.

Obligatorio: no

[NextToken](#)

Es una cadena opaca que indica la posición en la que debe comenzar la siguiente lista de ubicaciones.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: [a-zA-Z0-9=_-]+

Obligatorio: no

Sintaxis de la respuesta

```
{
  "Locations": [
    {
      "LocationArn": "string",
      "LocationUri": "string"
    }
  ],
  "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[Locations](#)

Es una matriz que incluye una lista de ubicaciones.

Tipo: matriz de objetos [LocationListEntry](#)

NextToken

Es una cadena opaca que indica la posición en la que debe comenzar a arrojar la siguiente lista de ubicaciones.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: [a-zA-Z0-9=_-]+

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Devuelve todas las etiquetas asociadas a un AWS recurso.

Sintaxis de la solicitud

```
{
  "MaxResults": number,
  "NextToken": "string",
  "ResourceArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[MaxResults](#)

Especifica cuántos resultados quiere obtener en la respuesta.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 100.

Obligatorio: no

[NextToken](#)

Especifica una cadena opaca que indica la posición en la que debe comenzar la siguiente lista de resultados de la respuesta.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: `[a-zA-Z0-9=_- ]+`

Obligatorio: no

ResourceArn

Especifica el nombre de recurso de Amazon (ARN) del recurso sobre el que desea etiquetar información.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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})?>`

Obligatorio: sí

Sintaxis de la respuesta

```
{
  "NextToken": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Es la cadena opaca que indica la posición en la que debe comenzar la siguiente lista de resultados de la respuesta.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: [a-zA-Z0-9=_-]+

Tags

Matriz de etiquetas que se aplican al recurso especificado.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. La cantidad máxima es de 55 elementos.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Devuelve una lista de las ejecuciones de una tarea AWS DataSync de transferencia.

Sintaxis de la solicitud

```
{
  "MaxResults": number,
  "NextToken": "string",
  "TaskArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[MaxResults](#)

Especifica cuántos resultados desea obtener en la respuesta.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 100.

Obligatorio: no

[NextToken](#)

Especifica una cadena opaca que indica la posición en la que debe comenzar la siguiente lista de resultados de la respuesta.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: `[a-zA-Z0-9=_- ]+`

Obligatorio: no

[TaskArn](#)

Especifique el nombre de recurso de Amazon (ARN) de la tarea de ejecución sobre la que desea obtener información.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

Sintaxis de la respuesta

```
{
  "NextToken": "string",
  "TaskExecutions": [
    {
      "Status": "string",
      "TaskExecutionArn": "string",
      "TaskMode": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

Es la cadena opaca que indica la posición en la que debe comenzar la siguiente lista de resultados de la respuesta.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: [a-zA-Z0-9=_-]+

[TaskExecutions](#)

Una lista de las ejecuciones de la tarea.

Tipo: matriz de objetos [TaskExecutionListEntry](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Devuelve una lista de las AWS DataSync tareas que ha creado.

Sintaxis de la solicitud

```
{
  "Filters": [
    {
      "Name": "string",
      "Operator": "string",
      "Values": [ "string" ]
    }
  ],
  "MaxResults": number,
  "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[Filters](#)

Puede utilizar filtros de API para acotar la lista de recursos devueltos por ListTasks. Por ejemplo, para recuperar todas las tareas en una ubicación de origen específica, puede utilizar ListTasks con el nombre del filtro LocationId y Operator Equals con el ARN de la ubicación.

Tipo: matriz de objetos [TaskFilter](#)

Obligatorio: no

[MaxResults](#)

Número máximo de filas que se devolverán.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 100.

Obligatorio: no

[NextToken](#)

Cadena opaca que indica la posición en la que debe comenzar la siguiente lista de tareas.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: [a-zA-Z0-9=_-]+

Obligatorio: no

Sintaxis de la respuesta

```
{
  "NextToken": "string",
  "Tasks": [
    {
      "Name": "string",
      "Status": "string",
      "TaskArn": "string",
      "TaskMode": "string"
    }
  ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[NextToken](#)

Cadena opaca que indica la posición en la que debe comenzar a devolver la siguiente lista de tareas.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 65 535 caracteres.

Patrón: [a-zA-Z0-9=_-]+

Tasks

Lista de todas las tareas devueltas.

Tipo: matriz de objetos [TaskListEntry](#)

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 una tarea AWS DataSync de transferencia. Para cada tarea, solo puede ejecutar una tarea a la vez.

La ejecución de una tarea consta de varios pasos. Para obtener más información, consulte [Task execution statuses](#).

Important

Si planea transferir datos a o desde una ubicación de Amazon S3, consulte [cómo DataSync pueden afectar los cargos por solicitud de S3](#) y la [página de DataSync precios](#) antes de empezar.

Sintaxis de la solicitud

```
{
  "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"  
  }  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[Excludes](#)

Especifica una lista de reglas de filtro que determina qué archivos se excluyen de una tarea. La lista contiene una única cadena de filtro que consiste en los patrones que se excluyen. Los patrones están delimitados por “|” (es decir, una tubería), por ejemplo, “/folder1|/folder2”.

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Obligatorio: no

[Includes](#)

Especifica una lista de reglas de filtro que determina qué archivos se incluyen al ejecutar una tarea. El patrón debe contener una única cadena de filtro que consta de los patrones que se van a incluir. Los patrones están delimitados por “|” (es decir, una tubería), por ejemplo, “/folder1|/folder2”.

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Obligatorio: no

[ManifestConfig](#)

Configura un manifiesto, que es una lista de archivos u objetos que desea DataSync transferir. Para obtener más información y ejemplos de configuración, consulte [Especificar lo que se DataSync transfiere mediante un manifiesto](#).

Al usar este parámetro, la identidad de la persona que llama (el rol DataSync con el que estás usando) debe tener el `iam:PassRole` permiso. La [AWSDataSyncFullAccess](#) política incluye este permiso.

Para eliminar una configuración de manifiesto, especifique este parámetro como vacío.

Tipo: objeto [ManifestConfig](#)

Obligatorio: no

[OverrideOptions](#)

Indica cómo está configurada la tarea de transferencia. Estas opciones incluyen la forma en que DataSync gestiona los archivos, los objetos y sus metadatos asociados durante la transferencia. También puede especificar cómo verificar la integridad de los datos y establecer límites de ancho de banda para su tarea, entre otras opciones.

Cada opción tiene un valor predeterminado. A menos que lo necesites, no tienes que configurar ninguna opción antes de llamar [StartTaskExecution](#).

También puede anular sus opciones de tarea para cada ejecución de tareas. Por ejemplo, es posible que desee ajustar el `LogLevel` para una ejecución individual.

Tipo: objeto [Options](#)

Obligatorio: no

[Tags](#)

Especifica las etiquetas que desea aplicar al nombre de recurso de Amazon (ARN) que representa la ejecución de la tarea.

Las etiquetas son pares clave-valor que te ayudan a administrar, filtrar y buscar tus DataSync recursos.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: no

[TaskArn](#)

Especifica el nombre de recurso de Amazon (ARN) de la tarea que desea iniciar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

[TaskReportConfig](#)

Especifica cómo desea configurar un informe de tareas, que proporciona información detallada sobre la transferencia. DataSync Para obtener más información, consulte [Supervisar DataSync las transferencias con informes de tareas](#).

Al usar este parámetro, la identidad de la persona que llama (el rol DataSync con el que estás usando) debe tener el `iam:PassRole` permiso. La [AWSDataSyncFullAccess](#) política incluye este permiso.

Para eliminar una configuración de informe de tarea, especifique este parámetro como vacío.

Tipo: objeto [TaskReportConfig](#)

Obligatorio: no

Sintaxis de la respuesta

```
{
  "TaskExecutionArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

[TaskExecutionArn](#)

El ARN de la ejecución de la tarea en ejecución.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Ejemplos

Solicitud de ejemplo

En el siguiente ejemplo, se inicia la ejecución de una tarea mediante las opciones predeterminadas para la tarea 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"
```

```
}
```

Respuesta de ejemplo

Este ejemplo ilustra un uso de `StartTaskExecution`.

```
{  
  "TaskExecutionArn": "arn:aws:datasync:us-east-2:111222333444:task/  
task-08de6e6697796f026/execution/exec-04ce9d516d69bd52f"  
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 una etiqueta a un AWS recurso. Una etiqueta es un par clave-valor que le puede ayudar a administrar, filtrar y buscar sus recursos.

Estos incluyen AWS DataSync recursos, como ubicaciones, tareas y ejecuciones de tareas.

Sintaxis de la solicitud

```
{
  "ResourceArn": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

ResourceArn

Especifica el nombre de recurso de Amazon (ARN) del recurso al que se va a aplicar la etiqueta.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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})?$`

Obligatorio: sí

Tags

Las etiquetas que desea añadir al recurso especificado.

Tipo: matriz de objetos [TagListEntry](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos.

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Elimina las etiquetas de un AWS recurso.

Sintaxis de la solicitud

```
{
  "Keys": [ "string" ],
  "ResourceArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[Keys](#)

Especifica las claves de las etiquetas que quiere eliminar.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=. _:/-]+$`

Obligatorio: sí

[ResourceArn](#)

Especifica el nombre de recurso de Amazon (ARN) del recurso del que se van a eliminar las etiquetas.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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})?&
```

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Actualiza el nombre de un AWS DataSync agente.

Sintaxis de la solicitud

```
{  
  "AgentArn": "string",  
  "Name": "string"  
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[AgentArn](#)

El nombre de recurso de Amazon (ARN) del agente que hay que actualizar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

[Name](#)

El nombre que desea usar para configurar el agente.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\\s+=. _:@/-]+$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 las siguientes configuraciones de la ubicación de transferencia de Microsoft Azure Blob Storage con la que está utilizando. AWS DataSync

Para obtener más información, consulte [Configuración de DataSync transferencias con Azure Blob Storage](#).

Sintaxis de la solicitud

```
{
  "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"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

AccessTier

Especifica el nivel de acceso al que desea transferir sus objetos o archivos. Esto solo se aplica cuando se utiliza la ubicación como destino de transferencia. Para obtener más información, consulte [Niveles de acceso](#).

Tipo: cadena

Valores válidos: HOT | COOL | ARCHIVE

Obligatorio: no

[AgentArns](#)

(Opcional) Especifica el nombre de recurso de Amazon (ARN) del DataSync agente que se puede conectar con el contenedor de Azure Blob Storage. Si está configurando una transferencia entre nubes sin agente, no necesita especificar un valor para este parámetro.

Puede especificar más de un agente. Para obtener más información, consulte [Using multiple agents for your transfer](#).

Note

No puede añadir ni eliminar agentes de una ubicación de almacenamiento después de crearla inicialmente.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

[AuthenticationType](#)

Especifica el método de autenticación que se DataSync utiliza para acceder a Azure Blob Storage. DataSync puede acceder al almacenamiento de blobs mediante una firma de acceso compartido (SAS).

Tipo: cadena

Valores válidos: SAS | NONE

Obligatorio: no

BlobType

Especifica el tipo de blob que desea que tengan sus objetos o archivos al transferirlos a Azure Blob Storage. Actualmente, DataSync solo admite el traslado de datos a Azure Blob Storage como bloques blobs. Para obtener más información sobre los tipos de blobs, consulte la [Documentación de Azure Blob Storage](#).

Tipo: cadena

Valores válidos: BLOCK

Obligatorio: no

CmkSecretConfig

Especifica la información de configuración de un secreto DataSync administrado, como un token de autenticación o un conjunto de credenciales que se DataSync utiliza para acceder a una ubicación de transferencia específica, y a un lugar administrado por el cliente. AWS KMS key

Tipo: objeto [CmkSecretConfig](#)

Obligatorio: no

CustomSecretConfig

Especifica la información de configuración de un secreto administrado por el cliente, como un token de autenticación o un conjunto de credenciales que se DataSync utiliza para acceder a una ubicación de transferencia específica y a una administrada por el cliente. AWS KMS key

Tipo: objeto [CustomSecretConfig](#)

Obligatorio: no

LocationArn

Especifica el ARN de la ubicación de transferencia de Azure Blob Storage que va a actualizar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

[SasConfiguration](#)

Especifica la configuración de SAS que permite acceder DataSync a su Azure Blob Storage.

Tipo: objeto [AzureBlobSasConfiguration](#)

Obligatorio: no

[Subdirectory](#)

Especifica los segmentos de ruta si desea limitar su transferencia a un directorio virtual del contenedor (por ejemplo, /my/images).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 1024 caracteres.

Patrón: `^[\\p{L}\\p{M}\\p{Z}\\p{S}\\p{N}\\p{P}\\p{C}]*$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia de Amazon EFS que está utilizando. AWS DataSync

Para obtener más información, consulte [Configuración de DataSync transferencias con Amazon EFS](#).

Sintaxis de la solicitud

```
{
  "AccessPointArn": "string",
  "FileSystemAccessRoleArn": "string",
  "InTransitEncryption": "string",
  "LocationArn": "string",
  "Subdirectory": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[AccessPointArn](#)

Especifica el nombre de recurso de Amazon (ARN) del punto de acceso que se DataSync utiliza para montar el sistema de archivos Amazon EFS.

Para obtener más información, consulte [Acceso a los sistemas de archivos restringidos de Amazon EFS](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: (^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}\$)|(^\$)

Obligatorio: no

FileSystemAccessRoleArn

Especifica un rol AWS Identity and Access Management (IAM) que permite acceder DataSync al sistema de archivos Amazon EFS.

Para obtener información sobre la creación de este rol, consulte [Creación de un rol de DataSync IAM para el acceso al sistema de archivos Amazon EFS](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `(^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*)|(^$)`

Obligatorio: no

InTransitEncryption

Especifica si desea DataSync utilizar el cifrado Transport Layer Security (TLS) 1.2 cuando transfiera datos hacia o desde su sistema de archivos Amazon EFS.

Si especifica un punto de acceso mediante `AccessPointArn` o un rol de IAM con `FileSystemAccessRoleArn`, debe establecer este parámetro en `TLS1_2`.

Tipo: cadena

Valores válidos: `NONE` | `TLS1_2`

Obligatorio: no

LocationArn

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de transferencia de Amazon EFS que va a actualizar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Subdirectory

Especifica una ruta de montaje para el sistema de archivos de Amazon EFS. Aquí es donde DataSync lee o escribe los datos en su sistema de archivos (en función de si se trata de una ubicación de origen o de destino).

De forma predeterminada, DataSync usa el directorio raíz (o [el punto de acceso](#) si lo proporciona `AccessPointArn`). También puede incluir subdirectorios usando barras diagonales (por ejemplo, `/path/to/folder`).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia de Amazon FSx for Lustre con la que estás utilizando. AWS DataSync

Para obtener más información, consulta [Cómo configurar las DataSync transferencias con FSx for Lustre](#).

Sintaxis de la solicitud

```
{
  "LocationArn": "string",
  "Subdirectory": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[LocationArn](#)

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de transferencia de FSx for Lustre que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

[Subdirectory](#)

Especifica una ruta de montaje FSx para su sistema de archivos de Lustre. La ruta puede incluir subdirectorios.

Cuando la ubicación se utiliza como fuente, DataSync lee los datos de la ruta de montaje. Cuando la ubicación se utiliza como destino, DataSync escribe los datos en la ruta de montaje. Si no incluye este parámetro, DataSync utiliza el directorio raíz del sistema de archivos (/).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\/\(\)\$\p{Zs}]+$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia de Amazon FSx for NetApp ONTAP con la que estás utilizando. AWS DataSync

Para obtener más información, consulta [Cómo configurar las DataSync transferencias con ONTAP FSx](#).

Sintaxis de la solicitud

```
{
  "LocationArn": "string",
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "Subdirectory": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

LocationArn

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de transferencia FSx de ONTAP que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Protocol

Especifica el protocolo de transferencia de datos que se DataSync utiliza para acceder al sistema de FSx archivos de Amazon.

Tipo: objeto [FsxUpdateProtocol](#)

Obligatorio: no

Subdirectory

Especifica una ruta al recurso compartido de archivos de la máquina virtual de almacenamiento (SVM) a la que desea transferir los datos o desde donde desea transferir los datos.

Puede especificar una ruta de unión (también conocida como punto de montaje), una ruta de qtree (para recursos compartidos de archivos NFS) o un nombre de recurso compartido (para recursos compartidos de archivos SMB). Por ejemplo, la ruta de montaje podría ser /vol1, /vol1/tree1 o /share1.

Note

No especifique una ruta de cruce en el volumen raíz del SVM. Para obtener más información, consulte [Administración FSx de máquinas virtuales de almacenamiento de ONTAP](#) en la Guía del usuario de Amazon FSx for NetApp ONTAP.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^[^\\u0000\\u0085\\u2028\\u2029\\r\\n]{1,255}$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia de Amazon FSx for OpenZFS con la que estás utilizando. AWS DataSync

Para obtener más información, consulte [Configurar DataSync transferencias con FSx OpenZFS](#).

Note

Los parámetros de solicitud relacionados con SMB no se admiten con la operación UpdateLocationFsxOpenZfs.

Sintaxis de la solicitud

```
{
  "LocationArn": "string",
  "Protocol": {
    "NFS": {
      "MountOptions": {
        "Version": "string"
      }
    },
    "SMB": {
      "Domain": "string",
      "MountOptions": {
        "Version": "string"
      },
      "Password": "string",
      "User": "string"
    }
  },
  "Subdirectory": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

LocationArn

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de transferencia FSx de OpenZFS que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Protocol

Especifica el protocolo de transferencia de datos que se AWS DataSync utiliza para acceder al sistema de FSx archivos de Amazon.

Tipo: objeto [FsxProtocol](#)

Obligatorio: no

Subdirectory

Especifica un subdirectorio en la ruta de la ubicación que debe empezar /fsx por. DataSync utiliza este subdirectorio para leer o escribir datos (dependiendo de si el sistema de archivos es una ubicación de origen o de destino).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\\-\\+\\.\\/\\(\\)\\$\\p{Zs}]+$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia del servidor de archivos de Amazon FSx para Windows con AWS DataSync la que estás utilizando.

Para obtener más información, consulte [Configurar DataSync las transferencias con el servidor FSx de archivos de Windows](#).

Sintaxis de la solicitud

```
{
  "Domain": "string",
  "LocationArn": "string",
  "Password": "string",
  "Subdirectory": "string",
  "User": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[Domain](#)

Especifica el nombre del dominio de Windows al que pertenece FSx el sistema de archivos del servidor de archivos de Windows.

Si tiene varios dominios de Active Directory en su entorno, la configuración de este parámetro garantiza que DataSync se conecte al sistema de archivos correcto.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 253 caracteres.

Patrón: `^[A-Za-z0-9](\\.|-+)?[A-Za-z0-9]{0,252}?$`

Obligatorio: no

LocationArn

Especifica el ARN de la ubicación de transferencia del FSx servidor de archivos de Windows que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Password

Especifica la contraseña del usuario con los permisos para montar y acceder a los archivos, las carpetas y los metadatos de los archivos del sistema de archivos FSx del servidor de archivos de Windows.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^.{0,104}$`

Obligatorio: no

Subdirectory

Especifica una ruta de montaje para el sistema de archivos mediante barras diagonales.

DataSync utiliza este subdirectorio para leer o escribir datos (dependiendo de si el sistema de archivos es una ubicación de origen o de destino).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\\-\\+\\.\\/\\(\\)\\$\\p{Zs}]+$`

Obligatorio: no

User

Especifica el usuario con los permisos para montar y acceder a los archivos, las carpetas y los metadatos de los archivos del sistema de archivos FSx del servidor de archivos de Windows.

Para obtener información sobre cómo elegir un usuario con el nivel de acceso adecuado para la transferencia, consulte [los permisos necesarios](#) FSx para las ubicaciones de los servidores de archivos de Windows.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E ] { 1 , 104 } $`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia del Sistema de archivos distribuido de Hadoop (HDFS) con la que está utilizando. AWS DataSync

Para obtener más información, consulte [Configuración de DataSync transferencias con](#) un clúster HDFS.

Sintaxis de la solicitud

```
{
  "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"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[AgentArns](#)

Los nombres de recursos de Amazon (ARNs) de los DataSync agentes que se pueden conectar al clúster de HDFS.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

[AuthenticationType](#)

El tipo de autenticación utilizado para determinar la identidad del usuario.

Tipo: cadena

Valores válidos: SIMPLE | KERBEROS

Obligatorio: no

[BlockSize](#)

El tamaño de los bloques de datos que se escribirán en el clúster de HDFS.

Tipo: entero

Rango válido: valor mínimo de 1 048 576. Valor máximo de 1 073 741 824.

Obligatorio: no

[KerberosKeytab](#)

La tabla de claves de Kerberos (keytab) que contiene asignaciones entre el Kerberos principal definido y las claves cifradas. Puede cargar el keytab desde un archivo proporcionando la dirección del archivo.

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 65 536 caracteres.

Obligatorio: no

[KerberosKrb5Conf](#)

El archivo `krb5.conf` que contiene la información de configuración de Kerberos. Puede cargar el archivo `krb5.conf` proporcionando la dirección del archivo. Si utiliza la AWS CLI, esta realizará la codificación base64 por usted. De lo contrario, proporcione texto codificado en base64.

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 131 072 caracteres.

Obligatorio: no

[KerberosPrincipal](#)

La entidad principal de Kerberos con acceso a los archivos y carpetas del clúster de HDFS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^[.]+$`

Obligatorio: no

[KmsKeyProviderUri](#)

El URI de Key Management Server (KMS) del clúster HDFS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `^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$`

Obligatorio: no

[LocationArn](#)

El nombre de recurso de Amazon (ARN) de la ubicación de clúster de HDFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

[NameNodes](#)

El NameNode que administra el espacio de nombres HDFS. NameNode Realiza operaciones como abrir, cerrar y cambiar el nombre de archivos y directorios. NameNode Contiene la información necesaria para asignar bloques de datos al DataNodes. Puede usar solo uno NameNode.

Tipo: matriz de objetos [HdfsNameNode](#)

Miembros de la matriz: número mínimo de 1 artículo.

Obligatorio: no

[QopConfiguration](#)

La configuración de calidad de protección (QOP) especifica la configuración de privacidad de llamada a procedimiento remoto (RPC) y transferencia de datos configurada en el clúster del sistema de archivos distribuido de Hadoop (HDFS).

Tipo: objeto [QopConfiguration](#)

Obligatorio: no

[ReplicationFactor](#)

El número en el DataNodes que se van a replicar los datos al escribir en el clúster HDFS.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 512.

Obligatorio: no

[SimpleUser](#)

El nombre de usuario utilizado para identificar al cliente en el sistema operativo host.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^[_ .A-Za-z0-9][_ .A-Za-z0-9]*$`

Obligatorio: no

[Subdirectory](#)

Un subdirectorio del clúster de HDFS. Este subdirectorio se utiliza para leer o escribir datos en el clúster de HDFS.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\\-\\+\\.\\/(\\)\\$\\p{Zs}]+$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia del Sistema de archivos de red (NFS) que está utilizando. AWS DataSync

Para obtener más información, consulte [Configuración de transferencias con un servidor de archivos NFS](#).

Sintaxis de la solicitud

```
{
  "LocationArn": "string",
  "MountOptions": {
    "Version": "string"
  },
  "OnPremConfig": {
    "AgentArns": [ "string" ]
  },
  "ServerHostname": "string",
  "Subdirectory": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[LocationArn](#)

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de transferencia de NFS que desea actualizar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

MountOptions

Especifica cómo DataSync se puede acceder a una ubicación mediante el protocolo NFS.

Tipo: objeto [NfsMountOptions](#)

Obligatorio: no

OnPremConfig

Los AWS DataSync agentes que se pueden conectar al servidor de archivos del Network File System (NFS).

Tipo: objeto [OnPremConfig](#)

Obligatorio: no

ServerHostname

Especifica el nombre DNS o la dirección IP de versión 4 (IPv4) del servidor de archivos NFS al que se conecta el DataSync agente.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(( [a-zA-Z0-9\ - ]* [a-zA-Z0-9] ) \. )* ( [A-Za-z0-9\ - : ]* [A-Za-z0-9] ) $`

Obligatorio: no

Subdirectory

Especifica la ruta de exportación del servidor de archivos NFS que desea DataSync montar.

Esta ruta (o un subdirectorio de la ruta) es DataSync desde donde se transfieren los datos hacia o desde. Para obtener información sobre cómo configurar una exportación DataSync, consulte [Acceso a los servidores de archivos NFS](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_ \- \+ \. / \ ( \) \p{Zs} ]+ $`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia de almacenamiento de objetos con AWS DataSync la que está utilizando.

Para obtener más información, consulte [Configurar DataSync las transferencias con un sistema de almacenamiento de objetos](#).

Sintaxis de la solicitud

```
{
  "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"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[AccessKey](#)

Especifica la clave de acceso (por ejemplo, un nombre de usuario) si se requieren credenciales para autenticarse en el servidor de almacenamiento de objetos.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 200 caracteres.

Patrón: `^.*$`

Obligatorio: no

[AgentArns](#)

(Opcional) Especifica los nombres de recursos de Amazon (ARNs) de los DataSync agentes que se pueden conectar al sistema de almacenamiento de objetos. Si está configurando una transferencia entre nubes sin agentes, no necesita especificar un valor para este parámetro.

Note

No puede añadir ni eliminar agentes de una ubicación de almacenamiento después de crearla inicialmente.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

[CmkSecretConfig](#)

Especifica la información de configuración de un secreto DataSync administrado, como un token de autenticación o un conjunto de credenciales que se DataSync utiliza para acceder a una ubicación de transferencia específica, y a un lugar administrado por el cliente AWS KMS key.

Tipo: objeto [CmkSecretConfig](#)

Obligatorio: no

[CustomSecretConfig](#)

Especifica la información de configuración de un secreto administrado por el cliente, como un token de autenticación o un conjunto de credenciales que se DataSync utiliza para acceder a una ubicación de transferencia específica y a una administrada por el cliente. AWS KMS key

Tipo: objeto [CustomSecretConfig](#)

Obligatorio: no

[LocationArn](#)

Especifica el ARN de la ubicación de almacenamiento de objetos que va a actualizar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

[SecretKey](#)

Especifica la clave secreta (por ejemplo, una contraseña) si se requieren credenciales para autenticarse en el servidor de almacenamiento de objetos.

Note

Si proporciona un secreto utilizando `SecretKey`, pero no proporciona los detalles de configuración del secreto, utilizando `CmkSecretConfig` o `CustomSecretConfig`, entonces DataSync almacena el token con el secreto de Secrets Manager de su AWS cuenta.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 200 caracteres.

Patrón: `^.*$`

Obligatorio: no

[ServerCertificate](#)

Especifica una cadena de certificados DataSync para autenticarse en el sistema de almacenamiento de objetos si el sistema utiliza una entidad de certificación (CA) privada o autofirmada. Debe especificar un único archivo `.pem` con una cadena de certificados completa (por ejemplo, `file:///home/user/.ssh/object_storage_certificates.pem`).

La cadena de certificados puede incluir:

- El certificado del sistema de almacenamiento de objetos
- Todos los certificados intermedios (si los hay)
- El certificado raíz de la CA firmante

Puede concatenar sus certificados en un archivo .pem (que puede tener un máximo de 32 768 bytes antes de la codificación base64). El siguiente comando cat de ejemplo crea un archivo `object_storage_certificates.pem` que incluye tres certificados:

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

Para usar este parámetro, configure el `ServerProtocol` para HTTPS.

La actualización de este parámetro no interfiere en las tareas que tiene en curso.

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 32 768 caracteres.

Obligatorio: no

[ServerHostname](#)

Especifica el nombre de dominio o la dirección IP de versión 4 (IPv4) del servidor de almacenamiento de objetos al que se conecta el DataSync agente.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^(( [a-zA-Z0-9\-\ ]* [a-zA-Z0-9] )\.)* ([A-Za-z0-9\-\ :]* [A-Za-z0-9])$`

Obligatorio: no

[ServerPort](#)

Especifica el puerto en el que el servidor de almacenamiento de objetos acepta el tráfico de red entrante (por ejemplo, el puerto 443).

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 65 536.

Obligatorio: no

[ServerProtocol](#)

Especifica el protocolo que usa el servidor de almacenamiento de objetos para comunicarse.

Tipo: cadena

Valores válidos: HTTPS | HTTP

Obligatorio: no

[Subdirectory](#)

Especifica el prefijo de objeto del servidor de almacenamiento de objetos. Si se trata de una ubicación de origen, DataSync solo copia los objetos con este prefijo. Si se trata de una ubicación de destino, DataSync escribe todos los objetos con este prefijo.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia de Amazon S3 con AWS DataSync la que está utilizando.

Important

Antes de comenzar, asegúrese de haber leído los siguientes temas:

- [Consideraciones sobre las clases de almacenamiento en las ubicaciones de Amazon S3](#)
- [Evalúa los costos de las solicitudes de S3 al usar DataSync](#)

Sintaxis de la solicitud

```
{
  "LocationArn": "string",
  "S3Config": {
    "BucketAccessRoleArn": "string"
  },
  "S3StorageClass": "string",
  "Subdirectory": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[LocationArn](#)

Especifica el nombre de recurso de Amazon (ARN) de la ubicación de transferencia de Amazon S3 que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

S3Config

Especifica el nombre de recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que se DataSync utiliza para acceder al bucket de S3.

Para obtener más información, consulte [Proporcionar DataSync acceso a los buckets de S3](#).

Tipo: objeto [S3Config](#)

Obligatorio: no

S3StorageClass

Especifica la clase de almacenamiento que desea que utilicen los objetos cuando Amazon S3 sea un destino de transferencia.

Para los depósitos incluidos Regiones de AWS, la clase de almacenamiento se establece de forma predeterminada en. STANDARD Para los depósitos activados AWS Outposts, la clase de almacenamiento se establece de forma predeterminada en. OUTPOSTS

Para obtener más información, consulte [Storage class considerations with Amazon S3 transfers](#).

Tipo: cadena

Valores válidos: STANDARD | STANDARD_IA | ONEZONE_IA | INTELLIGENT_TIERING | GLACIER | DEEP_ARCHIVE | OUTPOSTS | GLACIER_INSTANT_RETRIEVAL

Obligatorio: no

Subdirectory

Especifica un prefijo en el depósito de S3 que DataSync lee o escribe en él (en función de si el depósito es una ubicación de origen o de destino).

Note

DataSync no puede transferir objetos con un prefijo que comience con una barra (/) o que incluya ///./, o patrones. /./ Por ejemplo:

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

- `photos/./2006/March`

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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 los siguientes parámetros de configuración de la ubicación de transferencia del bloque de mensajes del servidor (SMB) que está utilizando. AWS DataSync

Para obtener más información, consulte [Configuración de DataSync transferencias con un servidor de archivos SMB](#).

Sintaxis de la solicitud

```
{
  "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"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[AgentArns](#)

Especifica el DataSync agente (o los agentes) que se pueden conectar al servidor de archivos SMB. Puede especificar un agente mediante un nombre de recurso de Amazon (ARN).

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

AuthenticationType

Especifica el protocolo de autenticación que se DataSync utiliza para conectarse al servidor de archivos SMB. DataSync el soporte NTLM (predeterminado) y la KERBEROS autenticación.

Para obtener más información, consulte [Proporcionar DataSync acceso a servidores de archivos SMB](#).

Tipo: cadena

Valores válidos: NTLM | KERBEROS

Obligatorio: no

DnsIpAddresses

Especifica las IPv4 direcciones de los servidores DNS a los que pertenece el servidor de archivos SMB. Este parámetro solo se aplica si AuthenticationType está establecido en. KERBEROS

Si tiene varios dominios en su entorno, la configuración de este parámetro garantiza que DataSync se conecte al servidor de archivos SMB correcto.

Tipo: matriz de cadenas

Miembros de la matriz: número máximo de 2 elementos.

Limitaciones de longitud: longitud mínima de 7. Longitud máxima de 39.

Patrón: `\\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]`

`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`

Obligatorio: no

[Domain](#)

Especifica el nombre de dominio de Windows al que pertenece el servidor de archivos SMB. Este parámetro solo se aplica si `AuthenticationType` está establecido en `NTLM`.

Si tiene varios dominios en su entorno, la configuración de este parámetro garantiza que DataSync se conecte al servidor de archivos correcto.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 253 caracteres.

Patrón: `^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}$`

Obligatorio: no

[KerberosKeytab](#)

Especifica el archivo de tabla de claves de Kerberos (keytab), que incluye las asignaciones entre las claves principales y de cifrado de Kerberos.

Para evitar errores de ejecución de tareas, asegúrese de que el principal de Kerberos que utiliza para crear el archivo keytab coincide exactamente con lo que ha especificado.

`KerberosPrincipal`

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 65 536 caracteres.

Obligatorio: no

[KerberosKrb5Conf](#)

Especifica un archivo de configuración de Kerberos (`krb5.conf`) que define la configuración del dominio de Kerberos.

El archivo debe estar codificado en base64. Si está utilizando el AWS CLI, la codificación está hecha por usted.

Tipo: objeto de datos binarios codificados en Base64

Limitaciones de longitud: longitud máxima de 131 072 caracteres.

Obligatorio: no

[KerberosPrincipal](#)

Especifica un director de Kerberos, que es una identidad de su dominio de Kerberos que tiene permiso para acceder a los archivos, las carpetas y los metadatos de los archivos de su servidor de archivos SMB.

Un principal de Kerberos podría tener este aspecto. HOST/kerberosuser@MYDOMAIN.ORG

Los nombres principales distinguen entre mayúsculas y minúsculas. La ejecución de la DataSync tarea fallará si el principal que especifique para este parámetro no coincide exactamente con el principal que utilizó para crear el archivo keytab.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: ^.+\$

Obligatorio: no

[LocationArn](#)

Especifica el ARN de la ubicación de SMB que desea actualizar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: ^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}\$

Obligatorio: sí

[MountOptions](#)

Especifica la versión del protocolo del bloque de mensajes del servidor (SMB) que se AWS DataSync utiliza para acceder a un servidor de archivos SMB.

Tipo: objeto [SmbMountOptions](#)

Obligatorio: no

Password

Especifica la contraseña del usuario que puede montar su servidor de archivos SMB y que tiene permiso para acceder a los archivos y las carpetas involucrados en la transferencia. Este parámetro solo se aplica si `AuthenticationType` está establecido en. NTLM

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^.{0,104}$`

Obligatorio: no

ServerHostname

Especifica el nombre de dominio o la dirección IP del servidor de archivos SMB al que se conecta el DataSync agente.

Recuerde lo siguiente al configurar este parámetro:

- No puede especificar una dirección IP de versión 6 (IPv6).
- Si utiliza la autenticación Kerberos, debe especificar un nombre de dominio.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 255 caracteres.

Patrón: `^((([a-zA-Z0-9\-\_]*[a-zA-Z0-9])\.)*)([A-Za-z0-9\-\_]*[A-Za-z0-9])$`

Obligatorio: no

Subdirectory

Especifica el nombre del recurso compartido exportado por el servidor de archivos SMB en el que se DataSync leerán o escribirán los datos. Puede incluir un subdirectorio en la ruta del recurso compartido (por ejemplo, `/path/to/subdirectory`). Asegúrese de que otros clientes de SMB de la red también puedan montar esta ruta.

Para copiar todos los datos del subdirectorio especificado, DataSync debe poder montar el recurso compartido SMB y acceder a todos sus datos. Para obtener más información, consulte [Proporcionar DataSync acceso a los servidores de archivos SMB](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\/\(\)\$\p{Zs}]+$`

Obligatorio: no

User

Especifica el nombre del usuario que puede montar su servidor de archivos SMB y que tiene permiso para acceder a los archivos y las carpetas involucrados en la transferencia. Este parámetro solo se aplica si `AuthenticationType` está establecido en. NTLM

Para obtener información sobre cómo elegir un usuario con el nivel de acceso adecuado para la transferencia, consulte [Proporcionar DataSync acceso a los servidores de archivos SMB](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^[^\\x22\\x5B\\x5D\\x5C\\x5E\\x5F\\x60\\x61\\x62\\x63\\x64\\x65\\x66\\x67\\x68\\x69\\x6A\\x6B\\x6C\\x6D\\x6E\\x6F\\x70\\x71\\x72\\x73\\x74\\x75\\x76\\x77\\x78\\x79\\x7A\\x7B\\x7C\\x7D\\x7E\\x7F\\x80\\x81\\x82\\x83\\x84\\x85\\x86\\x87\\x88\\x89\\x8A\\x8B\\x8C\\x8D\\x8E\\x8F\\x90\\x91\\x92\\x93\\x94\\x95\\x96\\x97\\x98\\x99\\x9A\\x9B\\x9C\\x9D\\x9E\\x9F\\xA0\\xA1\\xA2\\xA3\\xA4\\xA5\\xA6\\xA7\\xA8\\xA9\\xAA\\xAB\\xAC\\xAD\\xAE\\xAF\\xB0\\xB1\\xB2\\xB3\\xB4\\xB5\\xB6\\xB7\\xB8\\xB9\\xBA\\xBB\\xBC\\xBD\\xBE\\xBF\\xC0\\xC1\\xC2\\xC3\\xC4\\xC5\\xC6\\xC7\\xC8\\xC9\\xCA\\xCB\\xCC\\xCD\\xCE\\xCF\\xD0\\xD1\\xD2\\xD3\\xD4\\xD5\\xD6\\xD7\\xD8\\xD9\\xDA\\xDB\\xDC\\xDD\\xDE\\xDF\\xE0\\xE1\\xE2\\xE3\\xE4\\xE5\\xE6\\xE7\\xE8\\xE9\\xEA\\xEB\\xEC\\xED\\xEE\\xEF\\xF0\\xF1\\xF2\\xF3\\xF4\\xF5\\xF6\\xF7\\xF8\\xF9\\xFA\\xFB\\xFC\\xFD\\xFE\\xFF]{1,104}$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Actualiza la configuración de una tarea, que define dónde y cómo AWS DataSync transfiere los datos.

Sintaxis de la solicitud

```
{
  "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"
}

```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[CloudWatchLogGroupArn](#)

Especifica el nombre de recurso de Amazon (ARN) de un grupo de CloudWatch registros de Amazon para supervisar la tarea.

Para las tareas del modo mejorado, debe utilizarlas `/aws/datasync` como nombre de grupo de registros. Por ejemplo:

```
arn:aws:logs:us-east-1:111222333444:log-group:/aws/datasync:*
```

Para obtener más información, consulte [Supervisar las transferencias de datos con CloudWatch registros](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 562 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):logs:[a-z\-\0-9]+:[0-9]{12}:log-group:([^\:]*)(:\:)?$`

Obligatorio: no

[Excludes](#)

Especifica los filtros de exclusión que definen los archivos, objetos y carpetas de la ubicación de origen que no se DataSync desean transferir. Para obtener más información y ejemplos, consulte [Especificar qué se DataSync transfiere mediante filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Obligatorio: no

Includes

Especifica los filtros de inclusión que definen los archivos, objetos y carpetas de la ubicación de origen que DataSync deseas transferir. Para obtener más información y ejemplos, consulte [Especificar qué se DataSync transfiere mediante filtros](#).

Tipo: matriz de objetos [FilterRule](#)

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Obligatorio: no

ManifestConfig

Configura un manifiesto, que es una lista de archivos u objetos que se desean DataSync transferir. Para obtener más información y ejemplos de configuración, consulte [Especificar lo que se DataSync transfiere mediante un manifiesto](#).

Al usar este parámetro, la identidad de la persona que llama (la función de IAM DataSync con la que está utilizando) debe tener el `iam:PassRole` permiso. La [AWSDataSyncFullAccess](#) política incluye este permiso.

Para eliminar una configuración de manifiesto, especifique este parámetro como vacío.

Tipo: objeto [ManifestConfig](#)

Obligatorio: no

Name

Especifica el nombre de la tarea.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Obligatorio: no

Options

Indica cómo está configurada la tarea de transferencia. Estas opciones incluyen la forma en que DataSync gestiona los archivos, los objetos y sus metadatos asociados durante la transferencia.

También puede especificar cómo verificar la integridad de los datos y establecer límites de ancho de banda para su tarea, entre otras opciones.

Cada opción tiene un valor predeterminado. A menos que lo necesites, no tienes que configurar ninguna opción antes de llamar [StartTaskExecution](#).

También puede anular sus opciones de tarea para cada ejecución de tareas. Por ejemplo, es posible que desee ajustar el `LogLevel` para una ejecución individual.

Tipo: objeto [Options](#)

Obligatorio: no

[Schedule](#)

Especifica el momento en que quiere que la tarea se ejecute. Para obtener más información, consulte [Scheduling your task](#) (Programación de tareas).

Tipo: objeto [TaskSchedule](#)

Obligatorio: no

[TaskArn](#)

Especifica el ARN de la tarea que desea actualizar.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

[TaskReportConfig](#)

Especifica cómo desea configurar un informe de tareas, que proporciona información detallada sobre la DataSync transferencia. Para obtener más información, consulte [Supervisar DataSync las transferencias con informes de tareas](#).

Al usar este parámetro, la identidad de la persona que llama (la función de IAM que utilizas DataSync) debe tener el `iam:PassRole` permiso. La [AWSDataSyncFullAccess](#) política incluye este permiso.

Para eliminar una configuración de informe de tarea, especifique este parámetro como vacío.

Tipo: objeto [TaskReportConfig](#)

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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

Actualiza la configuración de la ejecución de una AWS DataSync tarea en ejecución.

Note

Actualmente, la única Option que puede modificar con UpdateTaskExecution es [BytesPerSecond](#) , que limita el ancho de banda de la ejecución de una tarea en ejecución o en cola.

Sintaxis de la solicitud

```
{
  "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"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte [Parámetros comunes](#).

La solicitud acepta los siguientes datos en formato JSON.

[Options](#)

Indica cómo está configurada la tarea de transferencia. Estas opciones incluyen la forma en que DataSync gestiona los archivos, los objetos y sus metadatos asociados durante la transferencia. También puede especificar cómo verificar la integridad de los datos y establecer límites de ancho de banda para su tarea, entre otras opciones.

Cada opción tiene un valor predeterminado. A menos que lo necesites, no tienes que configurar ninguna opción antes de llamar [StartTaskExecution](#).

También puede anular sus opciones de tarea para cada ejecución de tareas. Por ejemplo, es posible que desee ajustar el `LogLevel` para una ejecución individual.

Tipo: objeto [Options](#)

Obligatorio: sí

[TaskExecutionArn](#)

Especifica el nombre de recurso de Amazon (ARN) de la ejecución de la tarea que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte [Errores comunes](#).

InternalException

Esta excepción se produce cuando se genera un error en el servicio AWS DataSync .

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [Interfaz de la línea de comandos de AWS](#)
- [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](#)

Data Types

Los siguientes tipos de datos son compatibles:

- [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 una sola entrada en una lista (o matriz) de AWS DataSync agentes cuando se llama a la [ListAgents](#) operación.

Contenido

AgentArn

El nombre de recurso de Amazon (ARN) de un DataSync agente.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

Name

El nombre de un agente.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\\s+=. _:@/-]+$`

Obligatorio: no

Platform

Los detalles relacionados con la plataforma sobre el agente, como el número de versión.

Tipo: objeto [Platform](#)

Obligatorio: no

Status

El estado de un agente.

- Si el estado es ONLINE, el agente está configurado correctamente y listo para usarse.

- Si el estado es `OFFLINE`, el agente ha estado sin contacto con el DataSync durante cinco minutos o más. Esto puede suceder por varias razones. Para obtener más información, consulte [What do I do if my agent is offline?](#)

Tipo: cadena

Valores válidos: `ONLINE` | `OFFLINE`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

AzureBlobSasConfiguration

La configuración de firma de acceso compartido (SAS) que permite acceder AWS DataSync a su Microsoft Azure Blob Storage.

Para obtener más información, consulte los [tokens SAS](#) para acceder a su Azure Blob Storage.

Contenido

Token

Especifica un token SAS que proporciona permisos para acceder a Azure Blob Storage.

El token forma parte de la cadena URI de SAS que aparece después del URI del recurso de almacenamiento y de un signo de interrogación. Un token tiene un aspecto similar a este:

```
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: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: ^.+\$

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CmkSecretConfig

Especifica la información de configuración de un secreto DataSync administrado, como un token de autenticación o una clave secreta que se DataSync utiliza para acceder a una ubicación de almacenamiento específica, con una ubicación administrada por el cliente AWS KMS key.

Note

Puede usar cualquiera de las dos opciones CmkSecretConfig o CustomSecretConfig proporcionar credenciales para una solicitud. CreateLocation No proporciona ambos parámetros para la misma solicitud.

Contenido

KmsKeyArn

Especifica el ARN del gestionado por el cliente AWS KMS key que se DataSync utiliza para cifrar el DataSync secreto gestionado almacenado para. SecretArn DataSync proporciona esta clave a. AWS Secrets Manager

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):kms:[a-z\-\0-9]+:[0-9]{12}:key/.*)$`

Obligatorio: no

SecretArn

Especifica el ARN del AWS Secrets Manager secreto DataSync administrado que se utiliza para acceder a una ubicación de almacenamiento específica. Esta propiedad la genera DataSync y es de solo lectura. DataSync cifra este secreto con la clave KMS que especifique. KmsKeyArn

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-\0-9]+:[0-9]{12}:secret:.*)$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

CustomSecretConfig

Especifica la información de configuración de un secreto de Secrets Manager administrado por el cliente en el que un token de autenticación o clave secreta de un lugar de almacenamiento se almacena en texto sin formato. Esta configuración incluye el ARN secreto y el ARN de un rol de IAM que proporciona acceso al secreto.

Note

Puede usar `CmkSecretConfig` o proporcionar credenciales `CustomSecretConfig` para una solicitud. `CreateLocation` No proporcione ambos parámetros para la misma solicitud.

Contenido

SecretAccessRoleArn

Especifica el ARN del AWS Identity and Access Management rol que se DataSync utiliza para acceder al secreto especificado para. `SecretArn`

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam:[0-9]{12}:role/[a-zA-Z0-9+=,._-]+|)$`

Obligatorio: no

SecretArn

Especifica el ARN de un AWS Secrets Manager secreto.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-zA-Z0-9]+:[0-9]{12}:secret:.*)$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Ec2Config

La subred y los grupos de seguridad que se AWS DataSync utilizan para conectarse a uno de los [destinos de montaje](#) del sistema de archivos Amazon EFS.

Contenido

SecurityGroupArns

Especifica los nombres de recursos de Amazon (ARNs) de los grupos de seguridad asociados al destino de montaje de un sistema de archivos Amazon EFS.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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]+$`

Obligatorio: sí

SubnetArn

Especifica el ARN de una subred donde DataSync crea las [interfaces de red](#) para administrar el tráfico durante la transferencia.

La subred debe estar ubicada:

- En la misma nube privada virtual (VPC) que el sistema de archivos de Amazon EFS.
- En la misma zona de disponibilidad que al menos un destino de montaje del sistema de archivos de Amazon EFS.

Note

No es necesario especificar una subred que incluya un destino de montaje del sistema de archivos.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:subnet/.*$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FilterRule

Especifica los archivos, carpetas y objetos que se van a incluir o excluir al transferir archivos del origen al destino.

Contenido

FilterType

El tipo de regla de filtrado que se va a aplicar. AWS DataSync solo admite el tipo de regla SIMPLE_PATTERN.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^[A-Z0-9_]+$`

Valores válidos: SIMPLE_PATTERN

Obligatorio: no

Value

Una única cadena de filtro que consiste en los patrones que se incluyen o excluyen. Los patrones están delimitados por “|” (es decir, una tubería), por ejemplo: `/folder1|/folder2`

Tipo: cadena

Limitaciones de longitud: longitud máxima de 102 400 caracteres.

Patrón: `^[^\x00]+$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FsxProtocol

Especifica el protocolo de transferencia de datos que se AWS DataSync utiliza para acceder al sistema de FSx archivos de Amazon.

Contenido

NFS

Especifica la configuración del protocolo del Sistema de Archivos de Red (NFS) que se DataSync utiliza FSx para acceder al sistema de archivos OpenZFS o FSx a la máquina virtual de almacenamiento (SVM) del sistema de archivos ONTAP.

Tipo: objeto [FsxProtocolNfs](#)

Obligatorio: no

SMB

Especifica la configuración del protocolo del bloque de mensajes del servidor (SMB) que se DataSync utiliza para acceder al SVM del sistema de archivos FSx ONTAP.

Tipo: objeto [FsxProtocolSmb](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FsxProtocolNfs

Especifica la configuración del protocolo del Sistema de archivos de red (NFS) que se DataSync utiliza FSx para acceder al sistema de archivos OpenZFS o FSx a la máquina virtual de almacenamiento (SVM) del sistema de archivos ONTAP.

Contenido

MountOptions

Especifica cómo se DataSync puede acceder a una ubicación mediante el protocolo NFS.

Tipo: objeto [NfsMountOptions](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FsxProtocolSmb

Especifica la configuración del protocolo Server Message Block (SMB) que se AWS DataSync utiliza para acceder a la máquina virtual de almacenamiento (SVM) del sistema de archivos Amazon FSx for NetApp ONTAP. Para obtener más información, consulte [Proporcionar DataSync acceso a los sistemas de archivos de FSx ONTAP](#).

Contenido

Password

Especifique la contraseña de un usuario que tiene permiso para acceder a la SVM.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^[0,104]$`

Obligatorio: sí

User

Especifica un usuario que puede montar y acceder a los archivos, carpetas y metadatos que necesita en su SVM.

Para obtener información sobre cómo elegir un usuario con el nivel de acceso adecuado para la transferencia, consulte [Uso del protocolo de SMB](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^[^\\x22\\x5B\\x5D\\/\\:;|=, +*?\\x3C\\x3E]{1,104}$`

Obligatorio: sí

Domain

Especifica el nombre del dominio de Windows al que pertenece la máquina virtual de almacenamiento (SVM).

Si tiene varios dominios en su entorno, al configurar esta configuración se asegura de que DataSync se conecten al SVM correcto.

Si tiene varios dominios de Active Directory en su entorno, al configurar este parámetro se asegura de que DataSync se conecte al SVM correcto.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 253 caracteres.

Patrón: `^[A-Za-z0-9](\.|-+)?[A-Za-z0-9]{0,252}$`

Obligatorio: no

MountOptions

Especifica la versión del protocolo de bloque de mensajes del servidor (SMB) que se AWS DataSync utiliza para acceder a un servidor de archivos SMB.

Tipo: objeto [SmbMountOptions](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FsxUpdateProtocol

Especifica el protocolo de transferencia de datos que se AWS DataSync utiliza para acceder al sistema de FSx archivos de Amazon.

Note

No puede actualizar la configuración del protocolo del Sistema de archivos de red (NFS) FSx para las ubicaciones de ONTAP. DataSync actualmente solo es compatible con la versión 3 de NFS con este tipo de ubicación.

Contenido

NFS

Especifica la configuración del protocolo del Sistema de archivos de red (NFS) que se DataSync utiliza FSx para acceder al sistema de archivos OpenZFS o a la máquina virtual de almacenamiento (FSx SVM) del sistema de archivos ONTAP.

Tipo: objeto [FsxProtocolNfs](#)

Obligatorio: no

SMB

Especifica la configuración del protocolo del bloque de mensajes del servidor (SMB) que se DataSync utiliza para acceder a la máquina virtual de almacenamiento (FSx SVM) del sistema de archivos ONTAP.

Tipo: objeto [FsxUpdateProtocolSmb](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

FsxUpdateProtocolSmb

Especifica la configuración del protocolo Server Message Block (SMB) que se AWS DataSync utiliza para acceder a la máquina virtual de almacenamiento (SVM) del sistema de archivos Amazon FSx for NetApp ONTAP. Para obtener más información, consulte [Proporcionar DataSync acceso a los sistemas de archivos de FSx ONTAP](#).

Contenido

Domain

Especifica el nombre del dominio de Windows al que pertenece la máquina virtual de almacenamiento (SVM).

Si tiene varios dominios de Active Directory en su entorno, la configuración de este parámetro garantiza que DataSync se conecte al SVM correcto.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 253 caracteres.

Patrón: `^([A-Za-z0-9](\.|-+)?[A-Za-z0-9]){0,252})?$`

Obligatorio: no

MountOptions

Especifica la versión del protocolo de bloque de mensajes del servidor (SMB) que se AWS DataSync utiliza para acceder a un servidor de archivos SMB.

Tipo: objeto [SmbMountOptions](#)

Obligatorio: no

Password

Especifique la contraseña de un usuario que tiene permiso para acceder a la SVM.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^.{0,104}$`

Obligatorio: no

User

Especifica un usuario que puede montar y acceder a los archivos, carpetas y metadatos que necesita en su SVM.

Para obtener información sobre cómo elegir un usuario con el nivel de acceso adecuado para la transferencia, consulte [Uso del protocolo de SMB](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 104 caracteres.

Patrón: `^[^\\x22\\x5B\\x5D\\/\\: ; | = , + * ? \\x3C \\x3E ] { 1 , 104 } $`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

HdfsNameNode

El NameNode del sistema de archivos distribuido Hadoop (HDFS). NameNode Administra el espacio de nombres del sistema de archivos. NameNode Realiza operaciones como abrir, cerrar y cambiar el nombre de archivos y directorios. NameNode Contiene la información necesaria para asignar bloques de datos al DataNodes.

Contenido

Hostname

El nombre de host del NameNode clúster HDFS. Este valor es la dirección IP o el nombre del servicio de nombres de dominio (DNS) del. NameNode Un agente que se instala localmente usa este nombre de host para comunicarse con el de NameNode la red.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `^(([a-zA-Z0-9\-.]*[a-zA-Z0-9])\.)*([A-Za-z0-9\-.]*[A-Za-z0-9])$`

Obligatorio: sí

Port

El puerto que NameNode utiliza para escuchar las solicitudes de los clientes.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 65 536.

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

LocationFilter

Reduce la lista de recursos que arroja `ListLocations`. Por ejemplo, para ver todas sus ubicaciones de Amazon S3, cree un filtro con `"Name": "LocationType", "Operator": "Equals"` y `"Values": "S3"`.

Para obtener más información, consulte [Recursos de filtrado](#).

Contenido

Name

Nombre del filtro que se está utilizando. Cada llamada a la API admite una lista de filtros que están disponibles para ella (por ejemplo, `LocationType` para `ListLocations`).

Tipo: cadena

Valores válidos: `LocationUri` | `LocationType` | `CreationTime`

Obligatorio: sí

Operator

Es el operador que se utiliza para comparar los valores de los filtros (por ejemplo, `Equals` o `Contains`).

Tipo: cadena

Valores válidos: `Equals` | `NotEquals` | `In` | `LessThanOrEqualTo` | `LessThan` | `GreaterThanEqualTo` | `GreaterThan` | `Contains` | `NotContains` | `BeginsWith`

Obligatorio: sí

Values

Valores por los que quiere filtrar. Por ejemplo, es posible que desee mostrar solo las ubicaciones de Amazon S3.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `^[0-9a-zA-Z_\ \-\:\*\.\ \\/\?\-]*$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

LocationListEntry

Representa una sola entrada en una lista de ubicaciones. `LocationListEntry` devuelve una matriz que contiene una lista de ubicaciones cuando se llama a la [ListLocations](#) operación.

Contenido

LocationArn

El nombre de recurso de Amazon (ARN) de la ubicación. En el caso del Sistema de archivos de red (NFS) o Amazon EFS, la ubicación es la ruta de exportación. En el caso de Amazon S3, la ubicación es la ruta del prefijo que desea montar y utilizar como la raíz de la sincronización.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

LocationUri

Representa una lista URIs de ubicaciones. `LocationUri` devuelve una matriz que contiene una lista de ubicaciones cuando se llama a la [ListLocations](#) operación.

Formato: `TYPE://GLOBAL_ID/SUBDIR`.

TYPE designa el tipo de ubicación (por ejemplo, `nfs` o `s3`).

GLOBAL_ID es el identificador único global del recurso que respalda la ubicación. Un ejemplo de EFS es `us-east-2.fs-abcd1234`. Un ejemplo de Amazon S3 es el nombre del bucket, como `myBucket`. Un ejemplo de NFS es una IPv4 dirección válida o un nombre de host que cumpla con el Servicio de nombres de dominio (DNS).

SUBDIR es una ruta del sistema de archivos válida, delimitada por barras diagonales, según la convención `*nix`. En el caso de NFS y Amazon EFS, es la ruta de exportación para montar la ubicación. En el caso de Amazon S3, es la ruta del prefijo que desea montar y utilizar como la raíz de la sincronización.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4360 caracteres.

Patrón: `^(efs|nfs|s3|smb|hdfs|fsx[a-z0-9-]+)://[a-zA-Z0-9.:/\-]+$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ManagedSecretConfig

Especifica la información de configuración de un secreto DataSync administrado, como un token de autenticación o un conjunto de credenciales que se DataSync utiliza para acceder a una ubicación de transferencia específica. DataSync utiliza la clave KMS AWS administrada de forma predeterminada para cifrar este secreto. AWS Secrets Manager

Contenido

SecretArn

Especifica el ARN de un AWS Secrets Manager secreto.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^(arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z\-\0-9]+:[0-9]{12}:secret:.*|)$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ManifestConfig

Configura un manifiesto, que es una lista de archivos u objetos que desea AWS DataSync transferir. Para obtener más información y ejemplos de configuración, consulte [Especificar lo que se DataSync transfiere mediante un manifiesto](#).

Contenido

Action

Especifica para qué se DataSync usa el manifiesto.

Tipo: cadena

Valores válidos: TRANSFER

Obligatorio: no

Format

Especifica el formato de archivo del manifiesto. Para obtener información, consulte [Crear un manifiesto](#).

Tipo: cadena

Valores válidos: CSV

Obligatorio: no

Source

Especifica el manifiesto que DataSync quieres usar y dónde está alojado.

Note

Debe especificar este parámetro si va a configurar un nuevo manifiesto a partir del 7 de febrero de 2024.

Si no lo haces, recibirás un código de estado 400 y un `ValidationException` error que indicará que te falta la función de IAM para acceder DataSync al depósito de S3 en el que alojas tu manifiesto. Para obtener más información, consulta [Cómo proporcionar DataSync acceso a tu manifiesto](#).

Tipo: objeto [SourceManifestConfig](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

NfsMountOptions

Especifica cómo DataSync se puede acceder a una ubicación mediante el protocolo NFS.

Contenido

Version

Especifica la versión de NFS que desea utilizar DataSync al montar el recurso compartido de NFS. Si el servidor se niega a utilizar la versión especificada, se producirá un error en la tarea.

Puede especificar las opciones siguientes:

- **AUTOMATIC**(predeterminado): DataSync elige la versión 4.1 de NFS.
- **NFS3**: versión de protocolo sin estado que permite escrituras asincrónicas en el servidor.
- **NFSv4_0**: versión de protocolo con estado y compatible con cortafuegos que admite delegaciones y pseudo sistemas de archivos.
- **NFSv4_1**: versión de protocolo con estado que admite sesiones, delegaciones de directorios y procesamiento de datos en paralelo. La versión 4.1 de NFS también incluye todas las funciones disponibles en la versión 4.0.

Note

DataSync actualmente solo es compatible con la versión 3 de NFS con Amazon FSx for NetApp ONTAP.

Tipo: cadena

Valores válidos: **AUTOMATIC** | **NFS3** | **NFS4_0** | **NFS4_1**

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

OnPremConfig

Los AWS DataSync agentes que se pueden conectar al servidor de archivos del Network File System (NFS).

Contenido

AgentArns

Los nombres de recursos de Amazon (ARNs) de los DataSync agentes que se pueden conectar al servidor de archivos NFS.

Puede especificar más de un agente. Para obtener más información, consulte [Uso de varios DataSync agentes](#).

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Options

Indica cómo está configurada la tarea de transferencia. Estas opciones incluyen la forma en que DataSync gestiona los archivos, los objetos y sus metadatos asociados durante la transferencia. También puede especificar cómo verificar la integridad de los datos y establecer límites de ancho de banda para su tarea, entre otras opciones.

Cada opción tiene un valor predeterminado. A menos que lo necesites, no tienes que configurar ninguna opción antes de llamar [StartTaskExecution](#).

También puede anular sus opciones de tarea para cada ejecución de tareas. Por ejemplo, es posible que desee ajustar el `LogLevel` para una ejecución individual.

Contenido

Atime

Especifica si deben conservarse los metadatos que indican la última vez que se leyó o escribió un archivo.

Note

El comportamiento de `Atime` no es totalmente estándar en todas las plataformas, por lo que solo DataSync se puede hacer si se hace el mejor esfuerzo.

- `BEST_EFFORT`(predeterminado): DataSync intenta conservar el `Atime` atributo original en todos los archivos fuente (es decir, la versión anterior a los `PREPARING` pasos de ejecución de la tarea). Se recomienda usar esta opción.
- `NONE`: ignora `Atime`.

Note

Si `Atime` se establece en `BEST_EFFORT`, `Mtime` debe establecerse en `PRESERVE`.
Si `Atime` se establece en `NONE`, `Mtime` también debe ser `NONE`.

Tipo: cadena

Valores válidos: `NONE` | `BEST_EFFORT`

Obligatorio: no

BytesPerSecond

Limita el ancho de banda utilizado por una DataSync tarea. Por ejemplo, si desea DataSync utilizar un máximo de 1 MB, establezca este valor en 1048576 (=1024*1024).

Note

No se aplica a las [tareas del modo mejorado](#).

Tipo: largo

Rango válido: valor mínimo de -1.

Obligatorio: no

Gid

Especifica la ID del grupo POSIX (GID) de los propietarios del archivo.

- INT_VALUE (predeterminado): conserva el valor entero del ID de usuario (UID) y del GID (recomendado), que está recomendado.
- NONE: ignoran los UID y GID.

Para obtener más información, consulte [Cómo se DataSync gestionan los metadatos de archivos y objetos](#).

Tipo: cadena

Valores válidos: NONE | INT_VALUE | NAME | BOTH

Obligatorio: no

LogLevel

Especifica el tipo de registros que se DataSync publican en un grupo de CloudWatch registros de Amazon Logs. Para especificar el grupo de registros, consulte [CloudWatchLogGroupArn](#).

- BASIC- Publica los registros solo con información básica (como los errores de transferencia).
- TRANSFER- Publica los registros de todos los archivos u objetos que transfiere la DataSync tarea y comprueba la integridad de los datos.
- OFF- No se publica ningún registro.

Tipo: cadena

Valores válidos: OFF | BASIC | TRANSFER

Obligatorio: no

Mtime

Especifica si se deben conservar los metadatos que indican la última vez que se escribió un archivo antes del PREPARING paso de ejecución de la tarea. Esta opción es obligatoria cuando necesita ejecutar la misma tarea más de una vez.

- PRESERVE(predeterminado): conserva el originalMtime, lo que se recomienda.
- NONE: ignora Mtime.

Note

Si Mtime se establece en PRESERVE, Atime debe establecerse en BEST_EFFORT.
Si Mtime se establece en NONE, Atime también se debe establecer en NONE.

Tipo: cadena

Valores válidos: NONE | PRESERVE

Obligatorio: no

ObjectTags

Especifica si desea DataSync poner PRESERVE objetos en las etiquetas (comportamiento predeterminado) al realizar transferencias entre sistemas de almacenamiento de objetos. Si desea que la DataSync tarea ignore las etiquetas de objetos, especifique el NONE valor.

Tipo: cadena

Valores válidos: PRESERVE | NONE

Obligatorio: no

OverwriteMode

Especifica si se DataSync deben modificar o conservar los datos en la ubicación de destino.

- ALWAYS(predeterminado): DataSync modifica los datos de la ubicación de destino cuando los datos de origen (incluidos los metadatos) cambian.

Si DataSync sobrescribe objetos, es posible que incurra en cargos adicionales por determinadas clases de almacenamiento de Amazon S3 (por ejemplo, por recuperación o eliminación anticipada). Para obtener más información, consulte [Storage class considerations with Amazon S3 transfers](#).

- NEVER- DataSync no sobrescribe los datos de la ubicación de destino aunque los datos de origen hayan cambiado. Puede utilizar esta opción para evitar que se sobrescriban los cambios realizados en los archivos u objetos del destino.

Tipo: cadena

Valores válidos: ALWAYS | NEVER

Obligatorio: no

PosixPermissions

Determina qué usuarios o grupos pueden acceder a un archivo para un propósito específico, como leer, escribir o ejecutar el archivo.

Para obtener más información, consulte [Cómo se gestionan DataSync los metadatos de archivos y objetos](#).

- PRESERVE(predeterminado): conserva los permisos de estilo POSIX, lo que se recomienda.
- NONE- Ignora los permisos de estilo POSIX.

Note

DataSync puede conservar los permisos actuales de una ubicación de origen.

Tipo: cadena

Valores válidos: NONE | PRESERVE

Obligatorio: no

PreserveDeletedFiles

Valor que especifica si los archivos del destino que no existen en el origen deben conservarse. Esta opción puede afectar su costo de almacenamiento Amazon S3. Si su tarea elimina objetos, es posible que se apliquen cargos mínimos por la duración de almacenamiento

para determinadas clases de almacenamiento. Para obtener información detallada, consulte [Consideraciones al trabajar con clases de almacenamiento de Amazon S3 en DataSync](#).

- PRESERVE(predeterminado): ignora dichos archivos de destino, lo cual es recomendable.
- REMOVE: elimina los archivos de destino que no están presentes en el origen.

 Note

Si establece este parámetro en REMOVE, no podrá configurar TransferMode en ALL. Al transferir todos los datos, DataSync no escanea la ubicación de destino y no sabe qué eliminar.

Tipo: cadena

Valores válidos: PRESERVE | REMOVE

Obligatorio: no

PreserveDevices

Especifica si se DataSync deben conservar los metadatos de los dispositivos de bloques y caracteres en la ubicación de origen y volver a crear los archivos con el nombre del dispositivo y los metadatos en el destino. DataSync copia únicamente el nombre y los metadatos de dichos dispositivos.

 Note

DataSync no puede copiar el contenido real de estos dispositivos porque no son terminales y no devuelven un marcador end-of-file (EOF).

- NONE(predeterminado): ignoran los dispositivos especiales (recomendado).
- PRESERVE: conserva los metadatos de los dispositivos de bloques y caracteres. Amazon EFS actualmente no admite esta opción.

Tipo: cadena

Valores válidos: NONE | PRESERVE

Obligatorio: no

SecurityDescriptorCopyFlags

Determina qué componentes del descriptor de seguridad de SMB se copian de los objetos de origen a los de destino.

Este valor solo se usa para transferencias entre ubicaciones de SMB y Amazon FSx for Windows File Server o entre dos FSx ubicaciones de Windows File Server. Para obtener más información, consulte [Cómo se gestionan DataSync los metadatos de archivos y objetos](#).

- OWNER_DACL(predeterminado): para cada objeto copiado, DataSync copia los siguientes metadatos:

- El propietario del objeto.
- Listas de control de acceso discrecional de NTFS (DACLS), que determinan si se debe conceder el acceso a un objeto.

DataSync no copiará las listas de control de acceso al sistema NTFS (SACLs) con esta opción.

- OWNER_DACL_SACL- Para cada objeto copiado, DataSync copia los siguientes metadatos:

- El propietario del objeto.
- Listas de control de acceso discrecional de NTFS (DACLS), que determinan si se debe conceder el acceso a un objeto.
- SACLs, que los administradores utilizan para registrar los intentos de acceso a un objeto protegido.

SACLs Para copiar es necesario conceder permisos adicionales al usuario de Windows que DataSync utilice para acceder a la ubicación de su SMB. Para obtener información sobre cómo elegir un usuario con los permisos correctos, consulta los permisos necesarios para [SMB](#), [FSx Windows File Server](#) o [FSx ONTAP](#) (según el tipo de ubicación de la transferencia).

- NONE: no se copia ninguno de los componentes del descriptor de seguridad de SMB. Los objetos de destino son propiedad del usuario que se proporcionó para acceder a la ubicación de destino. DACLS y SACLs se establecen en función de la configuración del servidor de destino.

Tipo: cadena

Valores válidos: NONE | OWNER_DACL | OWNER_DACL_SACL

Obligatorio: no

TaskQueueing

Especifica si las tareas de transferencia deben ponerse en cola en determinadas situaciones en los que [se ejecutan varias tareas](#). Este es ENABLED de forma predeterminada.

Tipo: cadena

Valores válidos: ENABLED | DISABLED

Obligatorio: no

TransferMode

Especifica si DataSync transfiere solo los datos (incluidos los metadatos) que difieren de una ubicación a otra después de una copia inicial o si transfiere todos los datos cada vez que se ejecuta la tarea. Si planea realizar transferencias recurrentes, es posible que solo desee transferir lo que haya cambiado desde la ejecución anterior de la tarea.

- CHANGED(predeterminado): tras la transferencia completa inicial, solo DataSync copia los datos y metadatos que difieran de la ubicación de origen y la de destino.
- ALL- DataSync copia todo el contenido de la fuente al destino sin comparar las diferencias entre las ubicaciones.

Tipo: cadena

Valores válidos: CHANGED | ALL

Obligatorio: no

Uid

Especifica el ID de usuario de POSIX (UID) del propietario del archivo.

- INT_VALUE (predeterminado): conserva el valor entero del ID de usuario (UID) y del ID de grupo (GID), que está recomendado.
- NONE: ignoran los UID y GID.

Para obtener más información, consulte [Metadatos copiados por DataSync](#).

Tipo: cadena

Valores válidos: NONE | INT_VALUE | NAME | BOTH

Obligatorio: no

VerifyMode

Especifica si se DataSync comprueba la integridad de los datos al final de la transferencia y cómo lo hace.

- **ONLY_FILES_TRANSFERRED**(recomendado): DataSync calcula la suma de verificación de los datos transferidos (incluidos los metadatos) en la ubicación de origen. Al final de la transferencia, compara esta suma DataSync de verificación con la suma de verificación calculada para esos datos en el destino.

Note

Esta es la opción predeterminada para las tareas del [modo mejorado](#).

Es conveniente utilizar esta opción cuando la transferencia se realice a S3 Glacier Flexible Retrieval o a las clases de almacenamiento de S3 Glacier Deep Archive. Para obtener más información, consulte [Storage class considerations with Amazon S3 locations](#).

- **POINT_IN_TIME_CONSISTENT**- Al final de la transferencia, DataSync comprueba todo el origen y el destino para comprobar que ambas ubicaciones estén completamente sincronizadas.

Note

Es la opción predeterminada para las [tareas del modo Básico](#) y, por el momento, no es compatible con las tareas del modo Mejorado.

Si utilizas un [manifiesto](#), DataSync solo escanea y verifica lo que aparece en el manifiesto.

No puede utilizar esta opción cuando la transferencia se realice a S3 Glacier Flexible Retrieval o a las clases de almacenamiento de S3 Glacier Deep Archive. Para obtener más información, consulte [Storage class considerations with Amazon S3 locations](#).

- **NONE**- DataSync comprueba la integridad de los datos solo durante la transferencia. A diferencia de otras opciones, no hay ninguna verificación adicional al final de la transferencia.

Tipo: cadena

Valores válidos: **POINT_IN_TIME_CONSISTENT** | **ONLY_FILES_TRANSFERRED** | **NONE**

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Platform

Los detalles relacionados con la plataforma sobre el AWS DataSync agente, como el número de versión.

Contenido

Version

La versión del agente. DataSync

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

PrivateLinkConfig

Especifica cómo se conecta su AWS DataSync agente AWS mediante un punto final de [servicio de nube privada virtual \(VPC\)](#). No se puede acceder a un agente que usa un punto de conexión de VPC a través de la red de Internet pública.

Contenido

PrivateLinkEndpoint

Especifica el punto de conexión de VPC proporcionado por el [AWS PrivateLink](#) al que se conecta el agente.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 7. Longitud máxima de 15.

Patrón: `\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`

Obligatorio: no

SecurityGroupArns

Especifica los nombres de recursos de Amazon (ARN) del grupo de seguridad que proporciona DataSync acceso al punto final de la VPC. Solo puede especificar un ARN.

Tipo: matriz de cadenas

Miembros de la matriz: número fijo de 1 elemento.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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]+$`

Obligatorio: no

SubnetArns

Especifica el ARN de la subred en la que se encuentra el punto de conexión de VPC. Solo puede especificar un ARN.

Tipo: matriz de cadenas

Miembros de la matriz: número fijo de 1 elemento.

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):ec2:[a-z\-\0-9]*:[0-9]{12}:subnet/.*$`

Obligatorio: no

VpcEndpointId

Especifica el ID del punto de conexión de VPC al que se conecta su agente.

Tipo: cadena

Patrón: `^vpce-[0-9a-f]{17}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

QopConfiguration

La configuración de calidad de protección (QOP) especifica la configuración de privacidad de llamada a procedimiento remoto (RPC) y transferencia de datos configurada en el clúster del sistema de archivos distribuido de Hadoop (HDFS).

Contenido

DataTransferProtection

La configuración de protección de transferencia de datos configurada en el clúster HDFS. Esta configuración corresponde a la configuración de `dfs.data.transfer.protection` en el archivo `hdfs-site.xml` en su clúster de Hadoop.

Tipo: cadena

Valores válidos: DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY

Obligatorio: no

RpcProtection

La configuración de protección de transferencia de datos configurada en el clúster de HDFS. Esta configuración corresponde a la configuración de `hadoop.rpc.protection` en el archivo `core-site.xml` en su clúster de Hadoop.

Tipo: cadena

Valores válidos: DISABLED | AUTHENTICATION | INTEGRITY | PRIVACY

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportDestination

Especifica dónde se DataSync carga el [informe de tareas](#).

Contenido

S3

Especifica el bucket de Amazon S3 en el que se DataSync carga el informe de tareas.

Tipo: objeto [ReportDestinationS3](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportDestinationS3

Especifica el bucket de Amazon S3 en el que se DataSync carga el [informe de tareas](#).

Contenido

BucketAccessRoleArn

Especifica el nombre de recurso de Amazon (ARN) de la política de IAM que permite DataSync cargar un informe de tareas en el bucket de S3. Para obtener más información, consulte [Permitir DataSync cargar un informe de tareas a un bucket de Amazon S3](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam:[0-9]{12}:role/.*$`

Obligatorio: sí

S3BucketArn

Especifica el ARN del depósito de S3 en el que se DataSync carga el informe.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 268.

Patrón: `^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}$`

Obligatorio: sí

Subdirectory

Especifica un prefijo de bucket para el informe.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\+\.\/(\\)\p{Zs}]*$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportOverride

Especifica el nivel de detalle de un aspecto concreto del [informe de DataSync tareas](#).

Contenido

ReportLevel

Especifica si su informe de tareas incluye solo errores o aciertos y errores.

Por ejemplo, es posible que el informe incluya principalmente solo aquello que no salió bien en la transferencia (ERRORS_ONLY). Al mismo tiempo, es conveniente que compruebe que su [filtro de tarea](#) funciona correctamente. En esta situación, puedes obtener una lista de los archivos que se DataSync han omitido correctamente y si se ha transferido algo que no has transferido (SUCSESSES_AND_ERRORS).

Tipo: cadena

Valores válidos: ERRORS_ONLY | SUCSESSES_AND_ERRORS

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportOverrides

El nivel de detalle incluido en cada aspecto del [informe de DataSync tareas](#).

Contenido

Deleted

Especifica el nivel de informes de los archivos, objetos y directorios que se DataSync intentaron eliminar en la ubicación de destino. Esto solo se aplica si [configura su tarea](#) para eliminar datos del destino que no estén en el origen.

Tipo: objeto [ReportOverride](#)

Obligatorio: no

Skipped

Especifica el nivel de informes de los archivos, objetos y directorios que se DataSync intentaron omitir durante la transferencia.

Tipo: objeto [ReportOverride](#)

Obligatorio: no

Transferred

Especifica el nivel de informes de los archivos, objetos y directorios que se DataSync intentaron transferir.

Tipo: objeto [ReportOverride](#)

Obligatorio: no

Verified

Especifica el nivel de informes de los archivos, objetos y directorios que se DataSync intentaron verificar al final de la transferencia.

Tipo: objeto [ReportOverride](#)

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

ReportResult

Indica si DataSync se ha creado un [informe de tareas](#) completo para la transferencia.

Contenido

ErrorCode

Indica el código asociado al error si no DataSync se puede crear un informe completo.

Tipo: cadena

Requerido: no

ErrorDetail

Proporciona detalles sobre los problemas al crear un informe.

Tipo: cadena

Requerido: no

Status

Indica si aún DataSync está trabajando en su informe, si ha creado un informe o si no puede crear un informe completo.

Tipo: cadena

Valores válidos: PENDING | SUCCESS | ERROR

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

S3Config

Especifica el nombre de recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que se DataSync utiliza para acceder al bucket de S3.

Para obtener más información, consulte [Proporcionar DataSync acceso a los buckets de S3](#).

Contenido

BucketAccessRoleArn

Especifica el ARN de la función de IAM que se DataSync utiliza para acceder al bucket de S3.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam:[0-9]{12}:role/.*$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

S3ManifestConfig

Especifica el bucket de S3 en el que alojas el manifiesto que AWS DataSync quieres usar. Para obtener más información y ejemplos de configuración, consulta [Especificar qué se DataSync transfiere mediante un manifiesto](#).

Contenido

BucketAccessRoleArn

Especifica la función AWS Identity and Access Management (IAM) que permite acceder DataSync al manifiesto. Para obtener más información, consulta [Cómo proporcionar DataSync acceso a tu manifiesto](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 2048 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

Obligatorio: sí

ManifestObjectPath

Especifica la clave de objeto de Amazon S3 de su manifiesto. Puede incluir un prefijo (por ejemplo, `prefix/my-manifest.csv`).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 4096 caracteres.

Patrón: `^[a-zA-Z0-9_\-\.\/\(\)\p{Zs}]*$`

Obligatorio: sí

S3BucketArn

Especifica el nombre de recurso de Amazon (ARN) del bucket de S3 en el que aloja el manifiesto.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 268.

Patrón: ^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}\$

Obligatorio: sí

ManifestObjectVersionId

Especifica el ID de versión del objeto del manifiesto que DataSync quieres usar. Si no lo estableces, DataSync utiliza la última versión del objeto.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: ^.+\$

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

SmbMountOptions

Especifica la versión del protocolo del bloque de mensajes del servidor (SMB) que se AWS DataSync utiliza para acceder a un servidor de archivos SMB.

Contenido

Version

De forma predeterminada, elige DataSync automáticamente una versión del protocolo SMB en función de la negociación con el servidor de archivos SMB. También puede configurarlo DataSync para usar una versión SMB específica, pero le recomendamos que lo haga solo si DataSync tiene problemas para negociar automáticamente con el servidor de archivos SMB.

A continuación, se enumeran las opciones para configurar la versión de SMB:

- AUTOMATIC(predeterminado): DataSync y el servidor de archivos SMB negocian la versión más alta de SMB que admitan mutuamente, entre la 2.1 y la 3.1.1.

Esta es la opción recomendada. Si, por el contrario, elige una versión específica que el servidor de archivos no admite, es posible que aparezca un error `Operation Not Supported`.

- SMB3: restringe la negociación del protocolo solo a la versión 3.0.2 de SMB.
- SMB2: restringe la negociación del protocolo solo a la versión 2.1 de SMB.
- SMB2_0: restringe la negociación del protocolo solo a la versión 2.0 de SMB.
- SMB1: restringe la negociación del protocolo solo a la versión 1.0 de SMB.

Note

La SMB1 opción no está disponible al [crear una ubicación de Amazon FSx for NetApp ONTAP](#).

Tipo: cadena

Valores válidos: AUTOMATIC | SMB2 | SMB3 | SMB1 | SMB2_0

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

SourceManifestConfig

Especifica el manifiesto que AWS DataSync quieres usar y dónde está alojado. Para obtener más información y ejemplos de configuración, consulta [Especificar lo que se DataSync transfiere mediante un manifiesto](#).

Contenido

S3

Especifica el bucket de S3 en el que alojas el manifiesto.

Tipo: objeto [S3ManifestConfig](#)

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TagListEntry

Par clave-valor que representa una sola etiqueta que se ha aplicado a un recurso de AWS .

Contenido

Key

La clave de una etiqueta AWS de recurso.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=. _:/-]+$`

Obligatorio: sí

Value

El valor de una etiqueta AWS de recurso.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=. _:@/-]+$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskExecutionFilesFailedDetail

El número de objetos que DataSync no se pueden preparar, transferir, verificar ni eliminar durante la ejecución de la tarea.

Note

Se aplica únicamente a las [tareas del modo mejorado](#).

Contenido

Delete

El número de objetos que DataSync no se pueden eliminar durante la ejecución de la tarea.

Tipo: largo

Obligatorio: no

Prepare

El número de objetos que DataSync no se preparan durante la ejecución de la tarea.

Tipo: largo

Obligatorio: no

Transfer

El número de objetos que DataSync no se pueden transferir durante la ejecución de la tarea.

Tipo: largo

Obligatorio: no

Verify

El número de objetos que DataSync no se pueden verificar durante la ejecución de la tarea.

Tipo: largo

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulte lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskExecutionFilesListedDetail

El número de objetos que DataSync encuentra en sus ubicaciones.

Note

Se aplica solo a las [tareas del modo mejorado](#).

Contenido

AtDestinationForDelete

El número de objetos que DataSync se encuentran en la ubicación de destino. Este contador solo se aplica si [configura la tarea](#) para eliminar datos del destino que no estén en la fuente.

Tipo: largo

Obligatorio: no

AtSource

El número de objetos que DataSync se encuentran en la ubicación de origen.

- En el caso de un [manifiesto](#), solo se DataSync muestra lo que hay en el manifiesto (y no todo lo que se encuentra en la ubicación de origen).
- Con un [filtro de inclusión](#), solo DataSync muestra lo que coincide con el filtro de tu ubicación de origen.
- Con un filtro de exclusión, DataSync muestra todo lo que hay en la ubicación de origen antes de aplicar el filtro.

Tipo: largo

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)

- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskExecutionListEntry

Representa una sola entrada en una lista de ejecuciones de AWS DataSync tareas que se devuelve con la [ListTaskExecutions](#) operación.

Contenido

Status

Estado de una ejecución de una tarea. Para obtener más información, consulte [Task execution statuses](#).

Tipo: cadena

Valores válidos: QUEUED | CANCELLING | LAUNCHING | PREPARING | TRANSFERRING | VERIFYING | SUCCESS | ERROR

Obligatorio: no

TaskExecutionArn

Nombre de recurso de Amazon (ARN) de la ejecución de la tarea.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

TaskMode

El modo de tarea que está utilizando. Para obtener más información, consulte [Elegir un modo de tarea para la transferencia de datos](#).

Tipo: cadena

Valores válidos: BASIC | ENHANCED

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskExecutionResultDetail

Proporciona información detallada sobre el resultado de la ejecución de la AWS DataSync tarea.

Contenido

ErrorCode

Error que DataSync se produjo durante la ejecución de la tarea. Puede utilizar esta información para ayudar a [solucionar problemas](#).

Tipo: cadena

Requerido: no

ErrorDetail

La descripción detallada de un error que DataSync se produjo durante la ejecución de la tarea. Puede utilizar esta información para ayudar a [solucionar problemas](#).

Tipo: cadena

Requerido: no

PrepareDuration

El tiempo en milisegundos que duró la ejecución de la tarea durante el PREPARING paso. Para obtener más información, consulte [Task execution statuses](#).

En el caso de las tareas en modo mejorado, el valor es siempre 0. Para obtener más información, consulte [Cómo DataSync se prepara la transferencia de datos](#).

Tipo: largo

Rango válido: valor mínimo de 0.

Obligatorio: no

PrepareStatus

El estado del PREPARING paso de ejecución de la tarea. Para obtener más información, consulte [Task execution statuses](#).

Tipo: cadena

Valores válidos: PENDING | SUCCESS | ERROR

Obligatorio: no

TotalDuration

El tiempo en milisegundos durante el que se ejecutó la tarea.

Tipo: largo

Rango válido: valor mínimo de 0.

Obligatorio: no

TransferDuration

El tiempo en milisegundos que duró la ejecución de la tarea en el TRANSFERRING paso. Para obtener más información, consulte [Task execution statuses](#).

En el caso de las tareas en modo mejorado, el valor es siempre 0. Para obtener más información, consulte [Cómo se DataSync transfieren los datos](#).

Tipo: largo

Rango válido: valor mínimo de 0.

Obligatorio: no

TransferStatus

El estado del TRANSFERRING paso de la ejecución de la tarea. Para obtener más información, consulte [Task execution statuses](#).

Tipo: cadena

Valores válidos: PENDING | SUCCESS | ERROR

Obligatorio: no

VerifyDuration

El tiempo en milisegundos que duró la ejecución de la tarea en el VERIFYING paso. Para obtener más información, consulte [Task execution statuses](#).

En el caso de las tareas en modo mejorado, el valor es siempre 0. Para obtener más información, consulte [Cómo se DataSync verifica la integridad de los datos](#).

Tipo: largo

Rango válido: valor mínimo de 0.

Obligatorio: no

VerifyStatus

El estado del VERIFYING paso de la ejecución de la tarea. Para obtener más información, consulte [Task execution statuses](#).

Tipo: cadena

Valores válidos: PENDING | SUCCESS | ERROR

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskFilter

Puede utilizar filtros de API para acotar la lista de recursos devueltos por `ListTasks`. Por ejemplo, para recuperar todas las tareas en una ubicación de origen, puede utilizar `ListTasks` con el nombre del filtro `LocationId` y `Operator Equals` con el ARN de la ubicación.

Para obtener más información, consulte [Filtrar DataSync recursos](#).

Contenido

Name

Nombre del filtro que se está utilizando. Cada llamada a la API admite una lista de filtros que están disponibles para ella. Por ejemplo, `LocationId` para `ListTasks`.

Tipo: cadena

Valores válidos: `LocationId` | `CreationTime`

Obligatorio: sí

Operator

Es el operador que se utiliza para comparar los valores de los filtros (por ejemplo, `Equals` o `Contains`).

Tipo: cadena

Valores válidos: `Equals` | `NotEquals` | `In` | `LessThanOrEqualTo` | `LessThan` | `GreaterThanOrEqual` | `GreaterThan` | `Contains` | `NotContains` | `BeginsWith`

Obligatorio: sí

Values

Valores por los que quiere filtrar. Por ejemplo, es posible que desee mostrar solo las tareas para una ubicación de destino determinada.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Patrón: `^[0-9a-zA-Z_\ \-:\*\.\ \\/\?\-]*$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskListEntry

Representa una sola entrada en una lista de tareas. `TaskListEntry` devuelve una matriz que contiene una lista de tareas cuando se llama a la [ListTasks](#) operación. Una tarea incluye los sistemas de archivos de origen y destino que se van a sincronizar y las opciones que se van a utilizar en las tareas.

Contenido

Name

El nombre de la tarea .

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[a-zA-Z0-9\s+=._:@/-]+$`

Obligatorio: no

Status

El estado de la tarea.

Tipo: cadena

Valores válidos: AVAILABLE | CREATING | QUEUED | RUNNING | UNAVAILABLE

Obligatorio: no

TaskArn

El nombre de recurso de Amazon (ARN) de la tarea.

Tipo: cadena

Limitaciones de longitud: longitud máxima de 128 caracteres.

Patrón: `^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}$`

Obligatorio: no

TaskMode

El modo de tarea que está utilizando. Para obtener más información, consulte [Elegir un modo de tarea para la transferencia de datos](#).

Tipo: cadena

Valores válidos: BASIC | ENHANCED

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskReportConfig

Especifica cómo desea configurar un informe de tareas, que proporciona información detallada sobre la AWS DataSync transferencia.

Para obtener más información, consulte [Informes de tarea](#).

Contenido

Destination

Especifica el bucket de Amazon S3 en el que se DataSync carga el informe de tareas. Para obtener más información, consulte [Informes de tarea](#).

Tipo: objeto [ReportDestination](#)

Obligatorio: no

ObjectVersionIds

Especifica si el informe de tareas incluye la nueva versión de cada objeto transferido a un bucket de S3. Esto solo se aplica si [habilita el control de versiones en su bucket](#). Tenga en cuenta que si lo establece en INCLUDE, puede aumentar la duración de la ejecución de la tarea.

Tipo: cadena

Valores válidos: INCLUDE | NONE

Obligatorio: no

OutputType

Especifica el tipo de informe de tareas que desea:

- SUMMARY_ONLY: proporciona los detalles necesarios sobre la tarea, como el número de archivos, objetos y directorios transferidos y la duración de la transferencia.
- STANDARD: proporciona detalles completos sobre la tarea, incluida una lista completa de los archivos, objetos y directorios que se transfirieron, omitieron, verificaron, etc.

Tipo: cadena

Valores válidos: SUMMARY_ONLY | STANDARD

Obligatorio: no

Overrides

Personaliza el nivel de informes para algunos aspectos del informe de tareas. Por ejemplo, es posible que su informe generalmente solo incluya errores, pero puede especificar que desea una lista de aciertos y errores solo para los archivos que DataSync intentó eliminar en su ubicación de destino.

Tipo: objeto [ReportOverrides](#)

Obligatorio: no

ReportLevel

Especifica si desea que el informe de tareas incluya solo los errores de la transferencia o una lista de lo que se realizó correctamente y lo que no.

- **ERRORS_ONLY**: un informe muestra lo que no DataSync se pudo transferir, omitir, verificar y eliminar.
- **SUCCESSES_AND_ERRORS**: un informe muestra lo que DataSync se pudo y no se pudo transferir, omitir, verificar y eliminar.

Tipo: cadena

Valores válidos: **ERRORS_ONLY** | **SUCCESSES_AND_ERRORS**

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskSchedule

Configura la AWS DataSync tarea para que se ejecute según una [programación](#) (con un intervalo mínimo de 1 hora).

Contenido

ScheduleExpression

Especifica la programación de tareas mediante una expresión Cron o Rate.

Use expresiones Cron para las programaciones de tareas que se ejecuten a una hora y un día específicos. Por ejemplo, la siguiente expresión Cron crea un programa de tareas que se ejecuta a las 8:00 del primer miércoles de cada mes:

```
cron(0 8 * * 3#1)
```

Utilice expresiones Rate para los programas de tareas que se ejecuten a intervalos regulares. Por ejemplo, la siguiente expresión Rate crea un programa de tareas que se ejecuta cada 12 horas:

```
rate(12 hours)
```

Para obtener información sobre la sintaxis de las expresiones cron y rate, consulta la [Guía del EventBridge usuario de Amazon](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 256.

Patrón: `^[a-zA-Z0-9\ \_\\*\?\\,\\|\\^\\-\\\/\\#\\$\\(\\)\\+]*$`

Obligatorio: sí

Status

Especifica si habilitar o deshabilitar la programación de tareas. La programación está habilitada de forma predeterminada, pero puede haber situaciones en las que necesite deshabilitarla. Por ejemplo, es posible que tenga que pausar una transferencia periódica para solucionar un problema con la tarea o realizar tareas de mantenimiento en el sistema de almacenamiento.

DataSync podría deshabilitar su programación automáticamente si la tarea falla repetidamente con el mismo error. Para obtener más información, consulte [TaskScheduleDetails](#).

Tipo: cadena

Valores válidos: ENABLED | DISABLED

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

TaskScheduleDetails

Proporciona información sobre el [programa de la tarea](#) AWS DataSync .

Contenido

DisabledBy

Indica cómo se deshabilitó el programa de la tarea.

- USER- Su programación se ha desactivado manualmente mediante la [UpdateTask](#) operación o la DataSync consola.
- SERVICE- Tu programación se desactivó automáticamente DataSync porque la tarea falló repetidamente con el mismo error.

Tipo: cadena

Valores válidos: USER | SERVICE

Obligatorio: no

DisabledReason

Indica el motivo por el que el programa de la tarea está inhabilitado.

Si su programa ha sido inhabilitado por USER, verá un mensaje de `Manually disabled by user..`

Si su programa ha sido inhabilitado por SERVICE, verá un mensaje de error que lo ayudará a entender por qué la tarea sigue fallando. Para obtener información sobre cómo resolver DataSync errores, consulta [Solución de problemas relacionados con DataSync las transferencias](#).

Tipo: cadena

Limitaciones de longitud: longitud máxima de 8192.

Patrón: `^[\\w\\s.,'?!:;\\/=|<>()-]*$`

Obligatorio: no

StatusUpdateTime

Indica la última vez que se modificó el estado de la programación de tareas. Por ejemplo, si desactiva DataSync automáticamente tu programación debido a un error repetido, podrás ver cuándo se desactivó la programación.

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los idiomas específicos AWS SDKs, consulta lo siguiente:

- [AWS SDK para C++](#)
- [AWS SDK para Java V2](#)
- [AWS SDK para Ruby V3](#)

Errores comunes

En esta sección se enumeran los errores comunes a las acciones de la API de todos los AWS servicios. En el caso de los errores específicos de una acción de la API de este servicio, consulte el tema de dicha acción de la API.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

IncompleteSignature

La firma de la solicitud no se ajusta a AWS los estándares.

Código de estado HTTP: 400

InternalFailure

El procesamiento de la solicitud ha devuelto un error debido a un error o una excepción desconocidos.

Código de estado HTTP: 500

InvalidAction

La acción u operación solicitada no es válida. Compruebe que la acción se ha escrito correctamente.

Código de estado HTTP: 400

InvalidClientTokenId

El identificador de clave de AWS acceso o certificado X.509 proporcionado no existe en nuestros registros.

Código de estado HTTP: 403

NotAuthorized

No tiene permiso para realizar esta acción.

Código de estado HTTP: 400

OptInRequired

El identificador de clave de AWS acceso necesita una suscripción al servicio.

Código de estado HTTP: 403

RequestExpired

La solicitud llegó al servicio más de 15 minutos después del sello de fecha de la solicitud o más de 15 minutos después de la fecha de caducidad de la solicitud (por ejemplo, en el caso de los prefirados URLs), o el sello de fecha de la solicitud es más de 15 minutos en el futuro.

Código de estado HTTP: 400

ServiceUnavailable

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 503

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

ValidationError

La entrada no cumple las restricciones especificadas por un AWS servicio.

Código de estado HTTP: 400

Parámetros comunes

La siguiente lista contiene los parámetros que utilizan todas las acciones para firmar solicitudes de Signature Version 4 con una cadena de consulta. Los parámetros específicos de acción se enumeran en el tema correspondiente a la acción. Para obtener más información sobre la versión 4 de Signature, consulte [Firmar solicitudes de AWS API](#) en la Guía del usuario de IAM.

Action

Las acciones que se van a realizar.

Tipo: cadena

Obligatorio: sí

Version

La versión de API para la que está escrita la solicitud, expresada en el formato YYYY-MM-DD.

Tipo: cadena

Obligatorio: sí

X-Amz-Algorithm

El algoritmo de hash que utilizó para crear la solicitud de firma.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Valores válidos: AWS4-HMAC-SHA256

Obligatorio: condicional

X-Amz-Credential

El valor del ámbito de la credencial, que es una cadena que incluye la clave de acceso, la fecha, la región a la que se dirige, el servicio que solicita y una cadena de terminación ("aws4_request"). El valor se expresa en el siguiente formato: access_key/AAAAMMDD/region/service/aws4_request.

Para obtener más información, consulte [Crear una solicitud de AWS API firmada](#) en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-Date

La fecha utilizada para crear la firma. El formato debe ser ISO 8601 formato básico (AAAAMMDD'T'HHMMSS'Z'). Por ejemplo, la siguiente fecha y hora es un X-Amz-Date valor válido:20120325T120000Z.

Condición: X-Amz-Date es opcional en todas las solicitudes; puede utilizarse para anular la fecha empleada para firmar solicitudes. Si el encabezado de fecha se especifica en el formato básico ISO 8601, no X-Amz-Date es obligatorio. Cuando X-Amz-Date se usa, siempre anula el valor del encabezado de fecha. Para obtener más información, consulte [Elementos de la firma de una solicitud de AWS API](#) en la Guía del usuario de IAM.

Tipo: cadena

Obligatorio: condicional

X-Amz-Security-Token

El token de seguridad temporal que se obtuvo mediante una llamada a AWS Security Token Service (AWS STS). Para obtener una lista de servicios compatibles con las credenciales de seguridad temporales de AWS STS, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Condición: si utilizas credenciales de seguridad temporales de AWS STS, debes incluir el token de seguridad.

Tipo: cadena

Obligatorio: condicional

X-Amz-Signature

Especifica la firma codificada hexadecimal que se calculó a partir de la cadena que se va a firmar y la clave de firma derivada.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-SignedHeaders

Especifica todos los encabezados HTTP que se incluyeron como parte de la solicitud canónica.

Para obtener más información sobre cómo especificar encabezados firmados, consulte [Crear una solicitud de AWS API firmada](#) en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

Historial del documento

En la siguiente tabla se describen las adiciones importantes a la AWS DataSync documentación. También actualizamos la documentación con frecuencia para dar cuenta de los comentarios que nos envía.

Para recibir notificaciones sobre las actualizaciones de esta documentación, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Discovery ya no está disponible	A partir del 20 de mayo de 2025, Discovery dejará de estar DataSync disponible.	20 de mayo de 2025
AWS actualización de política gestionada: actualización de la política existente	La AWSDaSyncFullAccess política ha actualizado las declaraciones de permisos que eliminan las condiciones de etiquetado de los permisos que se DataSync utilizan para crear secretos de Secrets Manager.	13 de mayo de 2025
AWS actualización gestionada de la política: actualización de la política existente	La AWSDaSyncFullAccess política tiene nuevos permisos que permiten DataSync trabajar con ella AWS Secrets Manager.	7 de mayo de 2025
AWS actualización de política gestionada: actualización de la política existente	La AWSDaSyncFullAccess política tiene nuevos permisos que permiten DataSync trabajar con ella AWS Secrets Manager.	23 de abril de 2025

AWS actualización de política gestionada: actualización de la política existente	La AWSDDataSyncFullAccess política tiene nuevos permisos que DataSync permiten trabajar con AWS Secrets Manager y AWS Key Management Service.	23 de abril de 2025
AWS actualización de política gestionada: actualización de la política existente	AWSDDataSyncService RolePolicy Tiene nuevos permisos que permiten DataSync trabajar con ellos AWS Secrets Manager.	15 de abril de 2025
Realizar migraciones de datos de gran tamaño	Aprenda a planificar migraciones de datos a gran escala mediante DataSync la transferencia de archivos u objetos desde un almacenamiento local o desde otro tipo de almacenamiento en la nube. AWS	19 de febrero de 2025
Support para Kerberos con ubicaciones de pequeñas y medianas empresas	DataSync ahora puede usar la autenticación Kerberos al conectarse a servidores de archivos del bloque de mensajes del servidor (SMB).	28 de enero de 2025
New Región de AWS	AWS DataSync está disponible para transferencias de datos en la región de México (Central).	14 de enero de 2025
New Región de AWS	AWS DataSync está disponible para transferencias de datos en la región Asia Pacífico (Tailandia).	7 de enero de 2025

<u>Actualice las ubicaciones AWS de almacenamiento</u>	Ahora puede actualizar sus ubicaciones de FSx transferencia de Amazon S3, Amazon EFS y Amazon.	18 de diciembre de 2024
<u>Ya no es compatible con Snowball Edge</u>	A partir del 12 de noviembre de 2024, ya DataSync no es compatible AWS Snowball Edge.	13 de noviembre de 2024
<u>Nueva política AWS gestionada</u>	El rol DataSync vinculado al servicio denominado <code>AWSServiceRoleForDataSync</code> usa una nueva política administrada denominada <code>AWSDataSyncServiceRolePolicy</code> .	30 de octubre de 2024
<u>Presentamos el modo mejorado</u>	Con el modo mejorado, puede transferir un número prácticamente ilimitado de objetos entre ubicaciones de Amazon S3.	30 de octubre de 2024
<u>AWS actualizaciones de políticas gestionadas: actualización de una política existente</u>	La <code>AWSDataSyncFullAccess</code> política tiene un nuevo permiso para los servicios que funcionan con DataSync.	30 de octubre de 2024
<u>Soporte para cuentas de almacenamiento Azure v1 de uso general</u>	DataSync puede funcionar con cuentas Azure de almacenamiento de uso general en caso de transferencias de ida y vuelta. Microsoft Azure Blob Storage	4 de octubre de 2024

Nueva forma de configurar los programas de tareas	Puede configurar sus cronogramas de DataSync tareas mediante expresiones de tasas.	22 de agosto de 2024
New Región de AWS	AWS DataSync está disponible para transferencias de datos en la región Asia Pacífico (Malasia).	21 de agosto de 2024
Soporte para transferencias entre regiones sin agentes que incluyen una región opcional	Ya no necesitas un DataSync agente para las transferencias entre servicios AWS de almacenamiento cuando hay al menos una ubicación de almacenamiento habilitada. Región de AWS	24 de julio de 2024
AWS actualizaciones de políticas gestionadas: actualización de una política existente	La AWSDataSyncFullAccess política tiene un nuevo permiso para los servicios que funcionan con DataSync.	22 de julio de 2024
Tutorial entre cuentas de S3 actualizado	Se han eliminado algunos permisos de usuario de la cuenta de origen que ya no son necesarios para esta transferencia.	10 de junio de 2024
Nuevo estado de ejecución de tarea	El estado CANCELLING indica cuándo se cancela la ejecución de una tarea.	15 de mayo de 2024

<u>Nueva opción para pausar programas de tareas</u>	Puede deshabilitar la programación de AWS DataSync tareas cuando necesite solucionar problemas o realizar tareas de mantenimiento del sistema de almacenamiento.	24 de abril de 2024
<u>Cifrado TLS actualizado para los puntos de conexión de FIPS</u>	AWS DataSync utiliza el cifrado TLS_AES_128_GCM_SHA256 (secp256r1) para los puntos finales del servicio del Estándar Federal de Procesamiento de Información (FIPS).	22 de abril de 2024
<u>AWS actualizaciones de políticas gestionadas: actualización de una política existente</u>	La AWSDataSyncFullAccess política tiene un nuevo permiso para los servicios que funcionan con DataSync.	16 de febrero de 2024
<u>Transfiera archivos u objetos específicos con un manifiesto</u>	AWS DataSync puede transferir una lista de archivos u objetos mediante un manifiesto.	7 de febrero de 2024
<u>New Región de AWS</u>	AWS DataSync ahora está disponible para transferencias de datos en la región Canadá Oeste (Calgary).	20 de diciembre de 2023
<u>Compatibilidad con transferencias con proveedores de nube adicionales</u>	AWS DataSync ahora puede transferir datos entre los servicios AWS de almacenamiento y IBM Cloud Object Storage o Seagate Lyve Cloud.	7 de noviembre de 2023

<u>Compatibilidad con transferencias con Alibaba Cloud Object Storage Service</u>	AWS DataSync ahora puede transferir datos entre los servicios AWS de almacenamiento y Alibaba Cloud Object Storage Service.	25 de septiembre de 2023
<u>Compatibilidad con informes de tareas</u>	Supervise sus AWS DataSync transferencias con informes de tareas.	30 de agosto de 2023
<u>New Región de AWS</u>	AWS DataSync ahora está disponible para transferencias de datos en la región de Israel (Tel Aviv).	23 de agosto de 2023
<u>Compatibilidad con transferencias con proveedores de nube adicionales</u>	AWS DataSync ahora puede transferir datos entre los servicios AWS de almacenamiento y varios otros proveedores de servicios en la nube (como Wasabi Cloud Storage, DigitalOcean Spaces, y Oracle Cloud Infrastructure Object Storage).	8 de agosto de 2023
<u>Disponibilidad general de soporte de Microsoft Azure Blob Storage</u>	AWS DataSync ahora puede transferir objetos hacia y desde Microsoft Azure Blob Storage.	25 de julio de 2023
<u>Compatibilidad con TLS 1.3</u>	Al realizar transferencias entre ubicaciones de almacenamiento, AWS DataSync ahora cifra todo el tráfico de la red con Transport Layer Security (TLS) 1.3.	28 de junio de 2023

Nuevas métricas de Discovery DataSync	AWS DataSync Discovery ahora pueden indicarle cuántos LUNs (números de unidades lógicas) hay en un clúster de recursos de almacenamiento, una máquina virtual de almacenamiento (SVM) o un volumen.	28 de junio de 2023
New Región de AWS	AWS DataSync ahora está disponible para transferencias de datos en la región de Asia Pacífico (Melbourne).	24 de mayo de 2023
Compatibilidad con el almacenamiento compatible con S3 de Snowball Edge	Se puede utilizar AWS DataSync para transferir datos entre el almacenamiento AWS Snowball Edge y AWS los servicios de almacenamiento compatibles con Amazon S3.	18 de mayo de 2023
AWS actualizaciones de políticas gestionadas: actualización de una política existente	La AWSDataSyncFullAccess política tiene nuevos permisos para los servicios que funcionan con DataSync.	2 de mayo de 2023
Disponibilidad general de AWS DataSync Discovery	Utilice DataSync Discovery para acelerar su migración a AWS.	25 de abril de 2023
Versión preliminar pública de compatibilidad con Microsoft Azure Blob Storage	AWS DataSync ahora puede transferir objetos desdeMicrosoft Azure Blob Storage.	29 de marzo de 2023

Nueva política de IAM	Para admitir la función de DataSync detección , DataSync utiliza el rol vinculado al servicio denominado. <code>AWSServiceRoleForDataSyncDiscovery</code>	21 de marzo de 2023
New Regiones de AWS	AWS DataSync ahora está disponible en las siguientes regiones Regiones de AWS: Asia Pacífico (Hyderabad), Europa (España) y Europa (Zúrich).	6 de febrero de 2023
Uso de etiquetas en la ejecución de tareas	Ahora puedes etiquetar las ejecuciones de tus AWS DataSync tareas.	16 de diciembre de 2022
Compatibilidad con S3 Glacier Instant Retrieval	Ahora puede transferir objetos directamente a la clase de almacenamiento S3 Glacier Instant Retrieval.	16 de diciembre de 2022
Copia de metadatos del sistema de objetos	AWS DataSync ahora puede copiar los metadatos del sistema al transferirlos entre un sistema de almacenamiento de objetos y Amazon S3.	16 de diciembre de 2022
New Regiones de AWS	AWS DataSync ya está disponible en las regiones de China (Pekín) y China (Ningxia).	14 de diciembre de 2022
New Región de AWS	AWS DataSync ya está disponible en la región de Oriente Medio (EAU).	16 de noviembre de 2022

<u>Compatibilidad con certificados autofirmados con ubicaciones de almacenamiento de objetos</u>	AWS DataSync puede conectarse a ubicaciones de almacenamiento de objetos que utilizan certificados privados o autofirmados.	25 de octubre de 2022
<u>Obtener información sobre la compresión de datos</u>	AWS DataSync puede proporcionar el número físico de bytes transferidos a través de la red después de aplicar la compresión.	25 de octubre de 2022
<u>Versión preliminar pública de AWS DataSync Discovery</u>	Utilice DataSync Discovery para acelerar su migración a AWS.	21 de septiembre de 2022
<u>Nueva opción de migración de datos hacia o desde Google Cloud Storage</u>	Puede transferir datos hacia o desde Google Cloud Storage mediante la implementación de un agente de AWS DataSync en Google Cloud.	21 de julio de 2022
<u>Support for Amazon FSx for NetApp ONTAP file systems</u>	AWS DataSync ahora puede transferir archivos y carpetas desde y hacia los sistemas FSx de archivos ONTAP.	28 de junio de 2022
<u>Nuevas opciones de seguridad para ubicaciones de Amazon EFS</u>	AWS DataSync pueden acceder a los sistemas de archivos de Amazon EFS mediante TLS, puntos de acceso y funciones de IAM.	31 de mayo de 2022

Migración de datos hacia o desde Google Cloud Storage y Azure Files	Con AWS DataSync, puede transferir datos a o desde Google Cloud Storage y Azure Files. Para obtener más información, consulte Creating a location for object storage y Creating a location for SMB .	24 de mayo de 2022
Nueva configuración de AWS DataSync tareas	Con la opción Copiar etiquetas de objetos, puede especificar si desea mantener las etiquetas de los objetos al realizar transferencias entre sistemas de almacenamiento de objetos.	5 de mayo de 2022
New Región de AWS	AWS DataSync ya está disponible en la región de Asia Pacífico (Yakarta).	19 de abril de 2022
Support para Amazon FSx para sistemas de archivos OpenZFS	AWS DataSync ahora puede transferir archivos y carpetas desde y hacia los sistemas de FSx archivos OpenZFS.	5 de abril de 2022
Soporte para los sistemas FSx de archivos Amazon for Lustre	AWS DataSync ahora puede transferir archivos y carpetas desde y hacia los sistemas FSx de archivos Lustre.	10 de diciembre de 2021
Compatibilidad con el Sistema de archivos distribuido de Hadoop (HDFS)	AWS DataSync ahora admite la transferencia de archivos y carpetas desde y hacia clústeres HDFS.	3 de noviembre de 2021
New Región de AWS	AWS DataSync ya está disponible en la región de Asia Pacífico (Osaka).	28 de julio de 2021

[Transferencias totalmente automatizadas entre servicios AWS de almacenamiento](#)

AWS DataSync ahora puede transferir archivos u objetos entre Amazon S3, Amazon EFS o FSx Windows File Server con solo unos clics en la DataSync consola.

9 de noviembre de 2020

[Ajuste del ancho de banda de la red utilizado por una tarea en ejecución](#)

AWS DataSync ahora permite a los clientes ajustar el ancho de banda de red que utiliza una DataSync tarea en ejecución. Esto ayuda a minimizar el impacto en otros usuarios o aplicaciones cuando una tarea dura varios días.

9 de noviembre de 2020

[Soporte mejorado para las funciones de máquinas DataSync virtuales \(VM\) locales](#)

La consola host de la máquina virtual del AWS DataSync agente ahora admite funciones mejoradas, incluida la activación de un agente desde la consola local.

19 de octubre de 2020

[AWS DataSync ahora puede transferir datos hacia y desde AWS Outposts](#)

DataSync ahora admite la transferencia de objetos hacia y desde Amazon S3 en adelante AWS Outposts.

30 de septiembre de 2020

[Compatibilidad con el filtrado de API](#)

AWS DataSync ahora admite el filtrado de las llamadas a las `ListLocations` API `ListTasks` y las llamadas a las API, lo que le permite recuperar fácilmente la configuración de las tareas de transferencia de datos mediante filtros como el origen o el destino de la transferencia de datos.

18 de agosto de 2020

[Compatibilidad con la copia de datos de su almacenamiento de objetos autoadministrado](#)

AWS DataSync ahora admite la transferencia de datos entre el almacenamiento de objetos autogestionado y Amazon S3, Amazon Elastic File System o FSx Windows File Server.

27 de julio de 2020

[Compatibilidad con la máquina virtual basada en el kernel \(KVM\) de Linux y los hipervisores de Microsoft Hyper-V](#)

AWS DataSync ahora ofrece la posibilidad de implementar agentes locales en las plataformas de virtualización KVM y Microsoft Hyper-V, además de las opciones existentes y VMware de Amazon. EC2

1 de julio de 2020

[AWS DataSync ahora puede configurar automáticamente su configuración de Amazon CloudWatch Logs](#)

Al utilizarla DataSync, ahora tiene la opción de generar automáticamente la política de recursos y grupos de CloudWatch registros necesaria para publicar los registros de su transferencia de datos, lo que simplifica la creación de tareas y la configuración de la supervisión.

1 de julio de 2020

[AWS DataSync ahora puede transferir datos desde y hacia AWS Snowball Edge](#)

DataSync ahora admite la transferencia de archivos hacia y desde AWS Snowball Edge, el elemento más pequeño de los dispositivos AWS Snow Family de transferencia de datos y computación perimetral. Snowball Edge es portátil, robusto y seguro: lo suficientemente pequeño y liviano como para caber en una mochila y capaz de soportar entornos hostiles.

17 de junio de 2020

[New Región de AWS](#)

AWS DataSync ya está disponible en la región de África (Ciudad del Cabo) y en la región de Europa (Milán).

16 de junio de 2020

[Funciones de monitoreo mejoradas con registro a nivel de archivo](#)

Ahora puede habilitar el registro detallado de los archivos y objetos copiados entre sus servidores NFS, servidores SMB, buckets de Amazon S3, sistemas de archivos Amazon EFS y FSx sistemas de archivos Windows File Server.

24 de abril de 2020

[Support para copiar datos entre su recurso compartido SMB y Amazon FSx for Windows File Server](#)

Ahora puede copiar datos entre su recurso compartido SMB y el servidor de archivos FSx de Windows.

24 de enero de 2020

[Compatibilidad con la programación de tareas](#)

Ahora puede ejecutar tareas manualmente o programarlas para que se ejecuten según una programación específica.

20 de noviembre de 2019

[New Región de AWS](#)

AWS DataSync ahora está disponible en las regiones Asia-Pacífico (Hong Kong), Asia Pacífico (Bombay), Europa (Estocolmo), Sudamérica (São Paulo) y AWS GovCloud EEUU-Este.

20 de noviembre de 2019

[New Región de AWS](#)

AWS DataSync ya está disponible en la región de Canadá (centro), la región de Europa (Londres) y la región de Europa (París).

2 de octubre de 2019

<u>Compatibilidad con las clases de almacenamiento de Amazon S3</u>	Ahora puede transferir objetos directamente a clases de almacenamiento de Amazon S3.	24 de septiembre de 2019
<u>New Región de AWS</u>	AWS DataSync ya está disponible en la región de Oriente Medio (Baréin).	28 de agosto de 2019
<u>Compatibilidad con la copia de datos entre el recurso compartido de Server Message Block (SMB) y Amazon S3 o Amazon EFS</u>	Ahora puede copiar datos entre el recurso compartido de archivos SMB y Amazon S3 o Amazon EFS.	22 de agosto de 2019
<u>Compatibilidad para utilizar puntos de conexión de nube privada virtual (VPC)</u>	Ahora puede crear una conexión privada entre su agente AWS y ejecutar tareas en una red privada. Esto aumenta la seguridad de los datos a medida que se copian a través de la red.	5 de agosto de 2019
<u>Compatibilidad con los puntos de conexión del estándar federal de procesamiento de información (FIPS)</u>	Ahora puede utilizar puntos de conexión del FIPS para crear agentes y ejecutar tareas.	5 de agosto de 2019
<u>New Región de AWS</u>	AWS DataSync ahora está disponible en la región AWS GovCloud (EE. UU.-Oeste).	11 de junio de 2019

[Compatibilidad con el uso de filtros](#)

A partir de ahora, puede aplicar filtros para transferir únicamente un subconjunto de archivos de la ubicación de origen cuando transfiera datos desde la ubicación de origen a la de destino.

22 de mayo de 2019

[Primera versión de AWS DataSync](#)

Versión general del AWS DataSync servicio.

26 de noviembre de 2018

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el [AWS glosario](#) de la Glosario de AWS Referencia.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.