



Guía del usuario de

AWS Transfer Family



AWS Transfer Family: Guía del usuario de

Copyright © 2026 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 Transfer Family?	1
¿Cómo AWS Transfer Family funciona	4
Publicaciones de blog relevantes para Transfer Family	6
Requisitos previos	9
Regiones, puntos de conexión y cuotas	9
Inscríbase en AWS	10
Configurar almacenamiento	10
Configurar un bucket de Amazon S3	11
Configuración de un sistema de archivos Amazon EFS	16
Creación de una política y un rol de IAM	20
Creación de un rol de usuario	21
Funcionamiento de las políticas de sesión	24
Ejemplo de política de read/write acceso	28
Tutoriales de Transfer Family	32
Introducción a los puntos de conexión del servidor	33
Requisitos previos	33
Paso 1: Inicia sesión en la consola AWS Transfer Family	34
Paso 2: Crea un SFTP-enabled servidor	35
Paso 3: agregar un usuario de servicio administradas	36
Paso 4: transferencia de un archivo mediante un cliente	37
Cree un flujo de trabajo de descifrado	39
Paso 1: creación y configuración de un rol de ejecución de IAM	40
Paso 2: creación de un flujo de trabajo administrado	41
Paso 3: agregar el flujo de trabajo a un servidor y crear un usuario	42
Paso 4: creación de un par de claves PGP	44
Paso 5: Guarde la clave privada PGP en AWS Secrets Manager	45
Paso 6: cifrado de un archivo	46
Paso 7: ejecución del flujo de trabajo y visualización de los resultados	47
Cree y utilice conectores SFTP	48
Tipos de salida de conectores	49
Paso 1: Cree los recursos de apoyo necesarios	50
Paso 2: Crear y probar un conector SFTP	56
Paso 3: envíe y recupere archivos mediante el conector SFTP	61

Procedimientos para crear un servidor Transfer Family para usarlo como servidor SFTP remoto	66
Utilice un proveedor de identidad personalizado	69
Requisitos previos	69
Paso 1: Crear una CloudFormation pila	70
Paso 2: verificación de la configuración del método API Gateway para su servidor	71
Paso 3: visualización de los detalles del servidor de Transfer Family	72
Paso 4: comprobación de que el usuario puede conectarse al servidor	74
Paso 5: prueba de la conexión SFTP y la transferencia de archivos	74
Paso 6: limitación del acceso al bucket	75
Actualice Lambda si utiliza Amazon EFS	77
Configure una configuración de AS2	78
Paso 1: creación de los certificados para AS2	80
Paso 2: Importar certificados como recursos de certificados de Transfer Family	84
Paso 3: Cree perfiles para usted y su socio comercial	85
Paso 4: Crear un servidor Transfer Family que utilice el protocolo AS2	86
Paso 5: creación de un acuerdo entre usted y su socio	89
Paso 6: creación de un conector entre usted y su socio	91
Paso 7: prueba del intercambio de archivos a través de AS2 mediante Transfer Family	92
Configura una aplicación web básica	94
Requisitos previos	94
Paso 1: Cree los recursos de apoyo necesarios	95
Paso 2: Crear una aplicación web Transfer Family	96
Paso 3: Configura el uso compartido de Cross-origin recursos (CORS) para tu bucket	97
Paso 4: Agrega un usuario a tu aplicación web Transfer Family	98
Paso 5: Registrar una ubicación en Amazon S3 y crear una concesión de acceso	99
Paso 6: Acceda a su aplicación web Transfer Family como usuario	102
Siguiendo pasos	103
Integre Okta como su proveedor de identidad para las aplicaciones web	104
Configure una aplicación web con acceso selectivo a varios cubos	106
Requisitos previos	106
Paso 1: Crear una aplicación web Transfer Family	107
Paso 2: Configure las funciones de IAM para el acceso a S3	108
Paso 3: Configura S3 Access Grants	110
Paso 4: Registrar las ubicaciones de los depósitos de S3	111
Paso 5: Crear concesiones de acceso	111

Paso 6: Configure la política CORS para los buckets S3	112
Paso 7: Probar la configuración	113
Conclusión	113
Transfer Family para SFTP, FTPS y FTP	114
Opciones de proveedor de identidades	114
AWS Transfer Family matriz de tipos de punto final	116
Configurar un punto final de servidor Transfer Family	121
Crea un SFTP-enabled servidor	123
Crea un FTPS-enabled servidor	131
Crea un FTP-enabled servidor	140
Creación de un servidor en una VPC	149
Uso de nombres de host personalizados	174
FTP/FTPS Consideraciones sobre el NLB	178
Transfiera archivos a través del punto final del servidor	179
Comandos disponibles SFTP/FTPS/FTP	182
Encuentre su punto de conexión de Amazon VPC	183
Evite errores setstat	185
Uso de OpenSSH	38
Utilice WinSCP	187
Uso de Cyberduck	37
Uso FileZilla	191
Utilice un cliente Perl	192
Utilice LFTP	192
Procesamiento de carga posterior	192
Mensajes SFTP	194
Administración de usuarios	196
Amazon EFS frente a Amazon S3	197
Directorios lógico	198
Cuotas de grupo de Active Directory	199
Service-managed usuarios	200
Proveedor de identidades personalizado	210
Servicio de directorio para MS AD	249
Servicio de directorio para Entra ID	260
Usa directorios lógicos	268
Comprender el chroot y la estructura de directorios	268
Reglas para el uso de directorios lógicos	269

Implementación de directorios lógicos	271
Ejemplos de configuración de directorios lógicos	274
Configuración de directorios lógicos para Amazon EFS	276
Respuesta personalizada AWS Lambda	276
Acceda a FSx para los sistemas de archivos NetApp ONTAP	277
Descripción general de	278
Requisitos previos	279
Cómo funciona el almacenamiento FSx con Transfer Family	280
Creación de un punto de acceso S3 para FSx	281
Uso de alias de puntos de acceso S3 con FSx	283
Configuración de Transfer Family para el almacenamiento FSx	285
Administración de usuarios para el almacenamiento de FSx	287
Configuración de clientes de transferencia de archivos	288
Solución de problemas de almacenamiento FSx	290
Aplicaciones web Transfer Family	291
Regiones de AWS para aplicaciones web Transfer Family	292
Compatibilidad de navegadores para aplicaciones AWS Transfer Family web	292
Cómo crear una aplicación web Transfer Family	292
Configura tu proveedor de identidad	295
Configurar roles de IAM	297
Configurar una aplicación web Transfer Family	300
Crea una aplicación web de Transfer Family	300
Direccionamiento IP	302
Creación de una aplicación web de Transfer Family en una VPC	303
Crea una aplicación web de Transfer Family	304
Post-creation pasos	306
Cross-origin política de uso compartido de recursos (CORS)	306
Restricción del acceso a un punto de conexión de la VPC específico	307
Asigne o añada usuarios o grupos a una aplicación web Transfer Family	308
Configure el uso compartido de Cross-origin recursos (CORS) para su depósito	312
Configuración de las concesiones de acceso a Amazon S3	314
Usa una URL personalizada	320
Registro de aplicaciones web de Transfer Family	323
Habilitación de eventos de datos de Amazon S3	324
Ejemplos de registros de autenticación	326
Visualización de entradas de registro	333

Solución de problemas de sus aplicaciones web	334
Solucionar errores de red	335
Solucione el problema de que el bucket configurado no aparece	335
Solucionar errores de URL personalizadas	336
Soluciona errores varios	337
Aparecen cubos S3 duplicados en la aplicación web	337
Instrucciones para el usuario final	338
Cuotas de aplicaciones web	338
Usuarios de IAM Identity Center	339
Third-party usuarios finales	340
Interfaz de usuario final de Transfer Family	340
Acciones disponibles	341
Conectores SFTP	344
Creación de conectores SFTP	344
Elegir el tipo de salida del conector SFTP	345
Elegir el modo de direccionamiento IP	346
Almacene credenciales en Secrets Manager.	347
Cree un conector SFTP con salida gestionada por el servicio	349
Cree un conector SFTP con salida VPC-based	360
Prueba de un conector SFTP	372
Conectividad de VPC	373
Uso de conectores SFTP	374
Transferencia de archivos	375
Enumere el contenido de los directorios remotos	377
Mueva y elimine archivos en el servidor remoto	379
Supervisión de conectores SFTP	381
Utilice la API del conector para consultar el estado de las solicitudes de transferencia de archivos	381
Ver los eventos del conector SFTP en Amazon EventBridge	382
Ver los registros del conector SFTP en Amazon CloudWatch	382
Monitorización de conectores de tipo salida de VPC	382
Administración de conectores SFTP	384
Actualizar conectores SFTP	385
Ver los detalles del conector SFTP	386
Cuotas para conectores SFTP	387
Cuotas para conectores SFTP	387

Escalar sus conectores SFTP	389
Arquitecturas de referencia	390
Publicaciones de blog	390
Talleres	390
Soluciones	390
Arquitecturas de referencia de VPC	391
Transfer Family para AS2	393
Casos de uso de AS2	394
Plantillas AS2 CloudFormation	399
Personalización de plantillas AS2	399
Probar su implementación de AS2	399
Mejores prácticas para el despliegue de plantillas AS2	400
Configurar AS2	401
Configuraciones AS2	402
Cuotas de AS2	404
Características y funciones básicas de AS2	407
Administre los certificados AS2	409
Importar certificados AS2	410
Rotación de certificado AS2	412
Creación de perfiles de AS2	414
Crear un servidor AS2	415
Cree un servidor AS2 mediante la consola Transfer Family	415
Cree un servidor AS2 mediante una plantilla	419
Cree un acuerdo AS2	422
Configure los conectores AS2	424
Cree un conector AS2	425
Algoritmos de conector AS2	428
Autenticación básica para conectores AS2	429
Habilite la autenticación básica para los conectores AS2	430
Ver los detalles del conector	433
Transfiere mensajes AS2	436
Reciba mensajes AS2	437
Configuración de HTTPS para AS2	438
Transfiera archivos con conectores AS2	444
Nombres y ubicaciones de los archivos	447
Códigos de estado	449

Ejemplos de archivos de JSON	450
Encabezados HTTP personalizados para AS2	452
Descripción general de la plantilla	453
Cómo funciona	453
Características principales de	454
Detalles de la implementación	454
Despliegue y uso	455
Monitor AS2	456
Códigos de estado AS2	458
Códigos de error de AS2	459
Supervisión del vencimiento de los certificados	472
DaysUntilExpiry métrica	472
Prácticas recomendadas para la supervisión de certificados	473
Ejemplos de configuraciones de alarma	474
Gestión de flujos de trabajo de procesamiento de archivos	475
Crear un flujo de trabajo	477
Configuración y ejecución de un flujo de trabajo	479
Visualización de flujos de trabajo	481
Utilice pasos predefinidos	484
Copiar archivo	484
Descifrar el archivo	489
Etiquetado de archivos	495
Eliminar archivo	496
Variables con nombre para los flujos de trabajo	497
Ejemplo de flujo de trabajo de etiquetado y eliminación	497
Uso de pasos de procesamiento de archivos personalizados	502
Uso de varias funciones de Lambda de forma consecutiva	504
Acceso a un archivo después de un procesamiento personalizado	504
Ejemplos de eventos enviados AWS Lambda al subir el archivo	505
Ejemplo de función de Lambda para un paso de flujo de trabajo personalizado	506
Permisos de IAM para un paso personalizado	507
Políticas de IAM para flujos de trabajo	508
Relaciones de confianza del flujo de trabajo	510
Ejemplo de rol de ejecución: descifrado, copiado y etiquetado	510
Ejemplo de rol de ejecución: ejecutar un rol y eliminarlo	512
Gestión de excepciones para un flujo de trabajo	513

Monitoreo de la ejecución del flujo	514
CloudWatch iniciar sesión en un flujo de trabajo	514
CloudWatch métricas para flujos de trabajo	517
Creación de un flujo de trabajo a partir de una plantilla	517
Eliminación de un flujo de trabajo de un servidor de Transfer Family	521
Límites y restricciones	522
Administración de servidores	525
Ver una lista de servidores	525
Eliminar un servidor	526
Vea los detalles del servidor SFTP	527
Vea los detalles del servidor AS2	528
Compatibilidad con IPv6	530
Limitaciones de IPv6	531
Configuración de IPv6 para servidores	531
Utilice ALB para un servidor público AS2 de doble pila	532
Editar detalles del servidor	534
Edite los protocolos de transferencia de archivos	537
Editar el punto de conexión del servidor	539
Edite el registro	540
Editar la política de seguridad	541
Cambio del flujo de trabajo administrado	543
Cambiar los banners de visualización de su servidor	544
Puesta de un servidor de online u offline	544
Edite la configuración del proveedor de identidades	545
Cambiar a un proveedor de identidades gestionado por un servicio	545
Cambiar a AWS Directory Service	546
Cambiar a un proveedor de identidad personalizado	546
Preservación del usuario durante las transiciones entre proveedores de identidad	551
Consideraciones importantes a la hora de cambiar de proveedor de identidad	551
Administración de las claves de host del servidor	551
Cuándo importar las claves de host	553
Agregue una clave de host de servidor adicional	553
Eliminar una clave de host	555
Rotar las claves del host del servidor	556
Información adicional sobre la clave del host del servidor	558
Monitoree el uso dentro de la consola	558

Administrar los controles de acceso	565
Creación de una política de acceso a un bucket de S3	566
Creación de una política de sesión	567
Ejemplo de política de sesión	568
Sustituciones anidadas de las políticas de sesión	571
Gestión dinámica de permisos	571
Descripción de la arquitectura de permisos de Transfer Family	571
Dos enfoques para la administración de permisos	572
Implementación de políticas de sesión	573
Implementación por tipo de usuario	574
Ejemplo: simplificar la administración de funciones con políticas de sesión	574
CloudTrail registro	578
Habilitar el CloudTrail registro	580
Habilitación de eventos de datos de Amazon S3	580
Ejemplo de entrada de registro para crear un servidor	581
Registros de acceso a datos	582
Ejemplo de entrada de registro para un acceso correcto a los datos	582
Operaciones comunes de acceso a datos	585
CloudWatch registro	586
Tipos de CloudWatch registro para Transfer Family	586
Crear registros para servidores	589
Crear registros para servidores	591
Actualización del registro de un servidor	592
Vista de la configuración del servidor	595
Administrar el registro de los flujos de trabajo	597
Configurar un rol para CloudWatch	600
Visualización de las transmisiones de registros de Transfer Family	602
Creación de CloudWatch alarmas de Amazon	606
Registro de llamadas a la API de S3 a los registros de acceso de S3	607
Ejemplos para limitar el problema del suplente confuso	607
CloudWatch estructura de registro para Transfer Family	609
Registros estructurados en JSON para Transfer Family	609
Registros heredados de Transfer Family	613
Ejemplo de entradas de CloudWatch registro	616
Ejemplos de entradas de registro de sesiones de transferencia	617
Ejemplos de entradas de registro para conectores SFTP	618

Ejemplos de entradas de registro para conectores de celosía de VPC	620
Ejemplos de entradas de registro para errores en el algoritmo de intercambio de claves	621
Uso de CloudWatch métricas	622
Dimensiones de Transfer Family	627
Notificaciones de usuario	627
CloudWatch consultas	628
Administrar eventos usando EventBridge	631
Transfer Family eventos	632
Eventos de servidor SFTP, FTPS y FTP	632
Eventos del conector SFTP	636
Eventos AS2	637
Envío de eventos de Transfer Family	638
Creación de patrones de eventos	639
Probar patrones de Transfer Family eventos para eventos	640
Permisos	641
Recursos adicionales	641
Referencia detallada de los eventos	641
Eventos de servidor	642
Eventos de conector	650
Eventos de AS2	657
Seguridad	664
Ventajas de la seguridad de la conectividad de VPC	665
Modelo de seguridad VPC Lattice	665
Mejores prácticas de seguridad para la conectividad de VPC	666
Políticas de seguridad para servidores	666
Algoritmos criptográficos	668
Detalles de la política de seguridad	679
Políticas de seguridad para conectores SFTP	697
Algoritmos criptográficos	698
Detalles de la política de seguridad del conector SFTP	698
Post-Quantum políticas de seguridad	700
Acerca del intercambio de claves híbrido poscuántico en SSH	701
Modo de uso	702
Cómo probarlo	703
Protección de datos	707
Cifrado de datos en Transfer Family	708

Cifrado en reposo	709
Administración de claves	710
Descripción general del algoritmo	711
Autenticación SSH	712
Algoritmos PGP	713
Generación de claves SSH	714
Rotar claves SSH	720
Generar claves PGP	723
Administración de claves PGP	724
Clientes PGP admitidos	728
Identity and Access Management	730
Público	730
Autenticación con identidades	730
Administración del acceso con políticas	732
Cómo AWS Transfer Family funciona con IAM	734
Identity-based ejemplos de políticas	738
Tag-based ejemplos de políticas	741
Solución de problemas de identidades y accesos	745
Claves de condición de IAM	747
Validación de conformidad	749
Resiliencia	750
Puntos finales de VPC para API	751
Control del acceso mediante políticas de puntos finales de VPC	751
Creación de un punto de conexión de VPC	752
Seguridad de la infraestructura	753
Consideraciones sobre la NLB y la NAT	753
Seguridad de la infraestructura de conectividad de VPC	755
Cortafuegos de aplicaciones web	756
Cross-service prevención policial confusa	757
Roles de usuario de Transfer Family	759
Roles del flujo de trabajo	761
Funciones de Transfer Family Connector	762
logging/invokeFunciones de Transfer Family	764
AWS políticas gestionadas	765
AWSTransferConsoleFullAccess	766
AWSTransferFullAccess	766

AWSTransferLoggingAccess	766
AWSTransferReadOnlyAccess	766
Actualizaciones de políticas	767
Módulos Transfer Family Terraform	768
servidores SFTP	768
Conectores SFTP	768
COMO 2	769
Intercambio de datos entre empresas	769
Solución de problemas de Transfer Family	770
Problemas de autenticación	770
Fallos de autenticación: SSH/SFTP	771
Se gestionó un problema de dominios no coincidentes en AD	771
Se han superado los límites de grupos de Active Directory	772
Varios problemas de autenticación	772
Solución de problemas de Amazon API Gateway	773
Solución de los problemas al probar su proveedor de identidad	775
Duplicar buckets de Amazon S3 en una aplicación web	337
Problemas con el conector SFTP	776
Solución de los problemas al agregar claves de host confiables para su conector SFTP	776
La negociación clave falla	777
Regulación del conector SFTP	777
Optimización del rendimiento del conector SFTP	778
Solucionar problemas de conectividad de VPC	779
Problemas varios con el conector SFTP	782
Problemas de conectividad SFTP	783
Solucionar problemas de conectividad de SFTP	783
Solucione los problemas del cliente SFTP	784
Solución de los problemas de carga de archivos	784
Solucionar problemas con el conector SFTP del tipo de salida de la VPC	785
Problemas con los proveedores de identidad personalizados	787
Solucionar errores de integración de API Gateway	788
Solucionar problemas de tiempos de espera de funciones Lambda	789
Solucione problemas constantes de tiempo de espera de Lambda	790
Solucione los problemas de las excepciones KeyError	790
Problemas de flujo de trabajo	791
Solución de problemas de flujos de trabajo administrados	791

Solución de los problemas de descifrado del flujo de trabajo	794
Problemas de EFS	798
Solución de problemas de Amazon EFS	798
Problemas de almacenamiento y cifrado	800
Solución de problemas de políticas para buckets de Amazon S3 cifrados	801
Solución de los problemas con la excepción ResourceNotFound	801
Problemas de supervisión y alerta	802
Solucione problemas con las métricas faltantes o incompletas CloudWatch	802
Solucione problemas de eventos faltantes EventBridge	803
Cross-region problemas de transferencia	804
Solucionar problemas de permisos de transferencia entre regiones	805
Solucione los problemas de rendimiento de las transferencias entre regiones	806
Problemas de implementación de Terraform	807
Solucione los errores de creación de recursos de Terraform	808
Solucione los problemas de administración del estado de Terraform	809
Problemas de integración de WAF	810
Solucione los problemas del WAF que bloquea el tráfico legítimo	810
Solucione los problemas de integración de WAF con proveedores de identidad personalizados	811
Service-managed problemas de los usuarios	812
Solución de los problemas de los usuarios administrados por el servicio	812
Problemas de AS2	813
Solución de los problemas de AS2	814
Problemas con el certificado AS2	814
Problemas con los recibos de AS2 MDN	814
Problemas de supervisión del vencimiento de los certificados	815
Referencia de API	817
Cómo realizar solicitudes a la API	818
Cabeceras de solicitud obligatorias para Transfer Family	819
Entrada y firma de la solicitud de Transfer Family	819
Respuestas de error	820
Bibliotecas disponibles	822
Proveedores de identidad	823
Convenciones	824
Formatos de ID	824
Formatos ARN	825

DNS y puntos finales	826
Puntos de conexión de API	826
Puntos finales del servidor	826
Historial de revisión	828
.....	dcccxlvii

¿Qué es AWS Transfer Family?

AWS Transfer Family es un servicio de transferencia segura que le permite transferir archivos dentro y fuera de los servicios de AWS almacenamiento. Transfer Family forma parte de la Nube de AWS plataforma. AWS Transfer Family ofrece un soporte totalmente gestionado para la transferencia de archivos a través de SFTP, AS2, FTPS, FTP y transferencias basadas en navegadores web directamente desde y hacia los servicios de almacenamiento. AWS Puede migrar, automatizar y supervisar sin problemas sus flujos de trabajo de transferencia de archivos manteniendo las configuraciones existentes del lado del cliente en materia de autenticación, acceso y firewalls, de modo que nada cambie para sus clientes, socios y equipos internos, ni para sus aplicaciones. Consulte [Primeros pasos AWS](#) para obtener más información y empezar a crear aplicaciones en la nube con Amazon Web Services.

AWS Transfer Family admite la transferencia de datos desde o hacia los siguientes servicios AWS de almacenamiento.

- Almacenamiento Amazon Simple Storage Service (Amazon S3). Para obtener más información sobre Amazon S3, consulte [Introducción a Amazon Simple Storage Service](#).
- Sistemas de archivos Amazon Elastic File System (Amazon EFS) de Amazon Elastic File System (Amazon EFS). Para obtener más información sobre EFS, consulte [¿Qué es Amazon Elastic File System?](#)

AWS Transfer Family admite la transferencia de datos a través de los siguientes protocolos:

- Protocolo seguro de transferencia de archivos (SFTP): versión 3

El documento oficial del IETF está aquí: [SSH File Transfer Protocol draft-ietf-secsh-filexfer-02.txt](#).

- Protocolo seguro de File Transfer (FTPS)
- Protocolo de File Transfer (FTP)
- Declaración de aplicabilidad 2 (AS2)
- Browser-based transferencias

 Note

Para las conexiones de datos FTP y FTPS, el rango de puertos que Transfer Family utiliza para establecer el canal de datos es 8192-8200.

Los protocolos de transferencia de archivos se utilizan en los flujos de intercambio de datos en diversos sectores, como son los servicios financieros, servicios sanitarios y el comercio minorista, entre otros. Transfer Family simplifica la migración de los flujos de trabajo de transferencia de archivos a AWS.

A continuación, se indican algunos casos de uso frecuentes para Amazon S3:

- Los datos se AWS transfieren cuando son subidos por terceros, como proveedores y socios.
- Subscription-based distribución de datos con sus clientes.
- Transferencias internas en el ámbito de una organización.

A continuación, se indican algunos casos de uso frecuentes para utilizar Transfer Family con Amazon EFS:

- Distribución de datos
- Cadena de suministro
- Administración de contenido
- Aplicaciones de servidor web

A continuación, se indican algunos casos de uso frecuentes para utilizar Transfer Family con AS2:

- Flujos de trabajo con requisitos de conformidad que se basan en contar con características de seguridad y protección de datos integradas en el protocolo
- Logística de la cadena de suministro
- Flujos de trabajo de pagos
- Business-to-business transacciones (B2B)
- Integraciones con los sistemas de planificación de recursos empresariales (ERP) y de gestión de relaciones con los clientes (CRM)

A continuación, se muestran algunos casos de uso habituales del uso de las aplicaciones web Transfer Family:

- Acceso simplificado a los datos de Amazon S3 para una gama más amplia y diversa de usuarios empresariales
- Administración centralizada del acceso a los datos para su fuerza laboral
- Visualización de las concesiones de acceso a Amazon S3 a través de una interfaz gestionada

Con Transfer Family, obtiene acceso a un servidor habilitado para el protocolo de transferencia de archivos AWS (o a una interfaz web de transferencia de archivos gestionada), sin necesidad de ejecutar ninguna infraestructura de servidor. Puede usar este servicio para migrar sus flujos de trabajo basados en la transferencia de archivos y, al AWS mismo tiempo, mantener los clientes y las configuraciones de sus usuarios finales tal como están. En el caso de los servidores, primero debe asociar el nombre de host al punto final del servidor, luego agregar los usuarios y proporcionarles el nivel de acceso adecuado. Una vez hecho esto, las solicitudes de transferencia de los usuarios se atenderán directamente desde el punto de conexión del servidor de Transfer Family.

En el caso de las aplicaciones web Transfer Family, determine los ajustes de configuración y aplique las personalizaciones opcionales. Una vez hecho esto, los usuarios pueden iniciar sesión y transferir datos directamente desde y hacia Amazon S3.

Transfer Family proporciona los siguientes beneficios:

- Un servicio completamente administrado que escala en tiempo real para satisfacer sus necesidades.
- No es necesario modificar sus aplicaciones ni mantener ninguna infraestructura de protocolo de transferencia de archivos.
- Con sus datos en un almacenamiento duradero de Amazon S3, puede utilizarlos de forma nativa Servicios de AWS para funciones de procesamiento, análisis, informes, auditoría y archivado.
- Con Amazon EFS como almacén de datos, obtiene un sistema de archivos elástico totalmente gestionado para utilizarlo con Nube de AWS servicios y recursos locales. Amazon EFS está diseñado para escalar a petabytes según la demanda sin interrumpir las aplicaciones, es decir, que aumenta y disminuye automáticamente a medida que se agregan o eliminan archivos. Esto ayuda a eliminar la necesidad de aprovisionar y administrar la capacidad para adaptarse al crecimiento.

- Un servicio de flujo de trabajo de transferencia de archivos sin servidor y totalmente administrado que facilita la configuración, ejecución, automatización y supervisión del procesamiento de archivos cargados mediante AWS Transfer Family.
- No hay costos iniciales, solo se paga por el uso del servicio.

En las siguientes secciones, encontrará una descripción de las diferentes características de Transfer Family, un tutorial de introducción, instrucciones detalladas sobre cómo configurar los distintos servidores con protocolos habilitados, cómo usar diferentes tipos de proveedores de identidad y la referencia de la API del servicio.

Para empezar a utilizar Transfer Family, consulte lo siguiente:

- [¿Cómo funciona AWS Transfer Family](#)
- [Requisitos previos](#)
- [Cómo empezar con los puntos de conexión de los AWS Transfer Family servidores](#)
- [Aplicaciones web Transfer Family](#)

¿Cómo funciona AWS Transfer Family

AWS Transfer Family es un AWS servicio totalmente gestionado que puede utilizar para transferir archivos desde y hacia el almacenamiento de Amazon Simple Storage Service (Amazon S3) o los sistemas de archivos Amazon Elastic File System (Amazon EFS) a través de los siguientes protocolos o navegadores web:

- Protocolo seguro de transferencia de archivos (SFTP): versión 3

El documento oficial del IETF está aquí: [SSH File Transfer Protocol draft-ietf-secsh-filexfer-02.txt](#).

- Protocolo seguro de File Transfer (FTPS)
- Protocolo de File Transfer (FTP)
- Declaración de aplicabilidad 2 (AS2)
- Browser-based transferencias

AWS Transfer Family admite hasta 3 zonas de disponibilidad y está respaldado por una flota redundante y con escalado automático para sus solicitudes de conexión y transferencia. Para ver un ejemplo sobre cómo crear una mayor redundancia y minimizar la latencia de la red mediante el

Latency-based enrutamiento, consulte la entrada del blog [Minimice la latencia de la red con la AWS transferencia para servidores SFTP](#).

Transfer Family Managed File Transfer Workflows (MFTW) es un servicio de flujo de trabajo de transferencia de archivos totalmente administrado y sin servidor que facilita la configuración, ejecución, automatización y supervisión del procesamiento de los archivos cargados mediante AWS Transfer Family. Los clientes pueden usar MFTW para automatizar varios pasos de procesamiento, como copiar, etiquetar, escanear compressing/decompressing, filtrar y encrypting/decrypting los datos que se transfieren mediante Transfer Family. Esto proporciona una visibilidad integral para el seguimiento y la auditabilidad. Para obtener más información, consulte [AWS Transfer Family flujos de trabajo gestionados](#).

AWS Transfer Family es compatible con cualquier cliente de protocolo de transferencia de archivos estándar. Algunos clientes de uso común son los siguientes:

- [OpenSSH](#): una utilidad de línea de comandos para Macintosh y Linux.
- [WinSCP](#): Windows-only un cliente gráfico.
- [Cyberduck](#): un cliente gráfico para Linux, Macintosh y Microsoft Windows.
- [FileZilla](#)— Un cliente gráfico para Linux, Macintosh y Windows.

AWS ofrece los siguientes talleres de Transfer Family.

- Cree una solución de transferencia de archivos que aproveche los SFTP/FTPS puntos de AWS Transfer Family conexión gestionados y Amazon Cognito y DynamoDB para la gestión de usuarios. Puede ver los detalles de este taller [aquí](#).
- [Cree un terminal Transfer Family con AS2 habilitado y un conector AS2 de Transfer Family. Puede ver los detalles de este taller aquí.](#)
- Cree una solución que proporcione orientación prescriptiva y un laboratorio práctico sobre cómo crear una arquitectura de transferencia de archivos segura y escalable AWS sin necesidad de modificar las aplicaciones existentes ni administrar la infraestructura de servidores. Puede ver los detalles de este taller [aquí](#).

Publicaciones de blog relevantes para Transfer Family

En la siguiente tabla se enumeran las entradas de blog que contienen información útil para los clientes de Transfer Family. La tabla está en orden cronológico inverso, de modo que las publicaciones más recientes se encuentran al principio de la tabla.

Título y enlace de la entrada del blog	Date
Implemente Okta como un proveedor de identidad personalizado para AWS Transfer Family	11 de agosto de 2025
Automatizar el procesamiento de reclamaciones de atención médica de papel a electrónico con AWS	29 de mayo de 2025
Cómo usar AWS Transfer Family y para protegerse contra el malware GuardDuty	30 de abril de 2025
Cómo FICO moderniza las transferencias de archivos con la automatización de ETL mediante AWS Transfer Family	24 de abril de 2025
Anunciamos aplicaciones AWS Transfer Family web para transferencias de archivos de Amazon S3 totalmente gestionadas	1 de diciembre de 2024
Seis consejos para mejorar la seguridad de su AWS Transfer Family servidor	24 de septiembre de 2024
Simplifique la autenticación de Active Directory con un proveedor de identidad personalizado para AWS Transfer Family	12 de agosto de 2024
Diseño transferencias de archivos gestionadas seguras y compatibles con conectores AWS Transfer Family SFTP y cifrado PGP	16 de mayo de 2024

Título y enlace de la entrada del blog	Date
Uso de Amazon Cognito como proveedor de identidad con Amazon AWS Transfer Family S3	14 de mayo de 2024
Cómo Transfer Family puede ayudarlo a crear una solución de transferencia de archivos gestionada segura y compatible	3 de enero de 2024
Detecte las amenazas de malware mediante AWS Transfer Family	20 de julio de 2023
Amplíe las cargas de trabajo de SAP con AWS Transfer Family	13 de julio de 2023
Cifre y descifre archivos con PGP y AWS Transfer Family	21 de junio de 2023
Autenticarse AWS Transfer Family con Azure Active Directory y AWS Lambda	15 de diciembre de 2022
Personalice las notificaciones de entrega de archivos mediante flujos de AWS Transfer Family trabajo administrados	14 de octubre de 2022
Building a cloud-native file transfer platform using AWS Transfer Family workflows	5 de enero de 2022
Habilitar la administración de claves de autoservicio de los usuarios con A AWS Transfer Family y AWS Lambda.	17 de diciembre de 2021
Mejore el control de acceso a AWS Transfer Family los datos con Amazon S3	5 de octubre de 2021
Mejore el rendimiento de las transferencias de archivos a través de Internet mediante el uso AWS Global Accelerator y los servicios AWS Transfer Family	7 de junio de 2021

Título y enlace de la entrada del blog	Date
Protección AWS Transfer Family con AWS Web Application Firewall y Amazon API Gateway	5 de mayo de 2021
Protección AWS Transfer Family con AWS Web Application Firewall y Amazon API Gateway	15 de enero de 2021
AWS Transfer Family soporte para Amazon Elastic File System	7 de enero de 2021
Habilite la autenticación por contraseña para su AWS Transfer Family uso AWS Secrets Manager	5 de noviembre de 2020
Centralice el acceso a los datos mediante AWS Transfer Family y AWS Storage Gateway	22 de junio de 2020
Uso de Amazon EFS AWS Lambda en sus aplicaciones sin servidor	18 de junio de 2020
Utilice la lista de direcciones IP permitidas para proteger sus servidores AWS Transfer Family	8 de abril de 2020
Minimice la latencia de la red con su AWS transferencia para servidores SFTP	19 de febrero de 2020
Impulse y modifique la migración de los servidores SFTP a AWS	12 de febrero de 2020
Simplifique su estructura de AWS SFTP con directorios lógicos y chroot	26 de septiembre de 2019
Uso de Okta como proveedor de identidad con AWS Transfer Family	30 de mayo de 2019

Requisitos previos

En las siguientes secciones se describen los requisitos previos necesarios para utilizar el servicio. AWS Transfer Family Como mínimo, debe crear un depósito de Amazon Simple Storage Service (Amazon S3) y proporcionar acceso a ese depósito a través de AWS Identity and Access Management una función (IAM). El rol también debe establecer una relación de confianza. Esa relación de confianza permite a Transfer Family asumir el rol de IAM y acceder al bucket, de modo que pueda atender las solicitudes de transferencia de archivos de los usuarios.

Para obtener información sobre el soporte de IPv6 para AWS Transfer Family servidores, consulte [Compatibilidad con IPv6 para servidores Transfer Family](#) el capítulo Administración de servidores.

Temas

- [AWS Regiones, puntos finales y cuotas compatibles con los servidores Transfer Family](#)
- [Inscríbete en AWS](#)
- [Configure el almacenamiento para usarlo con AWS Transfer Family los servidores](#)
- [Creación de una política y un rol de IAM](#)

AWS Regiones, puntos finales y cuotas compatibles con los servidores Transfer Family

Para conectarse mediante programación a un AWS servicio, se utiliza un punto final. Por ejemplo, el punto final para los clientes de la región EE.UU. Este (Ohio) (us-east-2) es. `transfer.us-east-2.amazonaws.com` Las cuotas de servicio, que también se denominan límites, establecen el número máximo de recursos u operaciones de servicio que puede haber en una cuenta de Cuenta de AWS. En esta guía, puedes encontrar las cuotas en [Cuotas de AS2](#) y [Cuotas para conectores SFTP](#).

Para obtener más información sobre AWS las regiones, los puntos finales y las cuotas de servicio compatibles, consulte los [AWS Transfer Family puntos finales y las cuotas](#) en. Referencia general de Amazon Web Services

En el caso de las aplicaciones web Transfer Family, las regiones compatibles aparecen en [Regiones de AWS para aplicaciones web Transfer Family](#). Para conocer las cuotas correspondientes a las aplicaciones web de Transfer Family, consulte [Cuotas de aplicaciones web](#).

Inscríbete en AWS

Cuando te registras en Amazon Web Services (AWS), tu AWS cuenta se registra automáticamente para todos los servicios de AWS, incluidos AWS Transfer Family. Solo se le cobrará por los servicios que utilice.

Si ya tienes una AWS cuenta, pasa a la siguiente tarea. Si no dispone de una cuenta de AWS, utilice el siguiente procedimiento para crear una.

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

Para suscribirse a una Cuenta de AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
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 una. 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](#).

Para obtener información sobre los precios y Calculadora de precios de AWS para obtener una estimación del costo de usar Transfer Family, consulta [AWS Transfer Family los precios](#).

Para obtener información sobre AWS la disponibilidad regional, consulta los [AWS Transfer Family puntos finales y las cuotas](#) en el Referencia general de AWS.

Configure el almacenamiento para usarlo con AWS Transfer Family los servidores

En este tema se describen las opciones de almacenamiento que puede utilizar con AWS Transfer Family. Puede utilizar Amazon S3 o Amazon EFS como almacenamiento para sus servidores Transfer Family.

Contenido

- [Configurar un bucket de Amazon S3](#)
 - [Puntos de acceso de Amazon S3](#)
 - [HeadObject Comportamiento de Amazon S3](#)
 - [Otorgue la capacidad de escribir y enumerar únicamente archivos](#)
 - [Gran cantidad de objetos de cero bits que provocan problemas de latencia](#)
- [Configuración de un sistema de archivos Amazon EFS](#)
 - [Propiedad de archivos de Amazon EFS](#)
 - [Configuración de los usuarios de Amazon EFS para Transfer Family](#)
 - [Configuración de los usuarios de Transfer Family en Amazon EFS](#)
 - [Creación de un usuario raíz de Amazon EFS](#)
 - [Comandos de Amazon EFS compatibles](#)

Configurar un bucket de Amazon S3

AWS Transfer Family accede a su bucket de Amazon S3 para atender las solicitudes de transferencia de sus usuarios, por lo que debe proporcionar un bucket de Amazon S3 como parte de la configuración de su servidor habilitado para el protocolo de transferencia de archivos. Puede usar un bucket existente o crear uno nuevo.

Note

No es necesario utilizar un servidor y un bucket de Amazon S3 que estén en la misma región de AWS , pero lo aconsejamos como práctica recomendada.

Al configurar los usuarios debe asignar a cada uno un rol de IAM. Este rol determina el nivel de acceso que tienen al bucket de Amazon S3.

Para obtener más información sobre la creación de un nuevo bucket, consulte la sección de [¿Como creo un bucket S3?](#) en la Guía del usuario de Amazon Simple Storage Service.

Note

Puede usar el bloqueo de objetos de Amazon S3 para evitar que se elimine o se sobrescriba un objeto durante un periodo de tiempo determinado o de manera indefinida. Esto funciona

de la misma manera con Transfer Family que con otros servicios. Si un objeto existe y está protegido, no se permite escribir en ese archivo ni eliminarlo. Para obtener más información acerca de Bloqueo de objetos en Amazon S3, consulte [Uso de Bloqueo de objetos en Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.

Puntos de acceso de Amazon S3

AWS Transfer Family es compatible con [los puntos de acceso Amazon S3](#), una función de Amazon S3 que le permite administrar fácilmente el acceso granular a los conjuntos de datos compartidos. Puede usar alias de punto de acceso de S3 en cualquier lugar donde utilice nombres de bucket de S3. Puede crear cientos de puntos de acceso en Amazon S3 para los usuarios que tienen diferentes permisos de acceso a los datos compartidos en un bucket de Amazon S3.

Por ejemplo, puede usar los puntos de acceso para permitir que tres equipos diferentes tengan acceso al mismo conjunto de datos compartido: un equipo puede leer los datos de S3, un segundo equipo puede escribir datos en S3 y el tercer equipo puede leer, escribir y eliminar datos de S3. Para implementar un control de acceso granular como el mencionado anteriormente, puede crear un punto de acceso S3 que contenga una política que dé acceso asimétrico a los diferentes equipos. Puede usar los puntos de acceso S3 con su servidor de Transfer Family para lograr un control de acceso detallado, sin necesidad de crear una política de bucket de S3 compleja que abarque cientos de casos de uso. Para obtener más información sobre cómo utilizar los puntos de acceso S3 con un servidor Transfer Family, consulte la entrada del blog [Enhance data access control with AWS Transfer Family Amazon S3](#).

Note

AWS Transfer Family actualmente no es compatible con los puntos de Multi-Region acceso Amazon S3.

HeadObject Comportamiento de Amazon S3

Note

Al crear o actualizar un servidor Transfer Family, puede optimizar el rendimiento de sus directorios de Amazon S3, lo que elimina las HeadObject llamadas.

En Amazon S3, los buckets y objetos son los principales recursos, y los objetos se almacenan en buckets. Amazon S3 puede imitar un sistema de archivos jerárquico, pero a veces puede comportarse de forma diferente a un sistema de archivos normal. Por ejemplo, los directorios no son un concepto de primera clase en Amazon S3, sino que se basan en claves de objetos. AWS Transfer Family deduce la ruta de un directorio dividiendo la clave de un objeto por la barra inclinada (/), tratando el último elemento como el nombre del archivo y, a continuación, agrupando los nombres de los archivos que tienen el mismo prefijo en la misma ruta. Zero-byte los objetos se crean para representar la ruta de una carpeta cuando se crea un directorio vacío con `mkdir` o mediante la consola Amazon S3. La clave de estos objetos termina en una barra diagonal al final. Estos objetos de cero bits se describen en [Organizar objetos en la consola de Amazon S3 mediante carpetas](#) de la Guía del usuario de Amazon S3.

Cuando ejecuta un `ls` comando y algunos resultados son objetos de cero bytes de Amazon S3 (estos objetos tienen claves que terminan en barra inclinada), Transfer Family emite una `HeadObject` solicitud para cada uno de estos objetos (consulte la referencia de [HeadObject](#) la API de Amazon Simple Storage Service para obtener más información). Esto puede provocar los siguientes problemas al utilizar Amazon S3 como almacenamiento con Transfer Family.

Otorgue la capacidad de escribir y enumerar únicamente archivos

En algunos casos, es posible que desee ofrecer únicamente acceso de escritura a sus objetos de Amazon S3. Por ejemplo, es posible que desee proporcionar acceso para escribir (o cargar) y enumerar objetos en un bucket, pero no para leer (descargar) objetos. Para ejecutar `ls mkdir` comandos mediante clientes de transferencia de archivos, debe tener Amazon S3 `ListObjects` y `PutObject` permisos. Sin embargo, cuando Transfer Family necesita realizar una `HeadObject` llamada para escribir o enumerar archivos, la llamada falla y aparece el error Acceso denegado, ya que esta llamada requiere el `GetObject` permiso.

 Note

Al crear o actualizar un servidor Transfer Family, puede optimizar el rendimiento de sus directorios de Amazon S3, lo que elimina las `HeadObject` llamadas.

En este caso, puede conceder el acceso añadiendo una condición de política AWS Identity and Access Management (IAM) que añada el `GetObject` permiso solo para los objetos que terminen en una barra diagonal (/). Esta condición impide `GetObject` las llamadas a los archivos (por lo que no se pueden leer), pero permite al usuario enumerar las carpetas y recorrerlas. El siguiente ejemplo de

política solo ofrece acceso de escritura y lista a sus buckets de Amazon S3. Para usar esta política, *amzn-s3-demo-bucket* sustitúyala por el nombre de tu bucket.

 Note

Para corregir el comportamiento de carga de WinSCP, asegúrate de añadir la "arn:aws:s3:::amzn-s3-demo-bucket/*.*filepart" línea tal y como se indica en el siguiente ejemplo de política. Esta línea garantiza el manejo correcto de los objetos .filepart para evitar errores.

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

```
    ]  
  }  
]  
}
```

Note

Esta política no permite a los usuarios añadir archivos. En otras palabras, un usuario al que se le asigne esta política no puede abrir archivos para añadirles contenido o modificarlos. Además, si su caso de uso requiere una llamada a `HeadObject` antes de cargar un archivo, esta política no le servirá.

Gran cantidad de objetos de cero bits que provocan problemas de latencia

Si sus buckets de Amazon S3 contienen una gran cantidad de estos objetos de cero bytes, Transfer Family emite muchas `HeadObject` llamadas, lo que puede provocar retrasos en el procesamiento. La solución recomendada para este problema es habilitar los directorios optimizados para reducir la latencia.

Por ejemplo, supongamos que va a su directorio principal y tiene 10 000 subdirectorios. En otras palabras, su bucket de Amazon S3 tiene 10 000 carpetas. En este escenario, si ejecuta el comando `ls` (`list`), la operación de lista tarda entre seis y ocho minutos. Sin embargo, si optimiza los directorios, esta operación solo tardará unos segundos. Esta opción se establece en la pantalla Configurar detalles adicionales durante el procedimiento de creación o actualización del servidor. Estos procedimientos se detallan en el [Configuración de un punto final de servidor SFTP, FTPS o FTP](#) tema.

Note

Los clientes GUI pueden emitir un `ls` comando fuera de su control, por lo que es importante que habilite esta configuración si es posible.

Si no optimiza o no puede optimizar sus directorios, una solución alternativa a este problema es eliminar todos los objetos de cero bytes. Tenga en cuenta lo siguiente:

- Los directorios vacíos dejarán de existir. Los directorios solo existen porque sus nombres están en la clave de un objeto.

- No impide que alguien vuelva a llamar `mkdir` y romper cosas una y otra vez. Puede mitigar esto mediante la elaboración de una política que impida la creación de directorios.
- Algunos escenarios utilizan estos objetos de 0 bits. Por ejemplo, tienes una estructura como `inboxes/customer1000` y el directorio de la bandeja de entrada se limpia todos los días.

Por último, otra posible solución es limitar el número de objetos visibles mediante una política que reduzca el número de `HeadObject` llamadas. Para que esta sea una solución viable, debe aceptar que solo podrá ver un conjunto limitado de todos sus subdirectorios.

Configuración de un sistema de archivos Amazon EFS

AWS Transfer Family accede a Amazon Elastic File System (Amazon EFS) para atender las solicitudes de transferencia de los usuarios. Por lo tanto, debe proporcionar un sistema de archivos Amazon EFS como parte de la configuración de su servidor habilitado para el protocolo de File Transfer. Puede usar un sistema de archivos existente o crear uno nuevo.

Tenga en cuenta lo siguiente:

- Si utiliza un servidor Transfer Family y un sistema de archivos Amazon EFS, el servidor y el sistema de archivos deben estar en el mismo lugar Región de AWS.
- No es necesario que el servidor y el sistema de archivos estén en la misma cuenta. Si el servidor y el sistema de archivos no están en la misma cuenta, la política del sistema de archivos debe conceder permisos explícitos al rol de usuario.

Para obtener información sobre cómo configurar varias cuentas, consulte [Administrar las AWS cuentas de su organización](#) en la Guía del AWS Organizations usuario.

- Al configurar los usuarios debe asignar a cada uno un rol de IAM. Este rol determina el nivel de acceso que tiene su sistema de archivos Amazon EFS.
- Para obtener más información sobre el montaje de un sistema de archivos Amazon EFS, consulte [Montaje de sistemas de archivos Amazon EFS](#).

Para obtener más información sobre cómo AWS Transfer Family funcionan juntos Amazon EFS, consulte [Using AWS Transfer Family to access files in your Amazon EFS file system](#) en la Guía del usuario de Amazon Elastic File System.

Propiedad de archivos de Amazon EFS

Amazon EFS utiliza el modelo de permisos de archivos de la Interfaz de sistema operativo portátil (POSIX) para representar la propiedad de los archivos.

En POSIX, los usuarios del sistema se clasifican en tres clases de permisos distintas: cuando permite a un usuario acceder a los archivos almacenados en un sistema de archivos Amazon EFS mediante AWS Transfer Family, debe asignarle un «perfil POSIX». Este perfil se utiliza para determinar su acceso a los archivos y directorios del sistema de archivos Amazon EFS.

- Usuario (u): propietario del archivo o directorio. Por lo general, el creador de un archivo o directorio también es el propietario.
- Grupo (g): conjunto de usuarios que necesitan un acceso idéntico a los archivos y directorios que comparten.
- Otros (o): todos los demás usuarios que tienen acceso al sistema, excepto el propietario y los miembros del grupo. Esta clase de permiso también se denomina “Pública”.

En el modelo de permisos POSIX, cada objeto del sistema de archivos (archivos, directorios, enlaces simbólicos, canales con nombre y conectores) está asociado a los tres conjuntos de permisos mencionados anteriormente. Los objetos de Amazon EFS tienen un Unix-style modo asociado. Este valor de modo define los permisos para realizar acciones en ese objeto.

Además, en los Unix-style sistemas, los usuarios y los grupos se asignan a identificadores numéricos, que Amazon EFS utiliza para representar la propiedad de los archivos. En el caso de Amazon EFS, los objetos pertenecen a un único propietario y a un único grupo. Amazon EFS usa estos ID numéricos para comprobar los permisos cuando un usuario intenta acceder a un objeto del sistema de archivos.

Configuración de los usuarios de Amazon EFS para Transfer Family

Antes de configurar los usuarios de Amazon EFS, puede realizar uno de los siguientes procedimientos:

- Puede crear usuarios y configurar sus carpetas de inicio en Amazon EFS. Para obtener más información, consulte [Configuración de los usuarios de Transfer Family en Amazon EFS](#).
- Si se siente cómodo añadiendo un usuario raíz, puede [Creación de un usuario raíz de Amazon EFS](#).

 Note

Los servidores de Transfer Family no admiten los puntos de acceso de Amazon EFS para establecer permisos POSIX. Los perfiles POSIX de los usuarios de Transfer Family (descritos en la sección anterior) ofrecen la posibilidad de establecer permisos POSIX. Estos permisos se establecen a nivel de usuario, para un acceso detallado, en función del UID, el GID y los GID secundarios.

Configuración de los usuarios de Transfer Family en Amazon EFS

Transfer Family asigna los usuarios a los directorios UID/GID y directorios que especifique. Si aún UID/GID/directories no existen en EFS, debe crearlos antes de asignarlos en Transfer a un usuario. Para obtener más información sobre como crear usuarios Amazon EFS, consulte [Trabajar con usuarios, grupos y permisos en el nivel del sistema de archivos de red \(NFS\)](#) en la Guía del usuario de Amazon Elastic File System.

Pasos para configurar los usuarios de Amazon EFS en Transfer Family

1. Asigne el UID y el GID de EFS para su usuario en Transfer Family mediante los campos [PosixProfile](#).
2. Si desea que el usuario comience en una carpeta específica al iniciar sesión, puede especificar el directorio EFS en el campo [HomeDirectory](#).

Puede automatizar el proceso mediante una CloudWatch regla y una función Lambda. Para ver un ejemplo de una función Lambda que interactúa con EFS, consulte Uso de [Amazon EFS para aplicaciones AWS Lambda sin servidor](#).

Además, puede configurar directorios lógicos para los usuarios de Transfer Family. Para obtener más información, consulte la sección [Configuración de directorios lógicos para Amazon EFS](#) del tema [Uso de directorios lógicos para simplificar las estructuras de directorios de Transfer Family](#).

Creación de un usuario raíz de Amazon EFS

Si a su organización le resulta cómodo habilitar el acceso de los usuarios raíz a través SFTP/FTPS de la configuración de sus usuarios, puede crear un usuario cuyo UID y GID sean 0 (usuario raíz) y, a continuación, utilizar ese usuario raíz para crear carpetas y asignar propietarios de ID POSIX al resto de los usuarios. La ventaja de esta opción es que no es necesario montar el sistema de archivos de Amazon EFS.

Siga los pasos descritos en [Añadir usuarios administrados por el servicio Amazon EFS](#) y, tanto para el ID de usuario como para el ID de grupo, introduzca 0 (cero).

 Tip

No permitas que esta cuenta de superusuario dure más tiempo del necesario. O bien, si conserva la cuenta de usuario raíz, asegúrese de mantenerla bien protegida.

Comandos de Amazon EFS compatibles

Los siguientes comandos son compatibles con Amazon EFS para AWS Transfer Family.

- `cd`
- `ls/dir`
- `pwd`
- `put`
- `get`
- `rename`
- `chown`: solo el usuario raíz (es decir, los usuarios con `uid=0`) puede cambiar la propiedad y los permisos de los archivos y directorios.
- `chmod`: solo el usuario raíz puede cambiar la propiedad y los permisos de los archivos y directorios.
- `chgrp`: se admite tanto para el usuario raíz como para el propietario del archivo, que solo puede cambiar el grupo de un archivo para convertirlo en uno de sus grupos secundarios.
- `ln -s/symlink`
- `mkdir`
- `rm/delete`
- `rmdir`
- `chmtime`

Creación de una política y un rol de IAM

En este tema se describen los tipos de políticas y roles con AWS Transfer Family los que se puede utilizar y se explica el proceso de creación de un rol de usuario. También describe cómo funcionan las políticas de sesión y proporciona un ejemplo de rol de usuario.

AWS Transfer Family utiliza los siguientes tipos de funciones:

- **Función de usuario:** permite a los usuarios gestionados por el servicio acceder a los recursos de Transfer Family necesarios. AWS Transfer Family asume esta función en el contexto de un ARN de usuario de Transfer Family.
- **Rol de acceso:** proporciona acceso únicamente a los archivos de Amazon S3 que se están transfiriendo. Para las transferencias AS2 entrantes, el rol de acceso utiliza el nombre de recurso de Amazon (ARN) para el acuerdo. Para las transferencias AS2 salientes, el rol de acceso utiliza el ARN para el conector.
- **Rol de invocación:** para usar con Amazon API Gateway como proveedor de identidad personalizado del servidor. Transfer Family asume este rol en el contexto de un ARN de servidor de Transfer Family.
- **Función de registro:** se utiliza para registrar entradas en Amazon CloudWatch. Transfer Family utiliza este rol para registrar los detalles de éxito y error junto con la información sobre las transferencias de archivos. Transfer Family asume este rol en el contexto de un ARN de servidor de Transfer Family. Para las transferencias AS2 salientes, el rol de acceso utiliza el ARN del conector.
- **Rol de ejecución:** permite a un usuario de Transfer Family llamar e iniciar flujos de trabajo. Transfer Family asume este rol en el contexto de un ARN de flujo de trabajo de Transfer Family.

Además de estos roles, también puede utilizar políticas de sesión. Se utiliza una política de sesión para limitar el acceso cuando es necesario. Tenga en cuenta que estas políticas son independientes, es decir, no se agregan a un rol. Más bien, se agrega una política de sesión directamente a un usuario de Transfer Family.

Note

Al crear un usuario de Transfer Family gestionado por un servicio, puede seleccionar la Auto-generate política en función de la carpeta de inicio. Se trata de un atajo útil si desea limitar el acceso de los usuarios a sus propias carpetas. Además, puede ver detalles sobre

las políticas de sesión y un ejemplo en [Funcionamiento de las políticas de sesión](#). También puede encontrar más información sobre las políticas de sesión en las [políticas de sesión](#) de la Guía del usuario de IAM.

Temas

- [Creación de un rol de usuario](#)
- [Funcionamiento de las políticas de sesión](#)
- [Ejemplo de política de read/write acceso](#)

Creación de un rol de usuario

Al crear un usuario, debe tomar algunas decisiones sobre su nivel de acceso. Estas decisiones incluyen a qué buckets de Amazon S3 o sistemas de archivos de Amazon EFS puede acceder el usuario, a qué partes de cada bucket de Amazon S3 y a qué archivos del sistema de archivos se puede acceder, y qué permisos tiene el usuario (por ejemplo, PUT o GET).

Para configurar el acceso, debe crear una política y un rol basados en la identidad AWS Identity and Access Management (IAM) que proporcionen esa información de acceso. Como parte de este procedimiento, debe proporcionar al usuario acceso al bucket Amazon S3 o al sistema de archivos de Amazon EFS que es el destino o la fuente de las operaciones de archivos. Para ello, deberá seguir estos pasos de alto nivel, que se describen con más detalle más adelante:

Creación de un rol de usuario

1. Cree una política de IAM para AWS Transfer Family. Esto se describe en [Para crear una política de IAM para AWS Transfer Family](#).
2. Cree un rol de IAM y adjunte la nueva política de IAM. Para ver un ejemplo, consulta [Ejemplo de política de read/write acceso](#).
3. Establezca una relación de confianza entre AWS Transfer Family y la función de IAM. Esto se describe en [Para establecer una relación de confianza](#).

Los siguientes procedimientos describen cómo crear una política y un rol de IAM.

Para crear una política de IAM para AWS Transfer Family

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.

2. En el panel de navegación, seleccione Políticas y, a continuación, Crear política.
3. En la página Create Policy (Crear política), elija la pestaña JSON.
4. En el editor que aparece, sustituya el contenido del editor por la política de IAM que desee asociar al rol de IAM.

Puede conceder read/write acceso o restringir el acceso de los usuarios a su directorio principal. Para obtener más información, consulte [Ejemplo de política de read/write acceso](#).

5. Elija Revisar política, indique un nombre y una descripción para la política y, a continuación, elija Crear política.

A continuación, cree un rol de IAM y asócielo la nueva política de IAM.

Para crear un rol de IAM para AWS Transfer Family

1. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.

En la página Crear rol, asegúrese de que servicio de AWS está seleccionado.
2. Elija Transfer (Transferencia) en la lista de servicios y, a continuación, elija Next: Permissions (Siguiendo: Permisos). Esto establece una relación de confianza entre AWS Transfer Family y AWS.
3. En la sección Asociar políticas de permisos, busque y elija la política que acaba de crear y, a continuación, elija Siguiendo: Etiquetas.
4. (Opcional) Introduzca una clave y un valor de etiqueta y seleccione Siguiendo: Revisión.
5. En la página Review (Revisión), escriba un nombre y una descripción para el nuevo rol y, a continuación, elija Create role (Crear rol).

Luego, establece una relación de confianza entre AWS Transfer Family y AWS.

Para establecer una relación de confianza

Note

En nuestros ejemplos, utilizamos tanto `ArnLike` como `ArnEquals`. Funcionalmente son idénticos y, por lo tanto, puede utilizar cualquiera de los dos al crear sus políticas. La documentación de Transfer Family utiliza `ArnLike` cuando la condición contiene un carácter comodín, y utiliza `ArnEquals` para indicar una condición de coincidencia exacta.

1. En la consola de IAM, elija el rol que acaba de crear.
2. En la página Summary (Resumen), elija Trust relationships (Relaciones de confianza) y, a continuación, elija Edit trust relationship (Editar relación de confianza)
3. En el editor Edit Trust Relationship, asegúrese de que el servicio sea "transfer.amazonaws.com". La política de acceso se muestra a continuación.

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

Le recomendamos que utilice las claves de condición `aws:SourceAccount` y `aws:SourceArn` para protegerse contra el problema del suplente confuso. La cuenta de origen es la propietaria del servidor y el ARN de origen es el ARN del usuario. Por ejemplo:

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

También puede usar la condición `ArnLike` si desea restringirlo a un servidor en particular en lugar de a cualquier servidor de la cuenta de usuario. Por ejemplo:

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

```
}  
}
```

Note

En los ejemplos anteriores, sustituya cada uno *user input placeholder* por su propia información.

Para obtener más información sobre el confuso problema del diputado y otros ejemplos, consulte [Cross-service confusa prevención de diputados](#).

4. Elija Actualizar política de confianza para actualizar la política de acceso.

Ahora ha creado un rol de IAM que le permite llamar AWS Transfer Family a AWS los servicios en su nombre. También ha asociado al rol la política de IAM que ha creado para permitir el acceso a su usuario. En la sección [Cómo empezar con los puntos de conexión de los AWS Transfer Family servidores](#) se asignan este rol y esta política al usuario o usuarios.

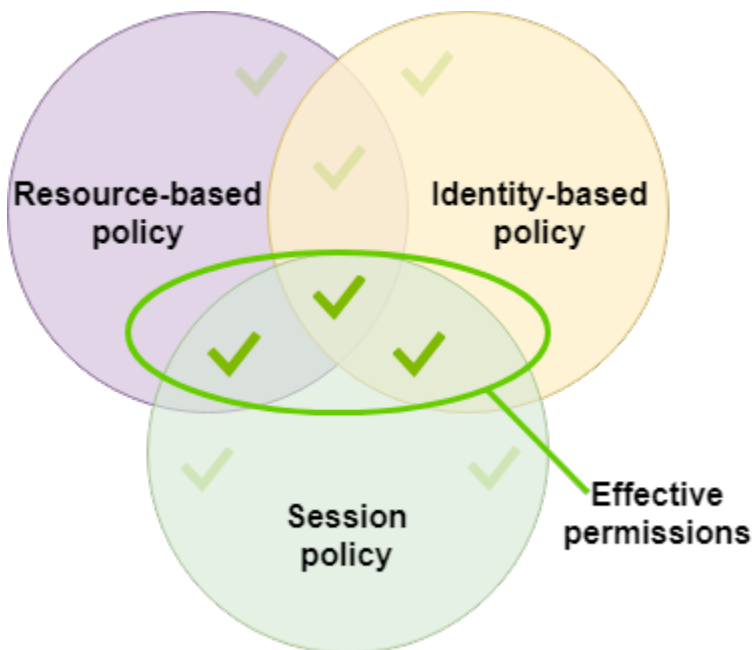
Véase también

- Para obtener más información general sobre las funciones de IAM, consulte [Crear una función para delegar permisos a un AWS servicio](#) en la Guía del usuario de IAM.
- Para obtener más información acerca de las políticas basadas en identidades para los recursos de Amazon S3, consulte [Identity and Access Management en Amazon S3](#) en la Guía del usuario de Amazon Simple Storage Service.
- Para obtener más información sobre las políticas basadas en la identidad para los recursos de Amazon EFS, consulte [Uso de IAM para controlar el acceso a los datos del sistema de archivos](#) en la Guía del usuario de Amazon Elastic File System.

Funcionamiento de las políticas de sesión

Cuando un administrador crea un rol, este suele incluir amplios permisos para abarcar varios casos de uso o miembros del equipo. Si un administrador configura la [URL de una consola](#), puede reducir los permisos de la sesión resultante mediante una política de sesión. Por ejemplo, si crea un rol con [read/write acceso](#), puede configurar una URL que limite el acceso de los usuarios únicamente a sus directorios principales.

Las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o usuario. Las políticas de sesión son útiles para bloquear a los usuarios, de modo que solo tengan acceso a las partes del bucket en las que los prefijos de los objetos contengan su nombre de usuario. Los siguientes permisos de la sesión son la intersección de las políticas de sesión y las políticas basadas en recursos más la intersección de las políticas de sesión y las políticas basadas en identidades.



Para obtener más detalles, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

En AWS Transfer Family, solo se admite una política de sesión cuando realiza una transferencia hacia o desde Amazon S3. El ejemplo de política siguiente es una política de ámbito reducido que limita el acceso de los usuarios a sus directorios home. Tenga en cuenta lo siguiente:

- Los estados de cuenta `GetObjectACL` y `PutObjectACL` solo son obligatorios si necesitas habilitar el acceso entre cuentas. Es decir, el servidor de Transfer Family necesita acceder a un bucket de otra cuenta.
- La longitud máxima de una ruta es 2048 caracteres. Para obtener más información, consulte el [Parámetro de solicitud de política](#) correspondiente a la acción de `CreateUser` en la Referencia de la API.
- Si su bucket de Amazon S3 está cifrado con AWS Key Management Service (AWS KMS), debe especificar permisos adicionales en su política. Para obtener más información, consulte [Protección y cifrado de datos](#).

- Si desea utilizar las políticas de sesión para crear permisos de acceso basados en los atributos del usuario sin crear funciones de IAM independientes para cada usuario, consulte [Enfoques de gestión dinámica de permisos](#).

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

 Note

En el ejemplo de política anterior se supone que los directorios principales de los usuarios están configurados para incluir una barra al final, lo que significa que se trata de un directorio. Si, por el contrario, establece el HomeDirectory de un usuario sin la barra final, debe incluirlo como parte de su política.

En el ejemplo anterior de política, anote el uso de los parámetros de la política `transfer:HomeFolder`, `transfer:HomeBucket` y `transfer:HomeDirectory`. Estos parámetros se establecen para el HomeDirectory que está configurado para el usuario, tal y como se describe en [HomeDirectoryyImplementación de su método de API Gateway](#). Estos parámetros tienen las siguientes definiciones:

- El parámetro `transfer:HomeBucket` se sustituye por el primer componente de HomeDirectory.
- El parámetro `transfer:HomeFolder` se sustituye por las partes restantes del parámetro HomeDirectory.
- Se ha eliminado la barra inclinada inicial (/) del parámetro `transfer:HomeDirectory` para que pueda usarse como parte de un nombre de recurso de Amazon (ARN) de S3 en una declaración de Resource.

 Note

Si utiliza directorios lógicos, es decir, el `homeDirectoryType` del usuario es LOGICAL, estos parámetros de política (HomeBucket, HomeDirectory y HomeFolder) no son compatibles.

Por ejemplo, supongamos que el parámetro HomeDirectory que está configurado para el usuario de Transfer Family es `/home/bob/amazon/stuff/`.

- `transfer:HomeBucket` toma el valor de `/home`.
- `transfer:HomeFolder` toma el valor de `/bob/amazon/stuff/`.
- `transfer:HomeDirectory` se convierte en `home/bob/amazon/stuff/`.

El primer "Sid" permite al usuario enumerar todos los directorios a partir de `/home/bob/amazon/stuff/`.

El segundo "Sid" limita los accesos del usuario put y get a la misma ruta, `/home/bob/amazon/stuff/`.

Ejemplo de política de read/write acceso

Conceder read/write acceso al bucket de Amazon S3

El siguiente ejemplo de política AWS Transfer Family permite el read/write acceso a los objetos de su bucket de Amazon S3.

Tenga en cuenta lo siguiente:

- Reemplace `amzn-s3-demo-bucket` con el nombre de su bucket de Amazon S3.
- Los estados de cuenta `GetObjectACL` y `PutObjectACL` solo son obligatorios si necesitas habilitar el acceso entre cuentas. Es decir, el servidor de Transfer Family necesita acceder a un bucket de otra cuenta.
- Las instrucciones `GetObjectVersion` y `DeleteObjectVersion` solo son obligatorias si el control de versiones está habilitado en el bucket de Amazon S3 al que se está accediendo.

Note

Si alguna vez ha activado el control de versiones para su bucket, necesitará estos permisos, ya que solo puede suspender el control de versiones en Amazon S3 y no desactivarlo por completo. Para obtener más información, consulte Buckets [sin control de versiones](#), [con control de versiones activado](#) y [con control de versiones suspendido](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ]
    }
  ]
}
```



```

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

```

Otorgue acceso al sistema de archivos a los archivos del sistema de archivos Amazon EFS

Note

Además de la política, también debe asegurarse de que los permisos de sus archivos POSIX concedan el acceso adecuado. Para obtener más información, consulte [Trabajar con usuarios, grupos y permisos en el nivel del sistema de archivos de red \(NFS\)](#) en la Guía del usuario de Amazon Elastic File System.

El siguiente ejemplo de política otorga acceso al sistema de archivos raíz a los archivos de su sistema de archivos Amazon EFS.

 Note

En los ejemplos siguientes, *region* sustitúyalo por tu región, *account-id* por la cuenta en la que se encuentra el archivo y *file-system-id* por el ID de tu Amazon Elastic File System (Amazon EFS).

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

El siguiente ejemplo de política otorga al sistema de archivos del usuario acceso a los archivos de su sistema de archivos de Amazon EFS.

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Tutoriales de Transfer Family

La guía AWS Transfer Family del usuario proporciona tutoriales detallados para varios casos de uso.

- [Cómo empezar con los puntos de conexión de los AWS Transfer Family servidores](#)- Cree un servidor SFTP Transfer Family con un usuario gestionado por el servicio y transfiera los archivos mediante un cliente.
- [Configuración y uso de conectores SFTP](#)- Configure un conector SFTP para transferir archivos entre el almacenamiento de Amazon S3 y un servidor SFTP.
- [Configuración de un método de Amazon API Gateway como proveedor de identidad personalizado](#)- Configure un método Amazon API Gateway como proveedor de identidad personalizado para cargar archivos a un AWS Transfer Family servidor.
- [Configuración de un flujo de trabajo gestionado para descifrar un archivo](#)- Cree un flujo de trabajo gestionado para descifrar archivos, cargar archivos cifrados en Amazon S3 y ver el contenido descifrado.
- [Configuración de una configuración AS2](#)- Configure un servidor AS2 Transfer Family, que incluya la importación de certificados, la creación de perfiles y acuerdos, la configuración del conector AS2 opcional y las pruebas.
- Los siguientes tutoriales le guiarán a través de la creación y configuración de aplicaciones web de Transfer Family. Elija el tutorial que mejor se adapte a sus necesidades:

[Tutorial: Cómo configurar una aplicación web básica de Transfer Family](#)- Aprenda a crear y configurar una aplicación web Transfer Family.

[Tutorial: Configuración de una aplicación AWS Transfer Family web con acceso selectivo a varios cubos](#)- Configure una aplicación web Transfer Family con permisos granulares de bucket de Amazon S3 para un solo usuario.

Temas

- [Cómo empezar con los puntos de conexión de los AWS Transfer Family servidores](#)
- [Configuración de un flujo de trabajo gestionado para descifrar un archivo](#)
- [Configuración y uso de conectores SFTP](#)
- [Configuración de un método de Amazon API Gateway como proveedor de identidad personalizado](#)
- [Configuración de una configuración AS2](#)

- [Tutorial: Cómo configurar una aplicación web básica de Transfer Family](#)
- [Tutorial: Configuración de una aplicación AWS Transfer Family web con acceso selectivo a varios cubos](#)

Cómo empezar con los puntos de conexión de los AWS Transfer Family servidores

Usa este tutorial para empezar con AWS Transfer Family (Transfer Family). Aprenderás a crear un SFTP-enabled servidor con punto final de acceso público mediante el almacenamiento de Amazon S3, a añadir un usuario con autenticación gestionada por el servicio y a transferir un archivo con Cyberduck.

Temas

- [Requisitos previos](#)
- [Paso 1: Inicia sesión en la consola AWS Transfer Family](#)
- [Paso 2: Crea un SFTP-enabled servidor](#)
- [Paso 3: agregar un usuario de servicio administradas](#)
- [Paso 4: transferencia de un archivo mediante un cliente](#)

Requisitos previos

Antes de comenzar, asegúrese de completar los requisitos que se detallan en [Requisitos previos](#). Como parte de esta configuración, se crea un bucket de Amazon Simple Storage Service (Amazon S3) y AWS Identity and Access Management un rol de usuario (IAM).

Se requieren permisos para usar la AWS Transfer Family consola y hay permisos necesarios para configurar otros AWS servicios que utiliza Transfer Family, como Amazon Simple Storage Service AWS Certificate Manager, Amazon Elastic File System y Amazon Route 53. Por ejemplo, a los usuarios que transfieren archivos dentro y fuera de AWS Transfer Family, les AmazonS3FullAccess otorga permisos para configurar y usar un bucket de Amazon S3. Algunos de los permisos de esta política son necesarios para crear buckets de Amazon S3.

Para utilizar la consola Transfer Family, necesita lo siguiente:

- AWSTransferConsoleFullAccess concede permisos a su usuario de SFTP para crear recursos de Transfer Family.

- IAMFullAccess(o específicamente una política que permita la creación de funciones de IAM) solo es necesaria si quieres que Transfer Family cree automáticamente una función de registro para tu servidor en Amazon CloudWatch Logs o una función de usuario para un usuario que inicie sesión en un servidor.
- Para crear y eliminar tipos de servidores de VPC, debe agregar las acciones ec2: CreateVpcEndpoint y ec2: DeleteVpcEndpoints a su política. Para obtener información sobre cómo limitar el acceso a los puntos de conexión de la VPC por motivos de seguridad, consulte. [Limitar el acceso a los terminales de VPC para los servidores Transfer Family](#)

Note

Las IAMFullAccesspolíticas AmazonS3FullAccessy, en sí mismas, no son necesarias para el uso general de. AWS Transfer Family Se presentan aquí como una forma sencilla de asegurarse de que están cubiertos todos los permisos que necesita. Además, se trata de políticas AWS administradas, que son políticas estándar que están disponibles para todos los clientes de AWS . Puede ver los permisos individuales de estas políticas y determinar el conjunto mínimo que necesita para sus fines.

Paso 1: Inicia sesión en la consola AWS Transfer Family

Inicio de sesión en Transfer Family

1. Inicie sesión en Consola de administración de AWS y abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. Para el seudónimo o el seudónimo de la cuenta, introduzca el identificador de su cuenta Cuenta de AWS.
3. En nombre de usuario de IAM, escriba el nombre del rol de usuario que ha creado para Transfer Family.
4. En Contraseña, introduce la contraseña AWS de tu cuenta.
5. Seleccione Iniciar sesión.

Paso 2: Crea un SFTP-enabled servidor

El protocolo de File Transfer (SFTP) Secure Shell (SSH) es un protocolo de red que se utiliza para la transferencia segura de datos a través de Internet. El protocolo es compatible con todas las funciones de seguridad y autenticación de SSH. Se utiliza ampliamente para intercambiar datos, incluida información confidencial, entre socios comerciales de diversos sectores, como los servicios financieros, la sanidad, el comercio minorista y la publicidad.

Para crear un servidor SFTP-enabled

1. Seleccione Servidores en el panel de navegación y, a continuación, elija Crear servidor.
2. En Elegir protocolos, seleccione SFTP y, a continuación, Siguiente.
3. En Elegir un proveedor de identidad, seleccione Administrado por el servicio para almacenar las identidades y claves de los usuarios en Transfer Family y, a continuación, seleccione Siguiente.
4. En Elegir punto de conexión, haga lo siguiente:
 - a. En el tipo de punto de conexión, seleccione el tipo de punto de conexión de acceso público.
 - b. En Nombre de host personalizado, elija Ninguno.
 - c. Elija Siguiente.
5. En Elegir un dominio, seleccione Amazon S3.
6. En Configurar detalles adicionales, en Opciones de algoritmos criptográficos, elija una política de seguridad que contenga los algoritmos criptográficos habilitados para su uso en el servidor. Nuestra política de seguridad más reciente es la predeterminada: para obtener más información, consulte. [Políticas de seguridad para AWS Transfer Family servidores](#)

Note

Solo si va a añadir un flujo de trabajo gestionado para su servidor, elija Crear un nuevo rol para el CloudWatchregistro. Para registrar los eventos del servidor, no es necesario crear un rol de IAM.

7. En Revisar y crear, elija Crear servidor. Se le redirigirá a la página Servidores.

Pueden transcurrir algunos minutos antes de que el estado del nuevo servidor cambie a Online. En ese momento, el servidor podrá realizar operaciones con los archivos, pero primero tendrá que crear

un usuario. Para obtener más información sobre la creación de usuarios, consulte [Administración de usuarios para puntos finales de servidor](#).

Paso 3: agregar un usuario de servicio administradas

Para añadir un usuario al SFTP-enabled servidor

1. En la página Servidores, seleccione el servidor al que desee añadir un usuario.
2. Seleccione Agregar usuario.
3. En la sección Configuración de usuario, en Nombre de usuario, introduzca el nombre de usuario. Este nombre de usuario debe tener un mínimo de 3 y un máximo de 100 caracteres. Puede utilizar los siguientes caracteres en el nombre de usuario: a—z, 0—9 A-Z, guión bajo '_', guión '-', punto '.' y signo '@'. El nombre de usuario no puede empezar con un guión '-', punto '.' o con el signo '@'.
4. En Access, elige el rol de IAM en el que lo creaste. [Creación de una política y un rol de IAM](#) Esta función de IAM incluye una política de IAM que contiene permisos para acceder a su bucket de Amazon S3, así como una relación de confianza con el AWS Transfer Family servicio. El procedimiento descrito en esta sección [Para establecer una relación de confianza](#) muestra cómo establecer la relación de confianza adecuada.
5. En Política, elija Ninguno.
6. En el directorio principal, elige el depósito de Amazon S3 en el que quieres almacenar los datos que transfieres mediante AWS Transfer Family. Introduzca la ruta al home directorio. Este es el directorio que ven los usuarios cuando inician sesión con su cliente.

Recomendamos usar una ruta de directorio que contenga el nombre de usuario para que tenga la opción de usar una política de sesión. Una política de sesión limita el acceso de un usuario al bucket de Amazon S3 al home directorio de ese usuario. Para obtener más información sobre el uso de las políticas de sesión, consulte [Funcionamiento de las políticas de sesión](#).

Si lo prefieres, puedes dejar este parámetro en blanco para usar el root directorio de tu bucket de Amazon S3. Si eliges esta opción, asegúrate de que tu rol de IAM proporciona acceso al root directorio.

7. Seleccione la casilla de verificación Restringido para impedir que los usuarios accedan a cualquier elemento ajeno a su home directorio. Esto también impide que los usuarios vean el nombre del bucket de Amazon S3 o el nombre de la carpeta.

8. Para la clave pública SSH, introduzca la parte de clave SSH pública del par de claves SSH en formato. `ssh-rsa <string>`

El servicio debe validar tu clave antes de que puedas añadir tu nuevo usuario. Para obtener más información acerca de cómo generar un key pair de claves SSH, consulte [Genere claves SSH para los usuarios administrados por el servicio](#).

9. (Opcional) En Clave y Valor, escriba una o varias etiquetas como pares clave-valor y seleccione Agregar etiqueta.
10. Seleccione Add (Añadir) para agregar el nuevo usuario al servidor que haya elegido.

El nuevo usuario aparecerá en la sección Usuarios de la página Detalles del servidor.

Paso 4: transferencia de un archivo mediante un cliente

Los archivos se transfieren a través del AWS Transfer Family servicio especificando la operación de transferencia en un cliente. AWS Transfer Family admite varios clientes. Para obtener más información, consulte [Transferencia de archivos a través de un punto de conexión mediante un cliente](#)

Esta sección contiene procedimientos para usar Cyberduck y OpenSSH.

Temas

- [Uso de Cyberduck](#)
- [Uso de OpenSSH](#)

Uso de Cyberduck

Para transferir archivos AWS Transfer Family mediante Cyberduck

1. Abra el cliente de [Cyberduck](#).
2. Elija Abrir conexión.
3. En el cuadro de diálogo Abrir conexión, elija SFTP (Protocolo de File Transfer SSH).
4. En Servidor, escriba el punto de conexión del servidor. El punto de conexión del servidor se encuentra en la página de detalles del servidor, consulte [Vea los detalles de los servidores SFTP, FTPS y FTP](#).
5. Para el número de puerto, introduzca **22** para SFTP.

6. En Usuario, escriba el nombre del usuario que creó en [Administración de usuarios para puntos finales de servidor](#).
7. En Clave privada de SSH, elija o introduzca la clave privada de SSH.
8. Elija Conectar.
9. Ejecute la transferencia de archivos.

En función del lugar donde se encuentren los archivos, elija entre las acciones siguientes:

- En el directorio local (el origen), seleccione los archivos que desea transferir, arrástrelos y suéltelos en el directorio de Amazon S3 (el destino).
- En el directorio de Amazon S3 (el origen), seleccione los archivos que desea transferir, arrástrelos y suéltelos en el directorio local (el destino).

Uso de OpenSSH

Siga las instrucciones indicadas a continuación para transferir archivos desde la línea de comandos mediante OpenSSH.

Note

Este cliente solo funciona con un SFTP-enabled servidor.

Para transferir archivos AWS Transfer Family mediante la utilidad de línea de comandos OpenSSH

1. En Linux o Macintosh, abra un terminal de comandos.
2. En el símbolo del sistema, escriba el comando siguiente: `% sftp -i transfer-key sftp_user@service_endpoint`

En el comando anterior, `sftp_user` es el nombre de usuario y `transfer-key` es la clave privada de SSH. Aquí `service_endpoint` está el punto final del servidor, tal y como se muestra en la AWS Transfer Family consola del servidor seleccionado.

Debe aparecer el símbolo del sistema `sftp`.

3. (Opcional) Para ver el directorio de inicio del usuario, introduzca el siguiente comando en la línea de comandos `sftp`: `sftp> pwd`

4. En la línea siguiente, escriba este texto: `sftp> cd /amzn-s3-demo-bucket/home/sftp_user`

En este ejercicio introductorio, este es el bucket de Amazon S3 al que se transfieren los archivos.

5. En la línea siguiente, escriba este comando: `sftp> put filename.txt`

El comando `put` transfiere el archivo al bucket de Amazon S3.

Aparecerá un mensaje similar al siguiente para indicar que la transferencia está en curso o que se ha completado.

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

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

Configuración de un flujo de trabajo gestionado para descifrar un archivo

En este tutorial se muestra cómo configurar un flujo de trabajo administrado que contenga un paso de descifrado. El tutorial también muestra cómo cargar un archivo cifrado en un bucket de Amazon S3 y, a continuación, ver el archivo descifrado en ese mismo bucket.

Note

El blog sobre AWS almacenamiento tiene una entrada que describe cómo descifrar archivos de forma sencilla sin escribir ningún código mediante los flujos de trabajo gestionados por Transfer Family, [cifrar y descifrar archivos con PGP](#) y. AWS Transfer Family

Temas

- [Paso 1: creación y configuración de un rol de ejecución de IAM](#)
- [Paso 2: creación de un flujo de trabajo administrado](#)
- [Paso 3: agregar el flujo de trabajo a un servidor y crear un usuario](#)
- [Paso 4: creación de un par de claves PGP](#)
- [Paso 5: Guarde la clave privada PGP en AWS Secrets Manager](#)

- [Paso 6: cifrado de un archivo](#)
- [Paso 7: ejecución del flujo de trabajo y visualización de los resultados](#)

Paso 1: creación y configuración de un rol de ejecución de IAM

Cree una función de ejecución AWS Identity and Access Management (IAM) que Transfer Family pueda utilizar para iniciar un flujo de trabajo. El proceso de creación de un rol de ejecución se describe en [Políticas de IAM para flujos de trabajo](#).

Note

Como parte de la creación de un rol de ejecución, asegúrese de establecer una relación de confianza entre el rol de ejecución y Transfer Family, tal y como se describe en [Para establecer una relación de confianza](#).

La siguiente política de roles de ejecución contiene todos los permisos necesarios para iniciar el flujo de trabajo que cree en este tutorial. Para utilizar esta política de ejemplo, sustituya *user input placeholders* por su propia información. `amzn-s3-demo-bucket` Sustitúyalo por el nombre del depósito de Amazon S3 en el que carga los archivos cifrados.

Note

No todos los flujos de trabajo requieren todos los permisos que se enumeran en este ejemplo. Puede restringir los permisos en función de los tipos de pasos de su flujo de trabajo específico. Los permisos necesarios para cada tipo de paso predefinido se describen en [Utilice pasos predefinidos](#). Los permisos necesarios para un paso personalizado se describen en [Permisos de IAM para un paso personalizado](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkflowsS3Permissions",
      "Effect": "Allow",
      "Action": [
```

```

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

```

Paso 2: creación de un flujo de trabajo administrado

Ahora necesita crear un flujo de trabajo que contenga un paso de descifrado.

Creación de un flujo de trabajo que contenga un paso de descifrado

1. Abre la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Flujos de trabajo y, a continuación, Crear flujo de trabajo.
3. Escriba la información siguiente:
 - Introduzca una descripción, por ejemplo, **Decrypt workflow example**.
 - En la sección Pasos nominales, seleccione Añadir paso.

4. En Elegir el tipo de paso, elija Descifrar archivo y, a continuación, elija Siguiente.
5. En el cuadro de diálogo Configurar parámetros, especifique lo siguiente:
 - Introduzca un nombre de paso descriptivo, por ejemplo, **decrypt-step**. No se permiten espacios en los nombres de los pasos.
 - Para el Destino de los archivos descifrados, elija Amazon S3.
 - Para el nombre del bucket de destino, elija el mismo bucket de Amazon S3 que especificó como `amzn-s3-demo-bucket` en la política de IAM que creó en el paso 1.
 - Para el prefijo de clave de destino, introduzca el nombre del prefijo (carpeta) en el que desee almacenar los archivos descifrados en el bucket de destino, por ejemplo, **decrypted-files/**.

 Note

Asegúrese de añadir una barra (/) final al prefijo.

- Para este tutorial, deja desactivada la opción Sobrescribir existente. Si se borra esta configuración, si intenta descifrar un archivo con el mismo nombre que un archivo existente, el procesamiento del flujo de trabajo se detiene y el nuevo archivo no se procesa.

Elija Siguiente para pasar a la pantalla de revisión.

6. Revise los detalles del paso. Si todo es correcto, seleccione Crear paso.
7. Su flujo de trabajo solo necesita un único paso de descifrado, por lo que no es necesario configurar ningún paso adicional. Seleccione Crear flujo de trabajo para crear el nuevo flujo de trabajo.

Anote el ID de flujo de trabajo del nuevo flujo de trabajo. Necesitará este ID en el siguiente paso. En este tutorial se utiliza *w-1234abcd5678efghi* como ejemplo el ID del flujo de trabajo.

Paso 3: agregar el flujo de trabajo a un servidor y crear un usuario

Ahora que tiene un flujo de trabajo con un paso de descifrado, debe asociarlo a un servidor de Transfer Family. En este tutorial se muestra cómo adjuntar el flujo de trabajo a un servidor de Transfer Family existente. Si lo desea, puede crear un nuevo servidor para usarlo con su flujo de trabajo.

Tras adjuntar el flujo de trabajo a un servidor, debe crear un usuario que pueda introducir el SFTP en el servidor y activar la ejecución del flujo de trabajo.

Configuración de un servidor de Transfer Family para ejecutar un flujo de trabajo

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Servidores y, a continuación, seleccione un servidor de la lista. Asegúrese de que este servidor es compatible con el protocolo SFTP.
3. En la página de detalles del servidor, desplácese hacia abajo hasta la sección Detalles adicionales y, a continuación, seleccione Editar.
4. En la página Editar detalles adicionales, en la sección Flujos de trabajo administrados, elija su flujo de trabajo y elija el rol de ejecución correspondiente.
 - En Flujos de trabajo para cargas completas de archivos, elija el flujo de trabajo que haya creado en [Paso 2: creación de un flujo de trabajo administrado](#), por ejemplo, **w-1234abcd5678efghi**.
 - En el rol de ejecución de flujos de trabajo administrados, elija el rol de IAM que creó en [Paso 1: creación y configuración de un rol de ejecución de IAM](#).
5. Desplácese hasta la parte inferior de la página y elija Guardar para guardar sus cambios.

Anote el ID del servidor que está utilizando. El nombre del AWS Secrets Manager secreto que se utiliza para almacenar las claves PGP se basa en parte en el ID del servidor.

Cómo añadir un usuario que pueda activar el flujo de trabajo

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Servidores y, a continuación, seleccione el servidor que utilice para el flujo de trabajo de descifrado.
3. En la página de detalles del servidor, desplácese hacia abajo hasta la sección Usuarios y seleccione Añadir usuario.
4. Para el nuevo usuario, introduzca los siguientes detalles:
 - En Nombre de usuario, introduzca **decrypt-user**.
 - En Rol, elija un rol de usuario que pueda acceder a su servidor.
 - En el Directorio de inicio, elija el bucket de Amazon S3 que utilizó anteriormente, por ejemplo, **amzn-s3-demo-bucket**.

- En el caso de las claves públicas de SSH, pega una clave pública que corresponda a la clave privada que tengas. Para obtener más información, consulte [Genere claves SSH para los usuarios administrados por el servicio](#).

5. Seleccione Añadir para guardar el nuevo usuario.

Anote el nombre de su usuario de Transfer Family para este servidor. El secreto se basa parcialmente en el nombre del usuario. Para simplificar, este tutorial usa un secreto predeterminado que puede usar cualquier usuario del servidor.

Paso 4: creación de un par de claves PGP

Utilice uno de los [clientes PGP compatibles](#) para generar un par de claves PGP. Este proceso se describe en detalle en [Generar claves PGP](#).

Generación de un par de claves PGP

1. Para este tutorial, puede usar el cliente gpg (GnuPG) versión 2.0.22 para generar un par de claves PGP que utilice RSA como algoritmo de cifrado. Para este cliente, ejecute el siguiente comando y proporcione una dirección de correo electrónico y una frase de contraseña. Puede usar cualquier nombre o dirección de correo electrónico que desee. Asegúrese de recordar los valores que utiliza, ya que tendrá que introducirlos más adelante en el tutorial.

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

Note

Si utiliza la versión 2.3.0 o posterior de GnuPG, debe ejecutar `gpg --full-gen-key`. Cuando se le pida el tipo de clave que desea crear, elija RSA o Elliptic Curve Cryptography (ECC, criptografía de curva elíptica). Si elige ECC, puede elegir NIST entre BrainPool y Curve25519 para la curva elíptica.

2. Exporte la clave privada mediante el siguiente comando. Sustituya `user@example.com` por la dirección de correo electrónico que utilizó al momento de generar la clave.

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


Este comando exporta la clave privada al archivo **workflow-tutorial-key.pgp**. Puede asignar al archivo de salida el nombre que desee. También puede eliminar el archivo de clave privada una vez que lo haya agregado AWS Secrets Manager.

Paso 5: Guarde la clave privada PGP en AWS Secrets Manager

Debe almacenar la clave privada en Secrets Manager, de una manera muy específica, para que el flujo de trabajo pueda encontrar la clave privada cuando el flujo de trabajo ejecute un paso de descifrado en un archivo cargado.

Note

Cuando guardas secretos en Secrets Manager, Cuenta de AWS incurres en cargos. Para obtener más información acerca de los precios, consulte [AWS Secrets Manager Precios](#).

Almacenamiento de una clave privada PGP en Secrets Manager

1. Inicia sesión en Consola de administración de AWS y abre la AWS Secrets Manager consola en <https://console.aws.amazon.com/secretsmanager/>.
2. En el panel de navegación izquierdo, seleccione Secretos.
3. En la página Secretos, seleccione Almacenar un nuevo secreto.
4. En la página Seleccionar tipo de secreto, en Tipo de secreto, seleccione Otro tipo de secreto.
5. En la sección de Key/value parejas, selecciona la Key/valuepestaña.
 - Clave: introduzca **PGPPrivateKey**.
 - valor: pegue el texto de su clave privada en el campo valor.
6. Seleccione Añadir fila y, en la sección de Key/value pares, elija la Key/valuepestaña.
 - Clave: introduzca **PGPPassphrase**.
 - valor: introduzca la contraseña que utilizó al generar su par de claves PGP en [Paso 4: creación de un par de claves PGP](#).
7. Elija Siguiente.

8. En la página Configurar secreto, introduzca un nombre y una descripción para el secreto. Puede crear un secreto para un usuario específico o uno que puedan usar todos los usuarios. Si su ID de servidor es **s-11112222333344445**, asigne el nombre al secreto de la siguiente manera.
 - Para crear un secreto predeterminado para todos los usuarios, asigne un nombre al secreto **aws/transfer/s-11112222333344445/@pgp-default**.
 - Para crear un secreto solo para el usuario que creó anteriormente, asigne un nombre al secreto **aws/transfer/s-11112222333344445/decrypt-user**.
9. Seleccione Siguiente y, a continuación, acepte los valores predeterminados de la página Configurar rotación. A continuación, elija Siguiente.
10. En la página de Revisión, elija Guardar para crear y almacenar el secreto.

Para obtener más información sobre cómo añadir tu clave privada PGP a Secrets Manager, consulta [Usar AWS Secrets Manager para almacenar tu clave PGP](#).

Paso 6: cifrado de un archivo

Use el programa gpg para cifrar un archivo para usarlo en su flujo de trabajo. Para cifrar el archivo, ejecute el siguiente comando:

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

Antes de ejecutar este comando, tenga en cuenta lo siguiente:

- Para el argumento **-r**, sustituya **marymajor@example.com** por la dirección de correo electrónico que utilizó al crear el par de claves PGP.
- La etiqueta **--openpgp** es opcional. Este indicador hace que el archivo cifrado se ajuste al estándar [RFC4880 de OpenPGP](#).
- Este comando crea un archivo cuyo nombre se encuentra **testfile.txt.gpg** en la misma ubicación que **testfile.txt**.

Important

Al cifrar archivos para usarlos con AWS Transfer Family flujos de trabajo, asegúrese siempre de especificar un destinatario no anónimo mediante el parámetro. **-r** El cifrado anónimo (sin especificar un destinatario) puede provocar errores de descifrado en el flujo de trabajo,

ya que el sistema no podrá identificar qué clave utilizar para el descifrado. La información sobre la depuración de este problema está disponible en. [Solucione problemas de cifrado de destinatarios anónimos](#)

Paso 7: ejecución del flujo de trabajo y visualización de los resultados

Para ejecutar el flujo de trabajo, debe conectarse al servidor de Transfer Family con el usuario que creó en el paso 3. A continuación, puede buscar en el bucket de Amazon S3 que especificó en el [paso 2.5 y configurar los parámetros de destino](#) para ver el archivo descifrado.

Ejecución del flujo de trabajo de descifrado

1. Abra un terminal de comandos.
2. Ejecute el siguiente comando y sustituya *your-endpoint* por su punto de conexión actual y *transfer-key* por la clave privada SSH de su usuario:

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

Por ejemplo, si la clave privada está almacenada en `~/.ssh/decrypt-user` y su punto de conexión es `s-11112222333344445.server.transfer.us-east-2.amazonaws.com`, el comando es el siguiente:

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

3. Ejecute el comando `pwd`. Si se ejecuta correctamente, este comando devuelve lo siguiente:

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

El directorio refleja el nombre del bucket de Amazon S3.

4. Ejecute el siguiente comando para cargar el archivo y activar el flujo de trabajo:

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

5. Como destino de los archivos descifrados, especificó la carpeta `decrypted-files/` al crear el flujo de trabajo. Ahora, puede ir a esa carpeta y enumerar el contenido.

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

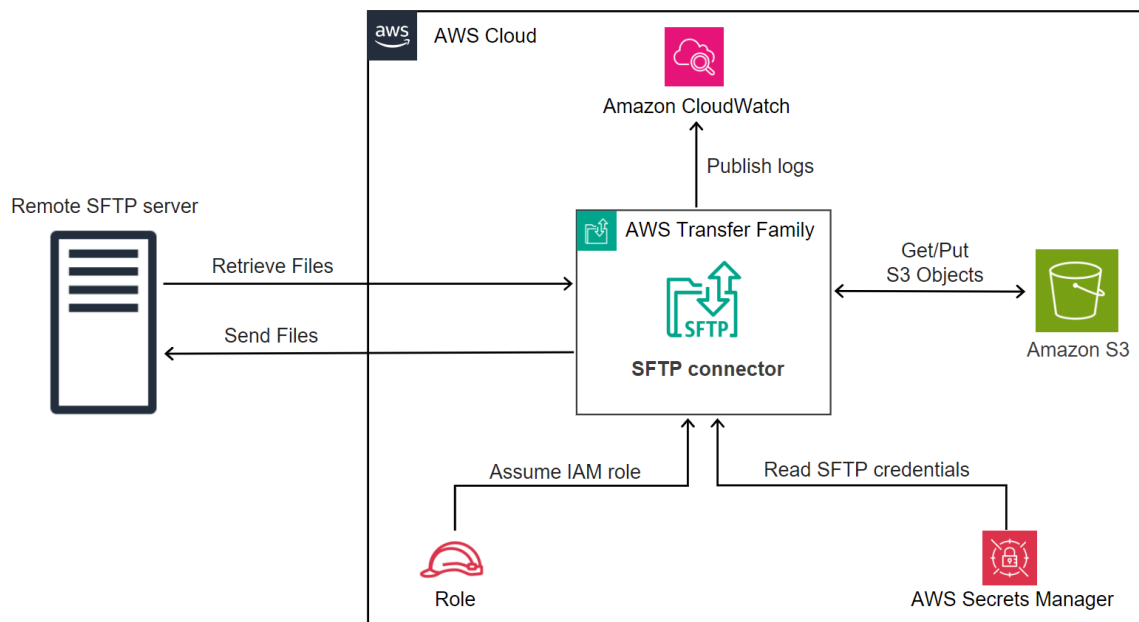
Si tiene éxito, el comando `ls` muestra el archivo `testfile.txt`. Puede descargar este archivo y comprobar que es el mismo que el archivo original que cifró anteriormente.

Configuración y uso de conectores SFTP

El propósito de un conector es establecer una relación entre su AWS almacenamiento y el servidor SFTP de un socio. Puede enviar archivos desde Amazon S3 a un destino externo propiedad de un socio. También puede usar un conector SFTP para recuperar archivos del servidor SFTP de un socio.

Este tutorial ilustra cómo configurar un conector SFTP con los tipos de salida gestionado por servicio y `VPC_LATTICE` y, a continuación, transferir archivos entre el almacenamiento de Amazon S3 y un servidor SFTP.

Un conector SFTP recupera las credenciales de SFTP para autenticarse en un servidor SFTP remoto y establecer AWS Secrets Manager una conexión. El conector envía o recupera archivos del servidor remoto y los almacena en Amazon S3. Puede elegir entre la salida gestionada por el servicio (mediante una infraestructura AWS gestionada) o la salida de VPC (enrutamiento a través de la Cross-VPC VPC mediante Resource Access). Se utiliza una función de IAM para permitir el acceso al bucket de Amazon S3 y a las credenciales almacenadas en Secrets Manager. Y puedes iniciar sesión en Amazon CloudWatch.



La siguiente entrada del blog proporciona una arquitectura de referencia para crear un flujo de trabajo de MFT con conectores SFTP, que incluye el cifrado de archivos mediante PGP antes de enviarlos a un servidor SFTP remoto mediante conectores SFTP: [diseño de transferencias de archivos gestionadas seguras y compatibles con conectores SFTP y cifrado PGP](#). AWS Transfer Family

Tipos de salida de conectores

Los conectores SFTP admiten dos tipos de salida que determinan cómo el conector enruta el tráfico a los servidores SFTP remotos:

- **SERVICE_MANAGED** (predeterminado): utiliza la infraestructura gestionada por AWS Transfer Family con direcciones IP estáticas para las conexiones salientes.
- **VPC**: dirige el tráfico a través de su VPC mediante Cross-VPC Resource Access, lo que permite la conectividad de puntos finales privados y el uso de sus propias puertas de enlace NAT.

Este tutorial cubre ambos tipos de salida. Elija el tipo de salida de VPC cuando necesite:

- Conéctese a servidores SFTP privados en su VPC (direcciones IP privadas)
- Conéctese a servidores SFTP locales mediante Direct Connect o VPN
- Dirija el tráfico de puntos finales públicos a través de su VPC para controles de seguridad
- Utilice sus propias direcciones IP elásticas para las conexiones salientes

Temas

- [Paso 1: Cree los recursos de apoyo necesarios](#)
- [Paso 2: Crear y probar un conector SFTP](#)
- [Paso 3: envíe y recupere archivos mediante el conector SFTP](#)
- [Procedimientos para crear un servidor Transfer Family para usarlo como servidor SFTP remoto](#)

Paso 1: Cree los recursos de apoyo necesarios

Puede utilizar conectores SFTP para copiar archivos entre Amazon S3 y cualquier servidor SFTP remoto. Para este tutorial, utilizaremos un AWS Transfer Family servidor como servidor SFTP remoto. Necesitamos crear y configurar los siguientes recursos:

- Cree buckets de Amazon S3 para almacenar archivos en su AWS entorno y enviar y recuperar archivos desde el servidor SFTP remoto.: [Creación de buckets de Amazon S3](#)
- Cree un AWS Identity and Access Management rol para acceder al almacenamiento de Amazon S3 y a nuestro secreto en Secrets Manager: [Cree un rol de IAM con los permisos necesarios](#).
- Cree un servidor Transfer Family que utilice el protocolo SFTP y un usuario gestionado por el servicio que utilice el conector SFTP para transferir archivos hacia o desde el servidor SFTP.: [Cree un servidor SFTP de Transfer Family y un usuario](#)
- Cree un AWS Secrets Manager secreto que almacene las credenciales utilizadas por el conector SFTP para iniciar sesión en el servidor SFTP remoto.: [Cree y almacene un secreto en AWS Secrets Manager](#)

Para los conectores de tipo salida de VPC, también necesita:

- Una VPC con las subredes y los grupos de seguridad adecuados
- Una puerta de enlace de recursos (se requieren 2 zonas de disponibilidad como mínimo):. [Crear una puerta de enlace de recursos \(solo tipo de salida de VPC\)](#)
- Una configuración de recursos que apunta a su servidor SFTP: [Crear una configuración de recursos \(solo tipo de salida de VPC\)](#). Para obtener más información, consulte [Configuraciones de recursos](#) en la Guía del usuario de Amazon VPC Lattice.

Creación de buckets de Amazon S3

Creación de un bucket de Amazon S3

1. Inicie sesión en la AWS Transfer Family consola en <https://console.aws.amazon.com/s3/>.
2. Elija una región e introduzca un nombre.

Para este tutorial, nuestro cubo está **US East (N. Virginia) us-east-1** incluido y el nombre **essftp-server-storage-east**.

3. Acepta los valores predeterminados y selecciona Crear depósito.

Para obtener información completa sobre la creación de buckets de Amazon S3, consulte [¿Cómo creo un bucket de S3?](#) en la Guía del usuario de Amazon Simple Storage Service.

Cree un rol de IAM con los permisos necesarios

Para el rol de acceso, cree una política con los siguientes permisos.

JSON

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

```

```

        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
},
{
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
}
]
}

```

Sustituya los elementos de la siguiente manera:

- Para `amzn-s3-demo-bucket`, el tutorial usa **`sftp-server-storage-east`**.
- Para `region`, el tutorial usa **`us-east-1`**.
- Para `account-id`, usa tu Cuenta de AWS ID.
- En `SecretName-6RandomCharacters` efecto, estamos a **using `sftp-connector1`** favor del nombre (tendrás tus propios seis caracteres aleatorios para tu secreto).

También debes asegurarte de que esta función contenga una relación de confianza que permita al conector acceder a tus recursos cuando atienda las solicitudes de transferencia de los usuarios. Para obtener más información sobre cómo establecer una relación de confianza, consulte [Para establecer una relación de confianza](#).

Note

Para ver los detalles del rol que vamos a usar en el tutorial, consulte [Función combinada de usuario y de acceso](#).

Cree y almacene un secreto en AWS Secrets Manager

Necesitamos almacenar un secreto en Secrets Manager para almacenar las credenciales de usuario de su conector SFTP. Puedes usar una contraseña, una clave privada SSH o ambas. Para el tutorial, usaremos una clave privada.

Note

Cuando guardas secretos en Secrets Manager, Cuenta de AWS incurres en cargos. Para obtener más información acerca de los precios, consulte [AWS Secrets Manager Precios](#).

Antes de comenzar el procedimiento para almacenar el secreto, recupere y formatee su clave privada. La clave privada debe corresponder a la clave pública que está configurada para el usuario en el servidor SFTP remoto. Para nuestro tutorial, la clave privada debe corresponder a la clave pública que está almacenada para nuestro usuario de prueba en el servidor SFTP de Transfer Family que utilizamos como servidor remoto.

Para ello, ejecute el siguiente comando:

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

Por ejemplo, si su archivo de clave privada se encuentra en `~/ssh/sftp-testuser-privatekey`, el comando es el siguiente.

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

Esto devuelve la clave en el formato correcto (con caracteres de nueva línea incrustados) a la salida estándar. Copie este texto en alguna parte, ya que tendrá que pegarlo en el siguiente procedimiento (en el paso 6).

Almacenamiento de las credenciales de usuario en Secrets Manager para un conector SFTP

1. Inicie sesión en Consola de administración de AWS y abra la AWS Secrets Manager consola en <https://console.aws.amazon.com/secretsmanager/>.
2. En el panel de navegación izquierdo, seleccione Secretos.
3. En la página Secretos, seleccione Almacenar un nuevo secreto.
4. En la página Seleccionar tipo de secreto, en Tipo de secreto, seleccione Otro tipo de secreto.

5. En la sección de Key/value parejas, selecciona la Key/value pestaña.
 - Clave: Entrar **Username**.
 - valor: introduzca el nombre de nuestro usuario, **sftp-testuser**.
6. Para introducir la clave, le recomendamos que utilice la pestaña Texto sin formato.
 - a. Seleccione Añadir fila y, a continuación, introduzca **PrivateKey**.
 - b. Elija la pestaña Texto sin formato. El campo ahora contiene el siguiente texto:

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

- c. Pegue el texto de su clave privada (guardado anteriormente) entre las comillas dobles vacías («»).

La pantalla debería tener el siguiente aspecto (los datos clave aparecen atenuados).



7. Elija Siguiente.
8. En la página Configurar el secreto, introduzca un nombre para el secreto. En este tutorial, asignamos un nombre al secreto **aws/transfer/sftp-connector1**.
9. Seleccione Siguiente y, a continuación, acepte los valores predeterminados de la página Configurar rotación. A continuación, elija Siguiente.
10. En la página de Revisión, elija Guardar para crear y almacenar el secreto.

Crear una puerta de enlace de recursos (solo tipo de salida de VPC)

Para los conectores de tipo salida de VPC, debe crear una puerta de enlace de recursos en su VPC. La puerta de enlace de recursos sirve como punto de entrada para Cross-VPC el acceso a los recursos.

Para crear una pasarela de recursos

1. Ejecute el siguiente comando para crear una puerta de enlace de recursos (sustituya el ID de VPC y los ID de subred por sus valores):

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

Note

Las pasarelas de recursos requieren subredes en al menos 2 zonas de disponibilidad.

2. Anote el ID de Resource Gateway de la respuesta para usarlo en el siguiente paso.

Crear una configuración de recursos (solo tipo de salida de VPC)

Cree una configuración de recursos que apunte a su servidor SFTP. Puede ser una dirección IP privada para los servidores de la VPC o un nombre DNS público para los servidores externos. Para obtener más información sobre las configuraciones de recursos, consulte [Configuraciones de recursos](#) en la Guía del usuario de Amazon VPC Lattice.

Para crear una configuración de recursos

1. Para un servidor SFTP privado, ejecute:

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

2. Para un servidor SFTP público (solo nombre DNS), ejecute:

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

 Note

Los puntos finales públicos deben usar nombres DNS, no direcciones IP.

3. Anote el ARN de configuración de recursos de la respuesta para usarlo al crear el conector.

Paso 2: Crear y probar un conector SFTP

En esta sección, creamos un conector SFTP que utiliza todos los recursos que creamos anteriormente. Para obtener más información, consulte [Creación de conectores SFTP](#).

Creación de un Conector SFTP

1. Abre la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>
2. En el panel de navegación izquierdo, seleccione Conectores SFTP y, a continuación, seleccione Crear conector SFTP.
3. Para el tipo de salida, elija una de las siguientes opciones:
 - Servicio gestionado (predeterminado): utiliza la infraestructura gestionada por AWS Transfer Family con direcciones IP estáticas para las conexiones salientes.
 - VPC Lattice: dirige el tráfico a través de su VPC mediante Resource Access. Cross-VPC Elija esta opción para la conectividad de puntos finales privados o para usar sus propias puertas de enlace NAT.

 Important

No puede cambiar el tipo de salida después de crear el conector. Elija con cuidado en función de sus requisitos de conectividad.

4. En la sección de Configuración del conector, proporcione la siguiente información:

- Para la URL, introduzca la URL del servidor SFTP remoto. Para el tutorial, introducimos la URL del servidor Transfer Family que estamos utilizando como servidor SFTP remoto.

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

1111aaaa2222bbbb3 Sustitúyalo por tu ID de servidor de Transfer Family.

- Para el rol de acceso, ingresa el rol que creamos anteriormente, **sftp-connector-role**.
- Para el ARN de configuración de recursos (solo tipo de salida de entramado de VPC), introduzca el ARN de la configuración de recursos que creó anteriormente:

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

- Para la función de registro, elija una función que incluya una política de confianza en el elemento principal. `transfer.amazonaws.com`

Consejo: Además de añadir Transfer Family como entidad de confianza, puede añadir la política `AWSTransferLoggingAccess` AWS gestionada al rol. Esta política se describe en detalle en [AWSTransferLoggingAccess](#).

Connector configuration

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

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.
 ☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

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

URL of the remote (target) SFTP server

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

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

5. En el panel Configuración SFTP, proporcione la siguiente información:

- Para las credenciales de Connector, elija el nombre del recurso de Secrets Manager que contiene las credenciales de SFTP. Para el tutorial, elija **aws/transfer/sftp-connector1**.
- En el caso de las claves de host confiables, pegue la parte pública de la clave de host. Puede recuperar esta clave ejecutándola `ssh-keyscan` para su servidor SFTP. Para obtener más información sobre cómo formatear y almacenar la clave de host de confianza, consulta la documentación [SftpConnectorConfig](#) sobre los tipos de datos.
- Para el número máximo de conexiones simultáneas, seleccione un valor entero entre 1 y 5: el valor predeterminado es 5.

SFTP configuration Info

Connector credentials Info

Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server

aws/transfer/sftp-connector1
Store a new secret

Trusted host keys - optional Info

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

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

ssh-rsa AAAAE
Remove

Add trusted host key

Maximum concurrent connections Info

Select the maximum number of concurrent connections that your connector can create to the remote server

5

- Una vez que haya confirmado todos los ajustes, elija **Crear conector** para crear el conector SFTP.

También puede crear conectores mediante AWS Command Line Interface

- Para crear un conector SFTP con salida gestionada por el servicio, ejecute el siguiente comando:

```
aws transfer create-connector \
  --url "sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
```

```
--sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-rsa AAAAB3NzaC..."
```

- Para crear un conector SFTP con VPC-based salida, ejecute el siguiente comando:

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

Tras crear un conector SFTP, le recomendamos que lo pruebe antes de intentar transferir cualquier archivo con el nuevo conector.

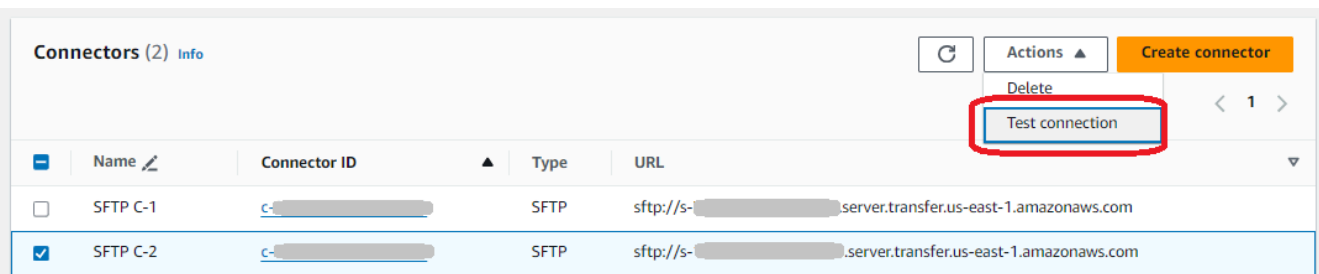
Note

En el caso de los conectores de tipo salida de VPC, la resolución del DNS puede tardar varios minutos después de la creación. Durante este tiempo, el estado del conector será PENDING y TestConnection volverá a ser «Conector no disponible». Espere a que aparezca el estado ACTIVE antes de intentar transferir los archivos.

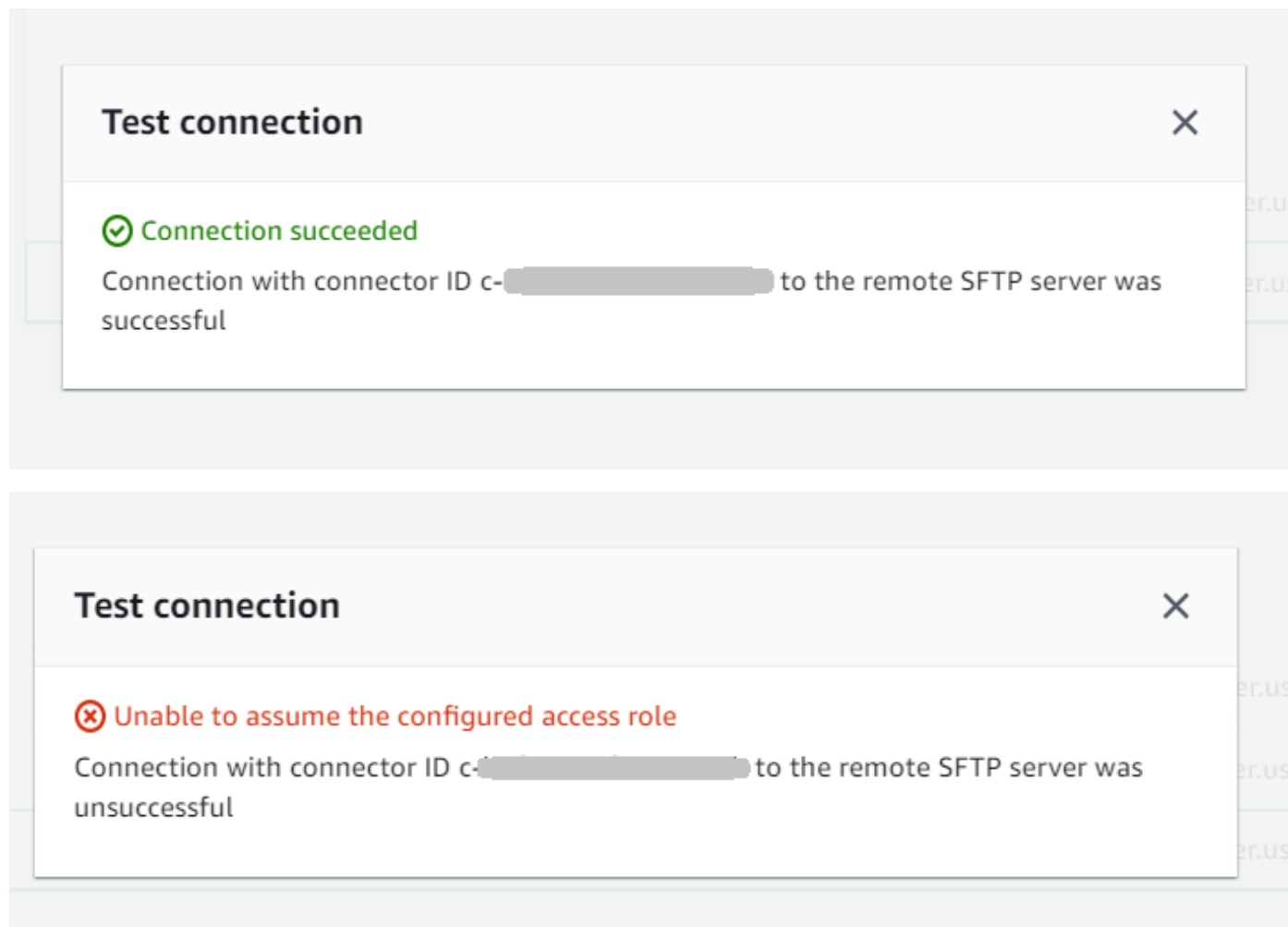
Test a connector using the console

Prueba de un conector SFTP

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, elija Conectores SFTP y seleccione un conector.
3. En el menú Acciones, seleccione Evento de prueba.



El sistema devuelve un mensaje que indica si la prueba se supera o no. Si la prueba no es satisfactoria, el sistema muestra un mensaje de error en función del motivo por el que no se ha realizado la prueba.



Test a connector using the CLI

Para probar un conector mediante el AWS Command Line Interface, ejecute el siguiente comando en una línea de comandos (*connector-id* sustitúyalo por su ID de conector real):

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

Si la prueba se realiza correctamente, se devolverán las siguientes líneas:

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


Si la prueba no tiene éxito, recibirá un mensaje de error descriptivo, por ejemplo:

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

Cuando describe un conector de tipo salida de VPC, la respuesta incluye los nuevos campos:

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

Tenga en cuenta que `ServiceManagedEgressIpAddresses` es nulo para los conectores de tipo salida de VPC, ya que el tráfico se dirige a través de la VPC en lugar de a través de la infraestructura gestionada. AWS

Paso 3: envíe y recupere archivos mediante el conector SFTP

Para simplificar, asumimos que ya tiene archivos en su bucket de Amazon S3.

Note

En el tutorial se utilizan buckets de Amazon S3 para las ubicaciones de almacenamiento de origen y destino. Si su servidor SFTP no utiliza el almacenamiento de Amazon S3, siempre

que aparezca `sftp-server-storage-east` en los siguientes comandos, puede sustituir la ruta por una ruta a las ubicaciones de los archivos accesibles desde su servidor SFTP.

- Enviamos un archivo con el nombre `SEND-to-SERVER.txt` del almacenamiento de Amazon S3 al servidor SFTP.
- Recuperamos un archivo con el nombre `RETRIEVE-to-S3.txt` del servidor SFTP al almacenamiento de Amazon S3.

 Note

En los siguientes comandos, sustitúyalo por *connector-id* tu ID de conector.

En primer lugar, enviamos un archivo desde nuestro bucket de Amazon S3 al servidor SFTP remoto. Desde una línea de comandos, ejecute el siguiente comando:

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

Su `sftp-server-storage-east` depósito ahora debería tener este aspecto.

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

incoming/

[Copy S3 URI](#)

Objects | Properties

Objects (1) Info

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

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

[Upload](#)

Find objects by prefix

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

Si no ves el archivo como esperabas, comprueba CloudWatch los registros.

Para comprobar tus CloudWatch registros

1. Abre la CloudWatch consola de Amazon en <https://console.aws.amazon.com/cloudwatch/>
2. Selecciona Grupos de registros en el menú de navegación de la izquierda.
3. Introduce tu ID de conector en la barra de búsqueda para buscar tus registros.
4. Seleccione el flujo de registro que se devuelve de la búsqueda.
5. Amplíe la entrada de registro más reciente.

Si se realiza correctamente, la entrada de registro tendrá el siguiente aspecto:

```
{
  "operation": "SEND",
  "timestamp": "2023-12-18T15:26:57.346283Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/sftp-server-storage-east/SEND-to-SERVER.txt",
```

```

"status-code": "COMPLETED",
"start-time": "2023-12-18T15:26:56.915864Z",
"end-time": "2023-12-18T15:26:57.298122Z",
"account-id": "account-id",
"connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
"remote-directory-path": "/sftp-server-storage-east/incoming"
}

```

Si la transferencia del archivo ha fallado, la entrada de registro contiene un mensaje de error que especifica el problema. Las causas más comunes de los errores son los problemas con los permisos de IAM y las rutas de archivo incorrectas.

A continuación, recuperamos un archivo del servidor SFTP y lo colocamos en un bucket de Amazon S3. Desde una línea de comandos, ejecute el siguiente comando:

```

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

```

Si la transferencia se realiza correctamente, su bucket de Amazon S3 contiene el archivo transferido, como se muestra aquí.

The screenshot shows the Amazon S3 console interface. At the top, the breadcrumb navigation indicates the path: Amazon S3 > Buckets > sftp-server-storage-east > incoming/. The main heading is 'incoming/'. Below this, there are tabs for 'Objects' and 'Properties'. The 'Objects' tab is active, showing a list of objects. The list has one object, 'RETRIEVE-to-S3.txt', which is a text file (txt) of 4.1 KB, last modified on December 18, 2023, at 10:26:58 (UTC-05:00), and stored in the Standard storage class. Above the list, there are buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', and 'Create folder'. There is also an 'Upload' button and a search bar labeled 'Find objects by prefix'.

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

Si se realiza correctamente, la entrada de registro tendrá el siguiente aspecto:

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

Solución de problemas de conectores de tipo salida de VPC

Si tiene problemas con los conectores de tipo salida de VPC, compruebe lo siguiente:

- El estado del conector es PENDIENTE: la resolución de DNS para los conectores de VPC puede tardar varios minutos. Espere a que el estado se active antes de intentar realizar la conexión.
- Tiempos de espera de conexión: compruebe que los grupos de seguridad permiten el tráfico en el puerto 22 entre las subredes de Resource Gateway y el servidor SFTP de destino.
- Errores de configuración de recursos: asegúrese de que la configuración de recursos apunte a la dirección IP o el nombre de DNS correctos y que la puerta de enlace de recursos esté en la misma VPC que su servidor SFTP (para puntos finales privados). Para obtener más información, consulte [Configuraciones de recursos](#) en la Guía del usuario de Amazon VPC Lattice.
- Problemas con los puntos finales públicos: en el caso de los puntos finales públicos, asegúrese de utilizar un nombre DNS, no una dirección IP, en la configuración de recursos. Compruebe que la VPC tenga una puerta de enlace NAT para el acceso saliente a Internet.
- Disponibilidad AZ: las pasarelas de recursos requieren subredes en al menos 2 zonas de disponibilidad. No todas las AZ son compatibles con VPC Lattice; compruebe las AZ compatibles en su región.

Consideraciones de costo para el tipo de salida de VPC:

- VPC Lattice cobra 0\$. 006/GB para el procesamiento de datos como proveedor de recursos (facturado directamente por VPC Lattice)
- AWS Transfer Family absorbe los 0 dólares. 01/GB costos por consumo de recursos (primer PB)
- Para los puntos finales públicos a través de VPC, se pueden aplicar cargos adicionales por transferencia de datos y puerta de enlace NAT.
- No hay cargos adicionales de Transfer Family más allá de los 0\$ estándar. 40/GB tarifa de procesamiento de datos

Procedimientos para crear un servidor Transfer Family para usarlo como servidor SFTP remoto

A continuación, describimos los pasos para crear un servidor Transfer Family que sirva como servidor SFTP remoto para este tutorial. Tenga en cuenta lo siguiente:

- Usamos un servidor Transfer Family para representar un servidor SFTP remoto. Los usuarios típicos de conectores SFTP tienen su propio servidor SFTP remoto. Consulte [Cree un servidor SFTP de Transfer Family y un usuario](#).
- Como utilizamos un servidor Transfer Family, también utilizamos un usuario de SFTP gestionado por el servicio. Y, para simplificar, combinamos los permisos que este usuario necesita para acceder al servidor Transfer Family con los permisos que necesita para usar nuestro conector. De nuevo, la mayoría de los casos de uso de conectores SFTP tienen un usuario SFTP independiente que no está asociado a un servidor Transfer Family. Consulte [Cree un servidor SFTP de Transfer Family y un usuario](#).
- Para el tutorial, dado que utilizamos el almacenamiento de Amazon S3 para nuestro servidor SFTP remoto, necesitamos crear un segundo depósito para poder transferir archivos de un depósito a otro. **sftp-server-storage-east**

Cree un servidor SFTP de Transfer Family y un usuario

La mayoría de los usuarios no necesitarán crear un servidor SFTP Transfer Family ni un usuario, ya que ya tienes un servidor SFTP con usuarios y puedes usar este servidor para transferir archivos de ida y vuelta. Sin embargo, para este tutorial, para simplificar, utilizamos un servidor Transfer Family que funciona como servidor SFTP remoto.

Siga el procedimiento descrito en [Crea un SFTP-enabled servidor](#) para crear un servidor y [Paso 3: agregar un usuario de servicio administradas](#) agregar un usuario. Estos son los detalles del usuario que vamos a utilizar para el tutorial:

- Cree su usuario gestionado por el servicio, `sftp-testuser`
 - Configure el directorio principal en `/sftp-server-storage-east/sftp-testuser`
 - Al crear el usuario, se almacena una clave pública. Más adelante, cuando crees el secreto en Secrets Manager, tendrás que proporcionar la clave privada correspondiente.
- Función: `sftp-connector-role`. Para el tutorial, utilizamos la misma función de IAM tanto para nuestro usuario de SFTP como para acceder al conector de SFTP. Al crear conectores para su organización, es posible que tenga funciones de usuario y de acceso independientes.
- Clave de host del servidor: debe usar la clave de host del servidor al crear el conector. Puede recuperar esta clave ejecutándola `ssh-keyscan` para su servidor. Por ejemplo, si el identificador de su servidor es `s-1111aaaa2222bbbb3` y su punto final está activado `us-east-1`, el siguiente comando recupera la clave de host del servidor:

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

Copie este texto en alguna parte, ya que tendrá que pegarlo en el [Paso 2: Crear y probar un conector SFTP](#) procedimiento.

Función combinada de usuario y de acceso

Para el tutorial, utilizamos un único rol combinado. Usamos esta función tanto para nuestro usuario de SFTP como para acceder al conector. El siguiente ejemplo contiene los detalles de este rol, por si desea realizar las tareas del tutorial.

El siguiente ejemplo concede los permisos necesarios para acceder a nuestros dos buckets en Amazon S3 y al secreto denominado `aws/transfer/sftp-connector1` almacenado en Secrets Manager. En el tutorial, este rol recibe un nombre `sftp-connector-role`.

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

```

        "s3:ListBucket",
        "s3:GetBucketLocation"
    ],
    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::sftp-server-storage-east",
        "arn:aws:s3:::sftp-server-storage-east"
    ]
},
{
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": [
        "arn:aws:s3:::sftp-server-storage-east/*",
        "arn:aws:s3:::sftp-server-storage-east/*"
    ]
},
{
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-east-1:111122223333:secret:aws/transfer/sftp-connector1-6RandomCharacters"
}
]
}

```

Para obtener información completa sobre la creación de roles para Transfer Family, siga el procedimiento descrito en [Creación de un rol de usuario](#) Para crear un rol.

Configuración de un método de Amazon API Gateway como proveedor de identidad personalizado

En este tutorial se muestra cómo configurar un método de Amazon API Gateway y utilizarlo como proveedor de identidad personalizado para cargar archivos en un AWS Transfer Family servidor. En este tutorial solo se utiliza la [plantilla de pila básica](#) y otras funciones básicas como ejemplo.

Temas

- [Requisitos previos](#)
- [Paso 1: Crear una CloudFormation pila](#)
- [Paso 2: verificación de la configuración del método API Gateway para su servidor](#)
- [Paso 3: visualización de los detalles del servidor de Transfer Family](#)
- [Paso 4: comprobación de que el usuario puede conectarse al servidor](#)
- [Paso 5: prueba de la conexión SFTP y la transferencia de archivos](#)
- [Paso 6: limitación del acceso al bucket](#)
- [Actualice Lambda si utiliza Amazon EFS](#)

Requisitos previos

Antes de crear los recursos de Transfer Family en CloudFormation, cree su almacenamiento y su rol de usuario.

Cómo especificar el almacenamiento y crear un rol de usuario

1. Según el almacenamiento que utilice, consulte la siguiente documentación:
 - Para crear un bucket de Amazon S3, consulte [¿Cómo se crea un bucket de S3?](#) en la Guía del usuario de la consola de Amazon Simple Storage Service.
 - Para crear un sistema de archivos Amazon EFS, consulte [Configuración de un sistema de archivos Amazon EFS](#).
2. Para crear un rol de usuario, consulte [Creación de una política y un rol de IAM](#)

Introduzca los detalles de su almacenamiento y su rol de usuario al crear su pila CloudFormation en la siguiente sección.

Paso 1: Crear una CloudFormation pila

Para crear una AWS CloudFormation pila a partir de la plantilla proporcionada

1. Abra la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
2. Seleccione Crear pila y seleccione Con recursos nuevos (estándar).
3. En el panel Requisitos previos: preparar plantilla, elija Elegir una plantilla existente.
4. Copie este enlace, [plantilla de pila básica](#), y péguelo en el campo URL de Amazon S3.
5. Haga clic en Next (Siguiente).
6. Especifique los parámetros, incluido un nombre para la pila. Asegúrese de hacer lo siguiente:
 - Sustituya los valores predeterminados por UserName y UserPassword.
 - Para UserHomeDirectory, introduzca los detalles del almacenamiento (ya sea un bucket de Amazon S3 o un sistema de archivos Amazon EFS) que creó anteriormente.
 - Sustituya la función UserRoleArn de usuario predeterminada por la que creó anteriormente. El rol AWS Identity and Access Management (IAM) debe tener los permisos adecuados. Para ver una política de bucket y de rol de IAM de ejemplo, consulte [Paso 6: limitación del acceso al bucket](#).
 - Si desea autenticarse con una clave pública en lugar de una contraseña, introduzca la clave pública en el UserPublicKey1 campo. La primera vez que se conecta al servidor mediante SFTP, proporciona la clave privada en lugar de una contraseña.
7. Seleccione Siguiente y, a continuación, vuelva a seleccionar Siguiente en la página Configurar opciones de pila.
8. Revise los detalles de la pila que esté creando y, a continuación, seleccione Crear pila.

Note

En la parte inferior de la página, en Capacidades, debe reconocer que CloudFormation podría crear recursos de IAM.

Paso 2: verificación de la configuración del método API Gateway para su servidor

Note

Para mejorar la seguridad, puede configurar un firewall de aplicaciones web. AWS WAF es un firewall de aplicaciones web que permite monitorizar las solicitudes HTTP y HTTPS que se reenvían a una Amazon API Gateway. Para obtener más información, consulte [Agregue un cortafuegos de aplicaciones web](#).

No habilite el almacenamiento en caché de API Gateway

No habilite el almacenamiento en caché para tu método API Gateway cuando lo utilices como proveedor de identidad personalizado para Transfer Family. El almacenamiento en caché es inapropiado e inválido para las solicitudes de autenticación porque:

- Cada solicitud de autenticación es única y requiere una respuesta en tiempo real, no una respuesta en caché
- El almacenamiento en caché no ofrece ningún beneficio, ya que Transfer Family nunca envía solicitudes duplicadas o repetidas a la API Gateway.
- Al habilitar el almacenamiento en caché, la API Gateway responderá con datos no coincidentes, lo que provocará que las respuestas a las solicitudes de autenticación no sean válidas

Comprobación de la configuración del método API Gateway para su servidor e implementación

1. Abra la consola de API Gateway en <https://console.aws.amazon.com/apigateway/>.
2. Elija la API de plantilla básica Transfer Custom Identity Provider que generó la CloudFormation plantilla.
3. En el panel Recursos, seleccione GET y, a continuación, Solicitud de método.
4. Para Acciones, elija Implementar API. Para la Etapa de implementación, elija prod y, a continuación, elija Implementar.

Una vez que el método API Gateway se haya implementado correctamente, consulte su rendimiento en la sección Stage Editor.

 Note

Copie la dirección URL de invocación que aparece en la parte superior de la página. Lo necesitará para el siguiente paso.

Paso 3: visualización de los detalles del servidor de Transfer Family

Al utilizar la plantilla para crear una CloudFormation pila, se crea automáticamente un servidor Transfer Family.

Visualización de los detalles del servidor de Transfer Family

1. Abra la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
2. Elija la pila que ha creado.
3. Elija la pestaña Recursos.

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

El ARN del servidor se muestra en la columna ID física de la TransferServer fila. El ID del servidor está contenido en el ARN, por ejemplo, s-11112222333344445.

- Abra la AWS Transfer Family consola en y <https://console.aws.amazon.com/transfer/>, en la página Servidores, elija el nuevo servidor.

El ID del servidor coincide con el ID que se muestra para el TransferServer recurso en CloudFormation.

Paso 4: comprobación de que el usuario puede conectarse al servidor

Comprobación de que el usuario puede conectarse al servidor, mediante la consola Transfer Family

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En la página Servidores, elija su nuevo servidor, elija Acciones y, a continuación, elija Probar.
3. Introduzca el texto de sus credenciales de inicio de sesión en el campo Nombre de usuario y en el campo Contraseña. Estos son los valores que estableció al implementar la CloudFormation pila.
4. Para Protocolo de servidor, seleccione SFTP y, para IP de origen, introduzca **127.0.0.1**.
5. Seleccione Probar

Si la autenticación del usuario se realiza correctamente, la prueba devuelve una respuesta `Status Code: 200` HTML y un objeto JSON que contiene los detalles de los roles y los permisos del usuario. Por ejemplo:

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

Si la prueba falla, agrega una de las políticas AWS administradas por API Gateway al rol que estás usando para tu API.

Paso 5: prueba de la conexión SFTP y la transferencia de archivos

Prueba de la conexión SFTP

1. En Linux o macOS, abra un terminal de comandos.
2. Ingrese uno de los siguientes comandos en función de si utiliza una contraseña o un par de claves para la autenticación.
 - Si utiliza una contraseña, introduzca este comando:

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

Escriba la contraseña cuando se le solicite.

- Si utiliza un par de claves, introduzca este comando:

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

Note

Para estos comandos `sftp`, inserte el código de la Región de AWS donde está ubicado su servidor de Transfer Family. Por ejemplo, si su servidor está en el este de EE. UU. (Ohio), introduzca **us-east-2**.

3. Cuando aparezca `sftp>`, asegúrese de que puede cargar (`put`), descargar (`get`) y ver directorios y archivos (`pwd` y `ls`).

Paso 6: limitación del acceso al bucket

Puede limitar quién accede a un bucket específico de Amazon S3. En el siguiente ejemplo, se muestran los ajustes que se deben utilizar en la CloudFormation pila y en la política que se seleccione para el usuario.

En este ejemplo, configuramos los siguientes parámetros para la CloudFormation pila:

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

Important

Este es un ejemplo de contraseña. Al configurar el método API Gateway, asegúrese de introducir una contraseña segura.

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

UserPublicKey1Es una clave pública que ha generado como parte de un public/private key pair.

role-id es exclusivo del rol de usuario que cree. La política asociada a myuser-api-gateway-role es la siguiente:

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

Para conectarse al servidor mediante SFTP, ingrese uno de los comandos siguientes en la ventana.

- Si utiliza una contraseña para autenticarse, ejecute el siguiente comando:

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


Escriba la contraseña cuando se le solicite.

- Si utiliza un par de claves para autenticarse, ejecute el siguiente comando:

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

Note

Para estos sftp comandos, utilice el ID de Región de AWS la ubicación del servidor Transfer Family. Por ejemplo, si su servidor está en el este de EE. UU. (Ohio), utilice us-east-2.

Cuando sftp aparezca la línea de comandos, accederá a su directorio de inicio, que podrá ver ejecutando el comando pwd. Por ejemplo:

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

El usuario no puede ver ningún directorio situado por encima del directorio de inicio. Por ejemplo:

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

Actualice Lambda si utiliza Amazon EFS

Si seleccionó Amazon EFS como la opción de almacenamiento para su servidor de Transfer Family, tendrá que editar la función de lambda de su pila.

Para añadir un perfil Posix a la función Lambda

1. Abra la consola Lambda en <https://console.aws.amazon.com/lambda/>
2. Elija la función de Lambda que ha creado. La función Lambda tiene el formato ***stack-name-GetUserConfigLambda - lambda-identifier***, donde ***stack-name*** es el nombre de la CloudFormation pila y ***lambda-identifier*** es el identificador de la función.

3. En la pestaña Código, seleccione `index.js` para ver el código de la función.
4. En response, añada la siguiente línea entre `Policy` y `HomeDirectory`:

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

Donde *uid-value* y *gid-value* son números enteros, 0 o mayores, que representan el ID de usuario y el ID de grupo, respectivamente.

Por ejemplo, después de agregar el perfil Posix, el campo de respuesta podría tener el siguiente aspecto:

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

Configuración de una configuración AS2

Este tutorial explica cómo configurar una configuración de la Declaración de Aplicabilidad 2 (AS2) con AWS Transfer Family. Tras completar los pasos descritos aquí, dispondrá de un AS2-enabled servidor preparado para aceptar mensajes AS2 de un socio comercial de muestra. También dispondrá de un conector que se puede utilizar para enviar mensajes de AS2 al socio comercial de muestra.

Note

Algunas partes de la configuración del ejemplo utilizan el AWS Command Line Interface (AWS CLI). Si aún no lo ha instalado AWS CLI, consulte [Instalación o actualización de la última versión de AWS CLI en la](#) Guía del AWS Command Line Interface usuario.

1. Cree certificados para usted y su socio comercial. Si tiene certificados existentes que pueda utilizar, puede omitir esta sección.

Este proceso se describe en [Paso 1: creación de los certificados para AS2](#).

2. Importar los certificados que se han creado en el paso 1.

Este proceso se describe en [Paso 2: Importar certificados como recursos de certificados de Transfer Family](#).

3. Para configurar sus socios comerciales, cree un perfil local y un perfil de socio.

Este proceso se describe en [Paso 3: Cree perfiles para usted y su socio comercial](#).

4. Cree un AWS Transfer Family servidor que utilice el protocolo AS2. Si lo desea, puede agregar una dirección IP elástica al servidor para que esté conectado a Internet.

Este proceso se describe en [Paso 4: Crear un servidor Transfer Family que utilice el protocolo AS2](#).

 Note

Debe crear un servidor de Transfer Family solo para transferencias entrantes. Si solo realiza transferencias salientes, no necesita un servidor de Transfer Family.

5. Crear un acuerdo entre usted y su socio comercial.

Este proceso se describe en [Paso 5: creación de un acuerdo entre usted y su socio](#).

 Note

Debe crear un acuerdo únicamente para las transferencias entrantes. Si solo realiza transferencias salientes, no necesita un acuerdo.

6. Crear un conector entre usted y su socio comercial.

Este proceso se describe en [Paso 6: creación de un conector entre usted y su socio](#).

 Note

Debe crear un conector únicamente para las transferencias salientes. Si solo realiza transferencias entrantes, no necesita conector.

7. Probar un intercambio de archivos AS2.

Este proceso se describe en [Paso 7: prueba del intercambio de archivos a través de AS2 mediante Transfer Family](#).

Una vez completados estos pasos, podrá realizar lo siguiente:

- Envíe archivos a un servidor AS2-enabled asociado remoto con el comando `Transfer Family start-file-transfer` AWS Command Line Interface (AWS CLI).
- Reciba archivos de un servidor AS2-enabled asociado remoto en el puerto 5080 a través de su terminal de nube privada virtual (VPC).

Paso 1: creación de los certificados para AS2

Ambas partes de un intercambio de AS2 necesitan certificados. X.509 Puede crear estos certificados de la forma que lo desee. En este tema, se describe cómo utilizar [OpenSSL](#) desde la línea de comandos para crear un certificado raíz y, a continuación, firmar los certificados subordinados. Las dos partes deben generar sus propios certificados.

Note

La longitud de la clave de los certificados AS2 debe ser de al menos 2048 bits y, como máximo, de 4096.

Para transferir archivos con un socio, tenga en cuenta lo siguiente:

- Puede adjuntar certificados a los perfiles. Los certificados contienen claves públicas o privadas.
- Su socio comercial le envía sus claves públicas y usted le envía las suyas.
- Su socio comercial cifra los mensajes con su clave pública y los firma con su clave privada. Por el contrario, usted encripta los mensajes con la clave pública de su socio y los firmas con su propia clave privada.

Note

Si prefiere administrar las claves con una interfaz gráfica de usuario, [Portecle](#) es una opción que puede utilizar.

Generación de certificados de ejemplo

Important

No envíe sus claves privadas a su socio. En este ejemplo, genera un conjunto de claves públicas y privadas autofirmadas para una de las partes. Si van a actuar como socios comerciales a efectos de prueba, puede repetir estas instrucciones para generar dos conjuntos de claves: uno para cada socio comercial. En este caso, no es necesario generar dos autoridades de certificación raíz (CA).

1. Ejecute el siguiente comando para generar una clave privada RSA con un módulo de 2048 bits de longitud.

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

2. Ejecute el siguiente comando para crear un certificado autofirmado con su archivo `root-ca-key.pem`.

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

El argumento `-subj` consta de los siguientes valores.

	Name	Description (Descripción)
C	Código de país	Un código de dos letras para el país en el que se encuentra la organización.
ST	Estado, región o provincia	Nombre del país o de la región donde se ubica su empresa. (En este caso,

	Name	Description (Descripción)
		región no se refiere a su Región de AWS.)
L	Nombre de la localidad	Nombre de la ciudad donde se ubica su empresa.
O	Nombre de la organización	El nombre legal completo de su empresa, incluidos los sufijos, como LLC, Corp, etc.
OU	Nombre de la unidad organizativa	La división de su empresa que se ocupa de este certificado.
CN	Nombre común o nombre de dominio completo (FQDN)	En este caso, estamos creando un certificado raíz, por lo que el valor es ROOTCA. En estos ejemplos, utilizamos CN para describir el propósito del certificado.

3. Cree una clave de firma y una clave de cifrado para su perfil local.

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

Note

Algunos AS2-enabled servidores, como OpenAS2, requieren que se utilice el mismo certificado tanto para la firma como para el cifrado. En este caso, puede importar la misma clave privada y el mismo certificado con ambos fines. Para ello, ejecute este comando en lugar de los dos comandos anteriores:

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

4. Ejecute los siguientes comandos para crear solicitudes de firma de certificados (CSR) para que firme la clave raíz.

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

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

5. A continuación, debe crear un archivo `signing-cert.conf` y un archivo `encryption-cert.conf`.

- Utilice un editor de texto para crear un archivo `signing-cert.conf` con los siguientes contenidos:

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

- Utilice un editor de texto para crear un archivo `encryption-cert.conf` con los siguientes contenidos:

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

6. Por último, para crear los certificados firmados, ejecute los siguientes comandos.

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

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

Paso 2: Importar certificados como recursos de certificados de Transfer Family

En este procedimiento, se explica cómo importar certificados mediante AWS CLI. Si en su lugar, desea utilizar la consola Transfer Family, consulte [the section called “Importar certificados AS2”](#).

Para importar los certificados de firma y cifrado que creó en el paso 1, ejecute los siguientes comandos `import-certificate`. Si utiliza el mismo certificado para cifrar y firmar, importe el mismo certificado dos veces (una con el uso `SIGNING` y otra con el uso `ENCRYPTION`).

Note

Si tiene un archivo que contiene tanto un certificado como su cadena, puede proporcionar ese archivo al `import-certificate` comando utilizando únicamente el `certificate` parámetro. Por ejemplo:

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

Si usa el `certificate` parámetro para cargar tanto el certificado como su cadena, no lo use. `certificate-chain`

Si combina el certificado y su cadena, la clave se formatea según los estándares PEM convencionales, que incluyen una nueva línea «\n» cada 64 caracteres. El certificado que se almacena es funcionalmente equivalente al que cargó, con la única diferencia de que la `DescribeCertificate` respuesta mediante el AWS CLI contendrá estos caracteres de nueva línea.

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

Este comando devuelve su firma `CertificateId`. En la siguiente sección, este identificador de certificado se denomina *my-signing-cert-id*.

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


Este comando devuelve el cifrado CertificateId. En la siguiente sección, este identificador de certificado se denomina *my-encrypt-cert-id*.

A continuación, importe los certificados de cifrado y firma de su socio ejecutando los siguientes comandos.

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

Este comando devuelve el cifrado de su socio CertificateId. En la siguiente sección, este identificador de certificado se denomina *partner-encrypt-cert-id*.

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

Este comando devuelve la firma de su socio CertificateId. En la siguiente sección, este identificador de certificado se denomina *partner-signing-cert-id*.

Paso 3: Cree perfiles para usted y su socio comercial

Este procedimiento explica cómo crear perfiles AS2 mediante el uso AWS CLI de. Si en su lugar, desea utilizar la consola Transfer Family, consulte [the section called “Creación de perfiles de AS2”](#).

Ejecute el siguiente comando para crear su perfil AS2 local. Este comando hace referencia a los certificados que contienen sus claves públicas y privadas.

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

Este comando devuelve su ID de perfil. En la siguiente sección, este ID se denomina *my-profile-id*.

Ahora, ejecute el siguiente comando para crear el perfil del socio. Este comando usa solo los certificados de clave pública de su socio. Para usar este comando, sustituya *user input placeholders* por su propia información; por ejemplo, el nombre AS2 y los ID de certificado de su socio.

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

Este comando devuelve el ID de perfil de su socio. En la siguiente sección, este ID se denomina *partner-profile-id*.

Note

En los comandos anteriores, *MYCORP* sustitúyalos por el nombre de su organización y *PARTNER-COMPANY* por el nombre de la organización de su socio comercial.

Paso 4: Crear un servidor Transfer Family que utilice el protocolo AS2

En este procedimiento se explica cómo crear un AS2-enabled servidor mediante Transfer Family AWS CLI.

Note

Muchos de los pasos del ejemplo utilizan comandos que cargan parámetros de un archivo. Para obtener más información sobre el uso de archivos para cargar parámetros, consulte [Cómo cargar parámetros desde un archivo](#).

Si desea utilizar la consola en su lugar, consulte la [Cree un servidor AS2 mediante la consola Transfer Family](#).

De forma similar a como se crea un AWS Transfer Family servidor SFTP o FTPS, se crea un AS2-enabled servidor mediante el `--protocols AS2` parámetro del `create-server` AWS CLI comando. Actualmente, Transfer Family solo admite los tipos de puntos de conexión de VPC y el almacenamiento de Amazon S3 con el protocolo AS2.

Al crear el AS2-enabled servidor para Transfer Family mediante el `create-server` comando, se crea automáticamente un punto final de VPC. Este punto de conexión expone el puerto TCP 5080 para que pueda aceptar mensajes de AS2.

Si desea exponer su punto de conexión de VPC públicamente a Internet, puede asociar direcciones IP elásticas a su punto de conexión de VPC.

Para utilizar estas instrucciones, necesita lo siguiente:

- El ID de su VPC (p. ej., vpc-abcdef01).
- Los ID de las subredes de VPC (p. ej., subnet-abcdef01, subnet-subnet-abcdef01, subnet-021345ab).
- Uno o más identificadores de los grupos de seguridad que permiten el tráfico entrante en el puerto TCP 5080 desde sus socios comerciales (p. ej., sg-1234567890abcdef0 y sg-abcdef01234567890).
- (Opcional) Las direcciones IP elásticas que desea asociar al punto de conexión de VPC.
- Si su socio comercial no está conectado a su VPC a través de una VPN, necesitará una puerta de enlace de Internet. Para más información, consulte [Conectar subredes a Internet por medio de una puerta de enlace de Internet](#) en la Guía del usuario de Amazon VPC.

Para crear un servidor AS2-enabled

1. Ejecute el comando siguiente. Reemplace cada *user input placeholder* por su propia información.

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

2. (Opcional) Puede hacer público el punto de conexión de VPC. Puede adjuntar direcciones IP elásticas a un servidor de Transfer Family solo mediante una operación update-server. Los siguientes comandos detienen el servidor, lo actualizan con direcciones IP elásticas y, a continuación, lo vuelven a iniciar.

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

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

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

Este comando `start-server` crea automáticamente un registro DNS para usted que contiene la dirección IP pública de su servidor. Para que su socio comercial pueda acceder al servidor, debe proporcionarle la siguiente información. En este caso, *your-region* se refiere a su Región de AWS.

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

La URL completa que proporciona a su socio comercial es la siguiente:

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

3. Para comprobar si se puede acceder al AS2-enabled servidor, utilice los siguientes comandos. Asegúrese de que se pueda acceder a su servidor a través de la dirección DNS privada de su punto de conexión de VPC o a través de su punto de conexión público (si asoció una dirección IP elástica a su punto de conexión).

Si el servidor está configurado correctamente, la conexión se realizará correctamente. Sin embargo, recibirá una respuesta con el código de estado HTTP 400 (solicitud incorrecta) si no está enviando un mensaje AS2 válido.

- Para un punto de conexión público (si asoció una dirección IP elástica en el paso anterior), ejecute el siguiente comando, sustituyendo el ID del servidor por la región.

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

- Si se conecta desde su VPC, ejecute los siguientes comandos para buscar el nombre de DNS privado del punto de conexión de VPC.

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

Este comando `describe-server` devuelve el ID del punto de conexión de VPC en el parámetro `VpcEndpointId`. Use este valor para ejecutar el siguiente comando.

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

Este comando `describe-vpc-endpoints` devuelve una matriz `DnsEntries` con varios parámetros `DnsName`. Utilice el nombre DNS regional (el que no incluye la zona de disponibilidad) en el siguiente comando.

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

Por ejemplo, el siguiente comando muestra ejemplos de valores para los marcadores de posición del comando anterior.

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

4. (Opcional) Configurar un rol de registro. Transfer Family registra el estado de los mensajes enviados y recibidos en un formato JSON estructurado en los CloudWatch registros de Amazon. Para proporcionar a Transfer Family acceso a los CloudWatch registros de tu cuenta, debes configurar un rol de registro en tu servidor.

Cree un rol AWS Identity and Access Management (de IAM) en el que confíe `transfer.amazonaws.com` y adjunte la política `AWSTransferLoggingAccess` administrada. Para obtener más información, consulte [Creación de una política y un rol de IAM](#). Anote el Nombre de recurso de Amazon (ARN) del rol de IAM que acaba de crear y asócielo al servidor si ejecuta el siguiente comando `update-server`:

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

Note

Aunque el rol de registro es opcional, le recomendamos que la configure de forma que pueda ver el estado de los mensajes y solucionar los problemas de configuración.

Paso 5: creación de un acuerdo entre usted y su socio

En este procedimiento, se explica cómo crear acuerdos AS2 mediante AWS CLI. Si en su lugar, desea utilizar la consola Transfer Family, consulte [the section called “Cree un acuerdo AS2”](#).

Los acuerdos unen los dos perfiles (local y asociado), sus certificados y una configuración de servidor que permite las transferencias AS2 entrantes entre dos partes. Puede enumerar sus elementos si ejecuta los siguientes comandos.

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

Este paso requiere un bucket de Amazon S3 y un rol de IAM con read/write acceso al bucket y desde él. Las instrucciones para crear este rol son las mismas que las de los protocolos SFTP, FTP y FTPS de Transfer Family y están disponibles en [Creación de una política y un rol de IAM](#).

Para crear un acuerdo, necesita los siguientes elementos:

- El nombre del bucket de Amazon S3 (y el prefijo del objeto, si se ha especificado) para almacenar los archivos AS2. Le recomendamos que especifique directorios independientes para los distintos tipos de archivos.
- El ARN del rol de IAM con acceso al bucket
- Su ID de servidor de Transfer Family
- Su ID de perfil y el ID de perfil de su socio

Guarde el siguiente código en un archivo, por ejemplo, `agreementDetails.json`. Reemplace cada *user input placeholder* por su propia información.

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

 Note

Para utilizar un único directorio base en lugar de directorios independientes, elimine la `CustomDirectories` línea y sus líneas de directorio individuales del código anterior y utilice el siguiente parámetro en su lugar:

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

No utilice un directorio base y parámetros de directorio independientes o el comando fallará.

A continuación, ejecute el siguiente comando.

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

Si se ejecuta correctamente, este comando devolverá el ID del acuerdo. A continuación, puede ver los detalles del acuerdo con el siguiente comando.

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

Paso 6: creación de un conector entre usted y su socio

En este procedimiento, se explica cómo crear conectores AS2 mediante AWS CLI. Si en su lugar, desea utilizar la consola Transfer Family, consulte [the section called "Configure los conectores AS2"](#).

Puede utilizar la operación de API `StartFileTransfer` para enviar archivos almacenados en Amazon S3 al punto de conexión AS2 de su socio comercial mediante un conector. Puede buscar los perfiles que se han creado anteriormente si ejecuta el siguiente comando.

```
aws transfer list-profiles
```

Al crear el conector, debe proporcionar la URL del servidor AS2 de su socio. Copie el siguiente texto en un archivo denominado `testAS2Config.json`.

```
{
  "Compression": "ZLIB",
  "EncryptionAlgorithm": "AES256_CBC",
  "LocalProfileId": "your-profile-id",
  "MdnResponse": "SYNC",
  "MdnSigningAlgorithm": "DEFAULT",
  "MessageSubject": "Your Message Subject",
```

```
"PartnerProfileId": "partner-profile-id",  
"PreserveContentType": "FALSE",  
"SigningAlgorithm": "SHA256"  
}
```

Note

Por EncryptionAlgorithm ejemplo, no especifique el DES_EDE3_CBC algoritmo a menos que sea compatible con un cliente antiguo que lo requiera, ya que se trata de un algoritmo de cifrado débil.

Ejecute el siguiente comando para crear el conector.

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

Paso 7: prueba del intercambio de archivos a través de AS2 mediante Transfer Family

Recibir un archivo de su socio comercial

Si asoció una dirección IP elástica pública a su punto de conexión de VPC, Transfer Family creó automáticamente un nombre DNS que contiene su dirección IP pública. El subdominio es el ID de su AWS Transfer Family servidor (del formatos-1234567890abcdef0). Proporcione la URL de su servidor a su socio comercial en el siguiente formato.

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

Si no asoció una dirección IP elástica pública a su punto de conexión de VPC, busque el nombre de host del punto de conexión de VPC que puede aceptar mensajes de AS2 a través de HTTP POST de sus socios comerciales en el puerto 5080. Para recuperar los detalles del punto de conexión de VPC, utilice el siguiente comando.

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


Por ejemplo, supongamos que el comando anterior devuelve un ID de punto de conexión de VPC de `vpce-1234abcd5678efghi`. A continuación, debe utilizar el siguiente comando para recuperar los nombres de DNS.

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

Este comando devuelve todos los detalles del punto de conexión de VPC que necesita para ejecutar el siguiente comando.

El nombre DNS aparece en la matriz `DnsEntries`. Su socio comercial debe estar dentro de su VPC para acceder a su punto de conexión de VPC (p. ej., a través de AWS PrivateLink o una VPN). Proporcione la URL del punto de conexión de VPC a su socio en el siguiente formato.

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

Por ejemplo, la siguiente URL muestra valores de ejemplo para los marcadores de posición de los comandos anteriores.

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

En este ejemplo, las transferencias correctas se almacenan en la ubicación especificada en el parámetro `base-directory` que especificó en [Paso 5: creación de un acuerdo entre usted y su socio](#). Si recibimos correctamente los archivos con el nombre `myfile1.txt` y `myfile2.txt`, los archivos se almacenan como `/path-defined-in-the-agreement/processed/original_filename.messageId.original_extension`. Aquí, los archivos se almacenan como `/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile1.messageId.txt` y `/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile2.messageId.txt`.

Si configuró una función de registro al crear su servidor Transfer Family, también puede comprobar el estado de los mensajes AS2 en sus CloudWatch registros.

Enviar un archivo a su socio comercial

Puedes usar Transfer Family para enviar mensajes AS2 haciendo referencia al ID del conector y a las rutas de acceso a los archivos, como se muestra en el siguiente comando `start-file-transfer` AWS Command Line Interface (AWS CLI):

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

Para obtener los detalles de los conectores, ejecute el siguiente comando:

```
aws transfer list-connectors
```

El comando `list-connectors` devuelve los ID de los conectores, las URL y los nombres de recursos de Amazon (ARN) de los conectores.

Para devolver las propiedades de un conector concreto, ejecute el siguiente comando con el ID que desee usar:

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

El comando `describe-connector` devuelve todas las propiedades del conector, incluidas la URL, los roles, los perfiles, los avisos de disposición de mensajes (MDNs), las etiquetas y las métricas de supervisión.

Para confirmar que el socio recibió correctamente los archivos, consulte los archivos JSON y MDN. Estos archivos se nombran de acuerdo con las convenciones descritas en [Nombres y ubicaciones de los archivos](#). Si configuró una función de registro al crear el conector, también puede comprobar en sus CloudWatch registros el estado de los mensajes AS2.

Tutorial: Cómo configurar una aplicación web básica de Transfer Family

Este tutorial explica cómo configurar una aplicación web Transfer Family. Las aplicaciones web Transfer Family ofrecen una interfaz sencilla para transferir datos desde y hacia Amazon S3 a través de un navegador web. Para obtener documentación detallada sobre esta función, consulte [Aplicaciones web Transfer Family](#).

Tutorial sobre la aplicación web: requisitos previos

- Cree una instancia de cuenta o una instancia de organización de AWS IAM Identity Center. Para obtener más información, consulte [Configura tu proveedor de identidad para las aplicaciones web Transfer Family](#).

Si no utiliza el Centro de Identidad de IAM como proveedor de identidad, se [Integre Okta como su proveedor de identidad para las aplicaciones web](#) muestra cómo utilizar un proveedor de identidad alternativo (en este caso Okta).

- Necesitas un bucket de Amazon S3 para interactuar con tu aplicación web Transfer Family. Para obtener más información, consulte [Configurar un bucket de Amazon S3](#)

Note

En este tutorial se asume que está utilizando el directorio del Centro de Identidad de IAM como proveedor de identidad. Si no es así, consulte [Configura tu proveedor de identidad para las aplicaciones web Transfer Family](#) antes de continuar con este tutorial.

Tras completar el tutorial, el usuario podrá iniciar sesión e interactuar con la aplicación web que cree.

Paso 1: Cree los recursos de apoyo necesarios

Debe añadir un usuario al directorio del centro de identidad de IAM. También necesita dos funciones: una para usarla como función de portador de identidad para su aplicación web y otra para configurar una concesión de acceso a Amazon S3. En el tutorial, permitimos que AWS los servicios creen estos roles por nosotros.

Para añadir un usuario

1. Inicie sesión en Consola de administración de AWS y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En el panel de navegación izquierdo, selecciona Usuarios.
3. Elija Añadir usuario y especifique los detalles del usuario.

Especifique un nombre de usuario, una dirección de correo electrónico y otra información necesaria. Puedes elegir entre enviar un correo electrónico al usuario con instrucciones para configurar su contraseña o puedes generar una contraseña de un solo uso para compartirla con él.

4. Selecciona Siguiente y, si lo deseas, asigna el nuevo usuario a uno o más grupos.
5. Seleccione Siguiente y revise sus opciones.

Si todo va bien, elija Añadir usuario para crear el nuevo usuario con los detalles que especificó.

Para el tutorial, el usuario de ejemplo es Bob Stiles, con el nombre de usuario bobstiles y la dirección de correo electrónico bobstiles@example.com.

Paso 2: Crear una aplicación web Transfer Family

Para crear una aplicación web Transfer Family

1. Inicia sesión en Consola de administración de AWS y abre la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, selecciona Aplicaciones web.
3. Seleccione Crear aplicación web.

Para el acceso de autenticación, ten en cuenta que el servicio busca automáticamente la AWS IAM Identity Center instancia que configuraste como requisito previo.

4. En el panel de tipos de permisos, selecciona Crear y usar un nuevo rol de servicio. El servicio crea el rol de portador de identidad para usted. Un rol de portador de identidad incluye la identidad de un usuario autenticado en sus sesiones.
5. En el panel de unidades de aplicaciones web, acepte el valor predeterminado de 1 o ajústelo a un valor superior si es necesario.
6. Agregue una etiqueta que le ayude a organizar sus aplicaciones web. Para el tutorial, introduzca el nombre de la clave y la aplicación web Tutorial para el valor.

Tip

Puede editar el nombre de la aplicación web directamente desde la página de la lista de aplicaciones web después de crearla.

7. Seleccione Siguiente para abrir la página Diseño de la aplicación web. En esta pantalla, proporcione la siguiente información.

Si lo desea, puede proporcionar un título para su aplicación web. También puede cargar archivos de imagen para su logotipo y su favicon.

- Para el título de la página, personalice el título de la pestaña del navegador que ven los usuarios cuando se conectan a la aplicación web. Si no escribes nada para el título de la página, el valor predeterminado es Transfer Web App.

- Para el logotipo, sube un archivo de imagen. El tamaño máximo de archivo para la imagen del logotipo es de 50 KB.
- Para el favicon, sube un archivo de imagen. El tamaño máximo de archivo para tu favicon es de 20 KB.

8. Selecciona Siguiente y, a continuación, selecciona Crear aplicación web.

Para ofrecer una experiencia de marca, puedes proporcionar una URL personalizada para que tus usuarios accedan a tu aplicación web Transfer Family. Para obtener más información, consulte [Actualice su terminal de acceso con una URL personalizada](#).

Paso 3: Configura el uso compartido de Cross-origin recursos (CORS) para tu bucket

Debe configurar el uso compartido de recursos entre orígenes (CORS) para todos los depósitos que utilice su aplicación web. Una configuración de CORS es un documento que define las reglas que identifican los orígenes a los que permitirá acceder a su depósito. Para obtener más información sobre CORS, consulte [Configuración del uso compartido de recursos entre orígenes \(CORS\)](#).

Para configurar el uso compartido Cross-origin de recursos (CORS) para su bucket de Amazon S3

1. Inicie sesión en la consola de Amazon S3 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/s3/>.
2. Selecciona Buckets en el panel de navegación izquierdo y busca tu bucket en el cuadro de diálogo de búsqueda y, a continuación, selecciona la pestaña Permisos.
3. En el uso compartido de Cross-origin recursos (CORS), selecciona Editar y pega el siguiente código. **AccessEndpoint** Sustitúyalo por el punto de acceso real de tu aplicación web. Asegúrese de no introducir barras diagonales finales, ya que al hacerlo se producirán errores cuando los usuarios intenten iniciar sesión en su aplicación web.
 - Ejemplo incorrecto: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Ejemplo correcto: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`

Si va a reutilizar un depósito para varias aplicaciones web, añada sus puntos finales de acceso a las aplicaciones web a la lista. AllowedOrigins

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

4. Seleccione Guardar cambios para actualizar el CORS.

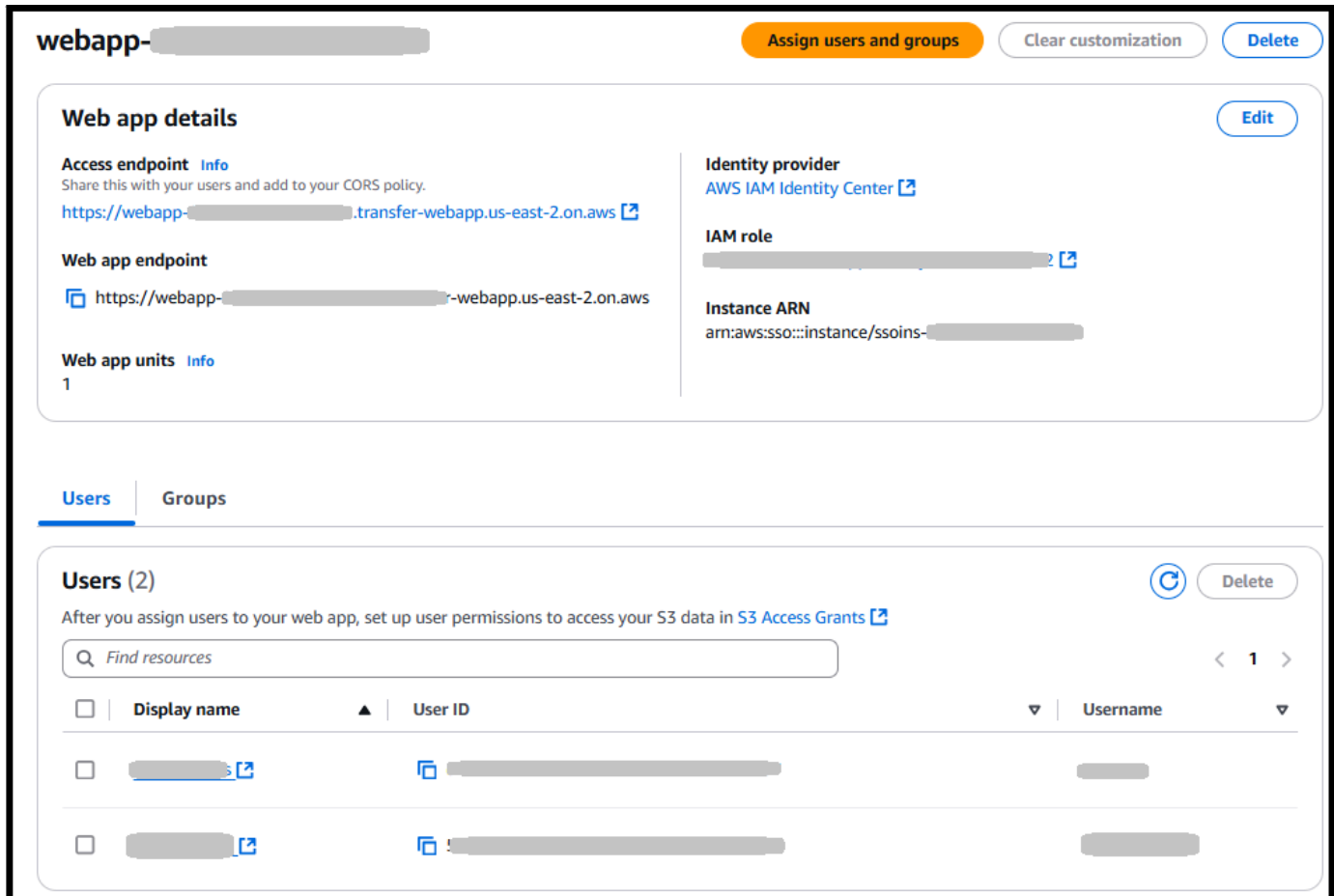
Paso 4: Agrega un usuario a tu aplicación web Transfer Family

Añada el usuario que creó anteriormente en el Centro de identidades de IAM.

Para asignar usuarios a una aplicación web Transfer Family

1. Navega hasta la aplicación web que creaste anteriormente.

2. Elija Asignar usuarios y grupos.



3. Para asignar el usuario que creó anteriormente en el Centro de identidades de IAM, seleccione Asignar usuarios y grupos existentes y, a continuación, seleccione Siguiente.
 - a. Busque el usuario por el nombre para mostrar. Tenga en cuenta que no aparece ningún usuario hasta que comience a introducir los criterios de búsqueda. Para añadir **Bob Stiles**, escribe bob en el cuadro de búsqueda. Si no encuentra a su usuario, vaya a la consola de administración del IAM Identity Center, busque al usuario y, a continuación, copie y pegue aquí su nombre para mostrar.
 - b. Elija el **Bob Stiles** usuario y, a continuación, seleccione Asignar.

Paso 5: Registrar una ubicación en Amazon S3 y crear una concesión de acceso

Después de asignar un usuario a su aplicación web, debe registrar un bucket y crear una concesión de acceso para ese usuario.

 Note

Debe tener una instancia de S3 Access Grants para poder continuar. Para obtener más información, consulte [Crear una instancia de S3 Access Grants](#) en la Guía del usuario de Amazon Simple Storage Service.

Para registrar una ubicación y crear una concesión de acceso

1. Inicie sesión en la consola de Amazon S3 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/s3/>.
2. Seleccione Access Grants en el panel de navegación izquierdo.
3. Seleccione Ver detalles para ver los detalles de su instancia de S3 Access Grants.
4. Seleccione la pestaña Ubicaciones y, a continuación, elija Registrar ubicación.
5. Proporcione la siguiente información.
 - Para el ámbito, busca un depósito o introduce el nombre del depósito y, si lo prefieres, un prefijo. Tenga en cuenta que el ámbito comienza con la cadena **s3://**.
 - Para el rol de IAM, elija Crear nuevo rol para que Amazon S3 cree un rol. Este rol permite a S3 Access Grants acceder al ámbito de ubicación especificado.

Seleccione Registrar ubicación para continuar.

6. Seleccione la pestaña Subvenciones, luego elija Crear subvención y proporcione los siguientes detalles.

- En Ubicación, selecciona Buscar ubicaciones y elige la ubicación que registraste en el paso anterior.
- En Subprefijo, introdúzcalo * para indicar que la concesión de acceso se aplica a todo el depósito.
- Para los permisos, seleccione Leer y escribir.
- Para el tipo de concesionario, elija la identidad del directorio en el Centro de identidades de IAM.
- En el tipo de identidad del directorio, seleccione Usuario.
- En el usuario/ID del IAM Identity Center, copie y pegue el ID de usuario de. **Bob Stiles** Este ID está disponible en el panel Usuarios de la aplicación web Transfer Family.

7. Seleccione Crear subvención.

Se crea la concesión de acceso.

Paso 6: Acceda a su aplicación web Transfer Family como usuario

Ahora, navegamos hasta la URL de la aplicación web e iniciamos sesión como el usuario que asignamos anteriormente.

Para iniciar sesión en la aplicación web Transfer Family

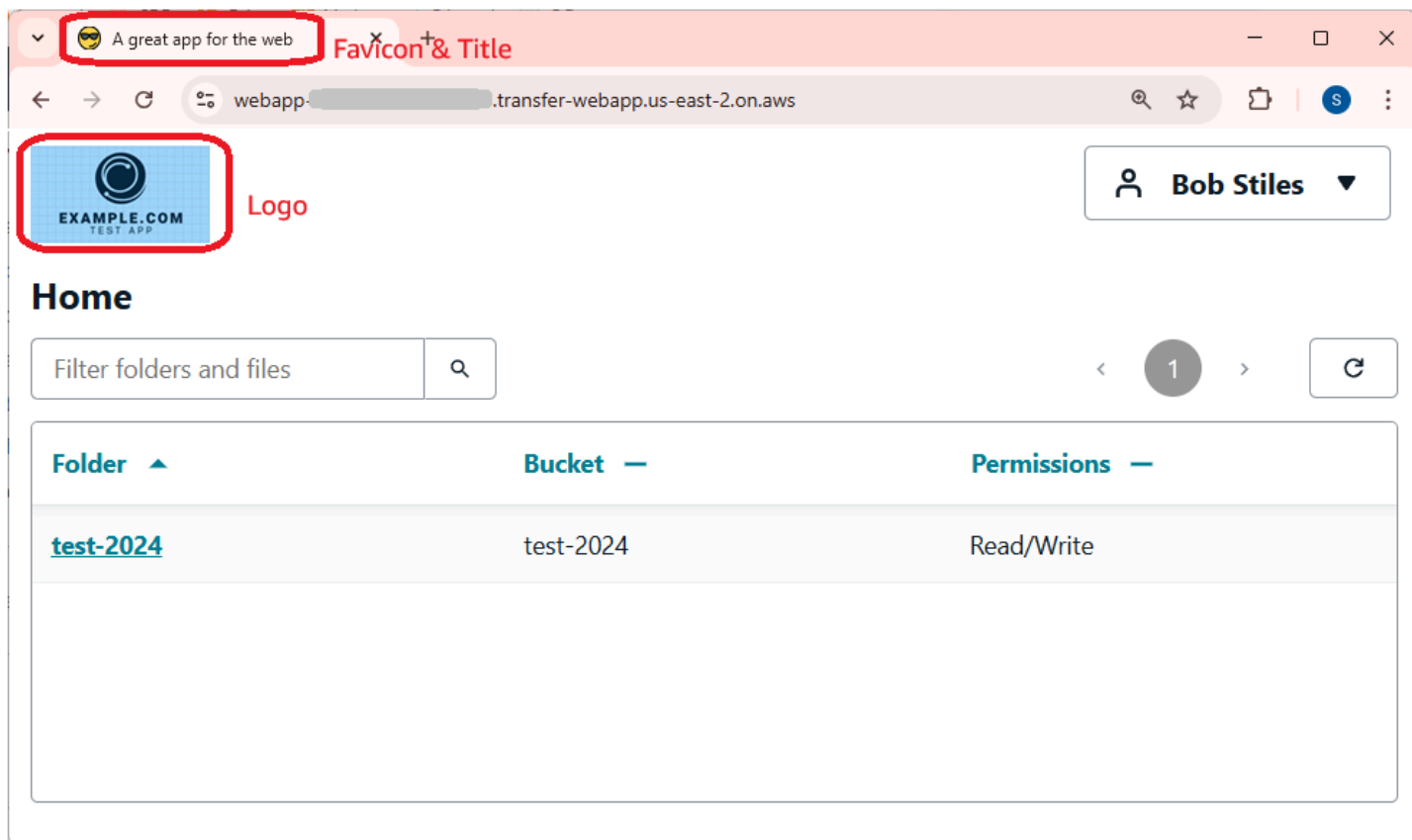
1. Navega hasta tu aplicación web
2. Elija el punto final de acceso en el panel de detalles de la aplicación web.

The screenshot shows the AWS Transfer Family console interface. At the top, there's a header with the text 'webapp-' followed by a redacted ID. To the right are three buttons: 'Assign users and groups' (orange), 'Clear customization' (blue), and 'Delete' (blue). Below this is a 'Web app details' section. On the left side of this section, the 'Access endpoint' is highlighted with a red box; it shows the URL 'https://webapp-[redacted].transfer-webapp.us-east-2.on.aws' with an external link icon. Below it, the 'Web app endpoint' is also shown with the same URL. To the right of the 'Access endpoint' section, there are three fields: 'Identity provider' (AWS IAM Identity Center), 'IAM role' (AWSTransferWebAppIdentityBearer-us-east-2), and 'Instance ARN' (arn:aws:sso::instance/ssoins-[redacted]). Below the 'Web app details' section, there are two tabs: 'Users' (selected) and 'Groups'. Under the 'Users' tab, there's a section titled 'Users (1)' with a 'Delete' button. Below this is a search bar 'Find resources' and a table with columns 'Display name', 'User ID', and 'Username'. The table has one row with a red box around it, showing 'Bob Stiles' as the display name, a redacted User ID, and 'bobstiles' as the username.

3. En la pantalla de inicio de sesión, introduce el usuario que has creado **ybobstiles**, a continuación, selecciona Siguiente.
4. Introduzca la contraseña que el sistema asignó a este usuario al crearlo y seleccione Siguiente.
5. Si su organización requiere la autenticación multifactor (MFA), debe configurarla ahora. Si no es así, vaya al paso 6.
 - a. Aparecerá una pantalla para registrar su dispositivo MFA. Elija una de las opciones disponibles y seleccione Siguiente.

- b. Realice los pasos necesarios para configurar el MFA para este usuario: los pasos dependen de la opción de MFA que elija.
- c. Puede que tenga que establecer una nueva contraseña para su usuario; si es necesario, hágalo ahora. Es posible que el sistema también requiera que vuelva a iniciar sesión con las nuevas credenciales de MFA que configuró.

Su usuario debería ver una pantalla similar a la siguiente. Ten en cuenta que esta captura de pantalla incluye la personalización del favicon y el logotipo.



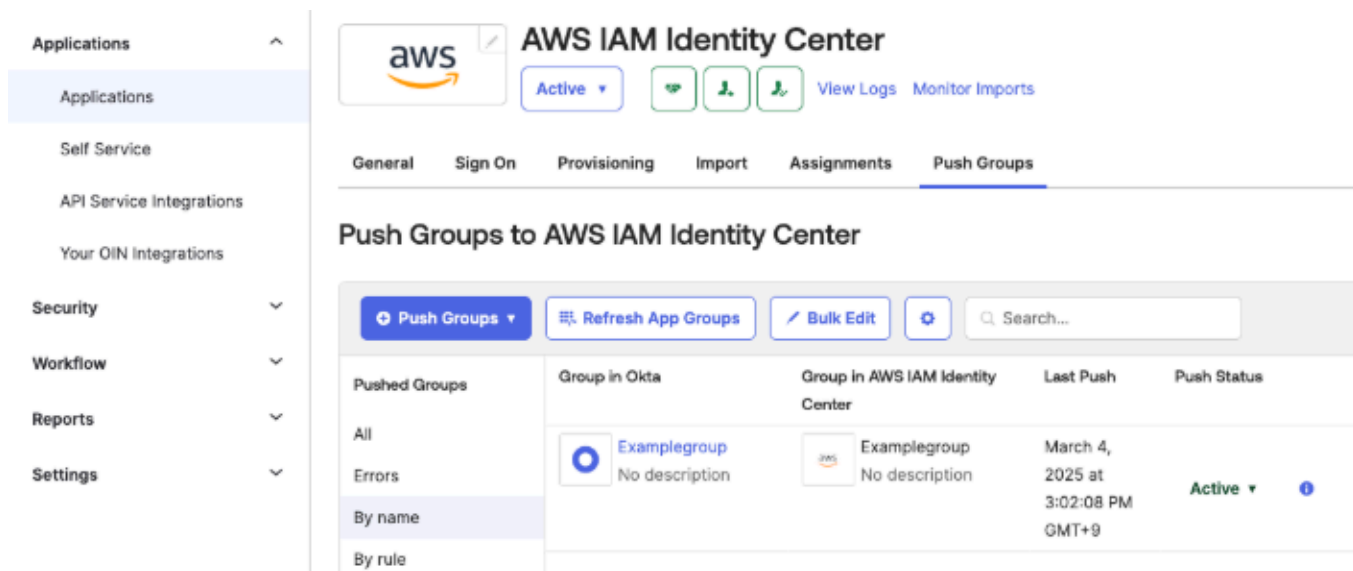
Siguientes pasos

Has configurado correctamente una aplicación web básica de Transfer Family con acceso estándar al bucket S3. Si necesitas un control más detallado de los permisos de los buckets, por ejemplo, permitir a los usuarios descargar de un bucket y subirlos a otro, consulta [Tutorial: Configuración de una aplicación AWS Transfer Family web con acceso selectivo a varios cubos](#).

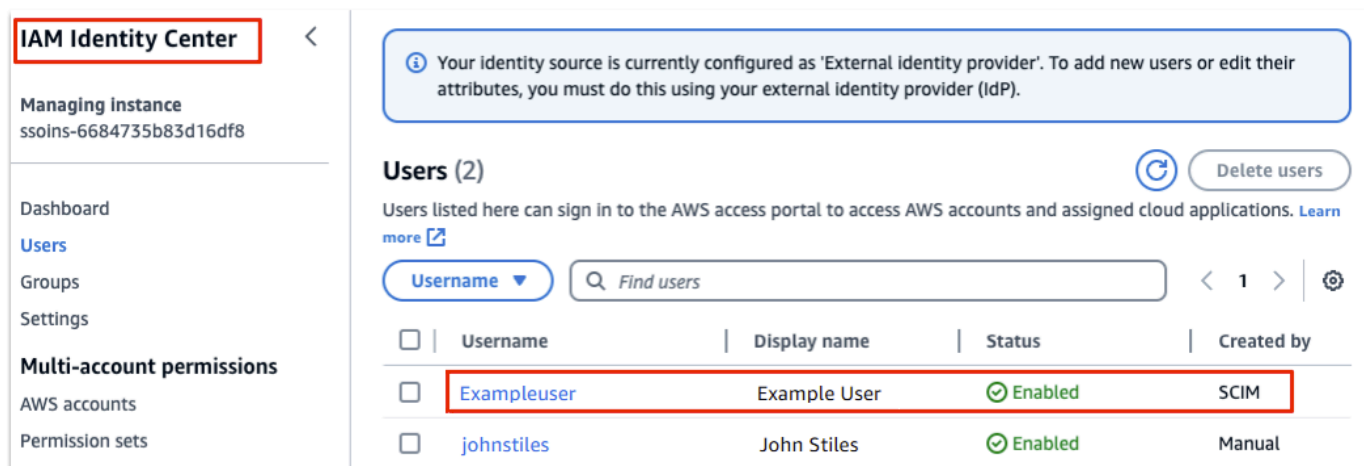
Integre Okta como su proveedor de identidad para las aplicaciones web

Puedes integrar un proveedor de identidad externo con las aplicaciones web Transfer Family. En esta sección, se describe cómo configurar Okta como tu proveedor de identidad.

1. En Okta, crea un usuario, un grupo y una aplicación. Para obtener más información sobre cómo hacerlo, consulte [Configurar SAML y SCIM con Okta e IAM Identity Center](#).



2. Conecta Okta e importa el usuario y el grupo de Okta a AWS IAM Identity Center. Siga los pasos 1 a 4 de [Configurar SAML y SCIM con Okta e IAM Identity Center](#).



IAM Identity Center

Managing instance
ssoins-6684735b83d16df8

Dashboard

Users

Groups

Settings

Multi-account permissions

AWS accounts

Permission sets

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

Groups (2)

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

Find groups by group name

< 1 >

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

3. Confirme que la fuente de identidad del Centro de Identidad de IAM sea SAML 2.0.

Settings

Details

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

Instance name - Edit

Region

US East (Ohio) | us-east-2

Instance ID

ssoins-

Date created

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

Organization ID

AWS Organizations not enabled

Instance ARN

arn:aws:sso:::instance/ssoins-

Identity source

Authentication

Management

Tags

Identity source

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

Identity source

External identity provider

Authentication method

SAML 2.0

Provisioning method

SCIM

AWS access portal URL

[https://.awsapps.com/start](#)

Identity store ID

d-

Issuer URL

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

4. Asigne su usuario y grupo, tal y como se describe en. [Paso 4: Agrega un usuario a tu aplicación web Transfer Family](#)
5. Para evitar que los usuarios tengan que usar MFA al iniciar sesión en su aplicación web, lleve a cabo los siguientes pasos en Okta.
 - a. Desde la consola de administración de Okta, accede a [Aplicaciones] - [Aplicaciones] y selecciona la aplicación. AWS IAM Identity Center
 - b. En la pestaña Iniciar sesión, selecciona [Autenticación de usuario] - Editar.
 - c. Selecciona Solo contraseña.

Después de realizar todos los demás pasos del tutorial, el usuario debería poder acceder a la aplicación web Transfer Family navegando hasta el punto de acceso de la aplicación web en un navegador web.

Tutorial: Configuración de una aplicación AWS Transfer Family web con acceso selectivo a varios cubos

Este tutorial lo guía a través de la configuración de una aplicación web Transfer Family con permisos de bucket específicos de Amazon S3 para un solo usuario. Aprenderá a configurar una solución que permita a los usuarios descargar de un bucket y subirlo a otro, manteniendo la seguridad. Se trata de un tutorial avanzado que se basa en los conceptos incluidos en el tutorial básico. Si eres nuevo en el mundo de las aplicaciones AWS Transfer Family web, considera la posibilidad de empezar con ellas [Tutorial: Cómo configurar una aplicación web básica de Transfer Family](#).

Requisitos previos

Antes de comenzar este tutorial, necesita lo siguiente:

- El centro de identidad de IAM está configurado en la misma región que su aplicación AWS Transfer Family web. Tenga en cuenta que solo se AWS permite una instancia del centro de identidad de IAM por AWS cuenta en todas las regiones.
- Al menos un usuario configurado en el Centro de identidad de IAM.
- Dos depósitos S3: uno para descargas y otro para cargas.

 Note

Este tutorial comparte muchos requisitos previos con el tutorial básico de la aplicación web. Para obtener más información sobre la configuración del Centro de identidades de IAM y la creación de usuarios, consulte. [Tutorial: Cómo configurar una aplicación web básica de Transfer Family](#)

Paso 1: Crear una aplicación web Transfer Family

Para crear una aplicación web Transfer Family

1. Inicia sesión en Consola de administración de AWS y abre la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, selecciona Aplicaciones web.
3. Seleccione Crear aplicación web.

Para el acceso de autenticación, ten en cuenta que el servicio busca automáticamente la AWS IAM Identity Center instancia que configuraste como requisito previo.

4. En el panel de tipos de permisos, selecciona Crear y usar un nuevo rol de servicio. El servicio crea el rol de portador de identidad para usted. Un rol de portador de identidad incluye la identidad de un usuario autenticado en sus sesiones.
5. En el panel de unidades de aplicaciones web, acepte el valor predeterminado de 1 o ajústelo a un valor superior si es necesario.
6. Agregue una etiqueta que le ayude a organizar sus aplicaciones web. Para el tutorial, introduzca el nombre de la clave y la aplicación web Tutorial para el valor.

 Tip

Puede editar el nombre de la aplicación web directamente desde la página de la lista de aplicaciones web después de crearla.

7. Seleccione Siguiente para abrir la página Diseño de la aplicación web. En esta pantalla, proporcione la siguiente información.

Si lo desea, puede proporcionar un título para su aplicación web. También puede cargar archivos de imagen para su logotipo y su favicon.

- Para el título de la página, personalice el título de la pestaña del navegador que ven sus usuarios cuando se conectan a la aplicación web. Si no escribes nada para el título de la página, el valor predeterminado es Transfer Web App.
- Para el logotipo, sube un archivo de imagen. El tamaño máximo de archivo para la imagen del logotipo es de 50 KB.
- Para el favicon, sube un archivo de imagen. El tamaño máximo de archivo para tu favicon es de 20 KB.

8. Selecciona Siguiente y, a continuación, selecciona Crear aplicación web.

Paso 2: Configure las funciones de IAM para el acceso a S3

Debe crear dos funciones de IAM: una con acceso solo para descargas al primer segmento y otra con acceso solo para carga al segundo segmento.

Política de confianza para ambos roles

Utilice la siguiente política de confianza para ambas funciones de IAM:

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


Política de IAM para el depósito de descargas

Cree un rol de IAM con la siguiente política para el acceso de solo lectura a su depósito de descargas:

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

Important

Sustituya amzn-s3-demo-bucket1 por el nombre real del depósito de descargas.

Política de IAM para el depósito de carga

Crea otro rol de IAM con la siguiente política para el acceso de escritura a tu depósito de carga:

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

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

Important

Sustituya amzn-s3-demo-bucket2 por el nombre real del depósito de carga.

Paso 3: Configura S3 Access Grants

1. Abra la consola S3 en <https://console.aws.amazon.com/s3/>.
2. En el panel de navegación, elija Access Grants.
3. Haga clic en Crear instancia de S3 Access Grants.
4. Seleccione la opción Añadir instancia del centro de identidad de IAM e introduzca el ARN de la instancia del centro de identidad.
5. Haga clic en Siguiente y, a continuación, en Cancelar para terminar de crear la instancia de S3 Access Grants sin continuar con los pasos adicionales.

Este paso crea la instancia de S3 Access Grants. Ahora registrará las ubicaciones y creará las concesiones de acceso.

Paso 4: Registrar las ubicaciones de los depósitos de S3

Registre ambos depósitos de S3 como ubicaciones con S3 Access Grants:

1. En la consola de S3 Access Grants, vaya a Ubicaciones y haga clic en Registrar ubicación.
2. En Ámbito de ubicación, elija el depósito de S3 específico para las descargas (amzn-s3-demo-bucket1).
3. Cuando se le pida que elija un rol de IAM, seleccione el rol de IAM de descarga que creó anteriormente.
4. Complete el proceso de registro.
5. Repita el proceso para registrar el depósito de carga (amzn-s3-demo-bucket2) y seleccione la función de IAM de carga cuando se le solicite.

Paso 5: Crear concesiones de acceso

Crea dos subvenciones, una para cada ubicación registrada:

1. En la consola de S3 Access Grants, vaya a Grants y haga clic en Crear concesión.
2. En Ubicación, haga clic en Buscar ubicación y seleccione la ubicación del depósito de descargas (amzn-s3-demo-bucket1).
3. En Subprefijo (opcional), introduzca * para permitir el acceso a todo el depósito o especifique una ruta para restringir el acceso a un prefijo específico. `folder1/folder2/*`

Si * se utiliza, se establecerá el alcance de la concesión en `s3://bucket-name/*`, lo que permitirá el acceso a todo el depósito. Para permitir el acceso solo a un prefijo específico, introduce una ruta como `folder1/folder2/*`, por ejemplo, que definirá el alcance de la concesión. `s3://bucket-name/folder1/folder2/*`

4. En Permisos y acceso, selecciona Leer para el segmento de descargas.
5. En Tipo de concesionario, elija la identidad del directorio en el Centro de identidades de IAM.
6. Para el tipo principal de IAM, seleccione Usuario e introduzca el seudónimo de su usuario del Centro de Identidad de IAM.
7. Complete el proceso de creación de la subvención.
8. Repite el proceso para crear una concesión para el depósito de carga (amzn-s3-demo-bucket2), pero selecciona los permisos. Read-write

Paso 6: Configure la política CORS para los buckets S3

Configure una política CORS para ambos buckets de S3 para permitir el acceso a través de: AWS Transfer Family WebApp

1. Abre la consola S3 y navega hasta tu depósito de descargas (amzn-s3-demo-bucket1).
2. Seleccione la pestaña Permisos.
3. Desplázate hacia abajo hasta la sección de uso compartido de Cross-origin recursos (CORS) y haz clic en Editar.
4. Añada la siguiente configuración de CORS y sustitúyala por la *WebAppEndpoint* URL de su WebApp terminal actual:

Puede encontrar la URL del punto de conexión de su aplicación web en la AWS Transfer Family consola de abajo WebApps. Tendrá un aspecto similar a `https://webapp-*****.transfer-webapp.us-west-2.on.aws`.

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

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

5. Haga clic en Guardar cambios.
6. Repite el proceso para tu depósito de carga (amzn-s3-demo-bucket2).

Paso 7: Probar la configuración

1. Abre la URL de tu aplicación AWS Transfer Family web. Puedes encontrar esta URL en la AWS Transfer Family consola, WebApps en el campo Punto final de acceso.
2. Inicie sesión con las credenciales de usuario del IAM Identity Center que configuró con las concesiones de acceso.
3. Tras iniciar sesión, debería ver las dos ubicaciones de S3 en la página de inicio.
4. Navegue hasta el depósito de descargas (amzn-s3-demo-bucket1) y compruebe que puede descargar archivos pero no subirlos.
5. Navegue hasta el depósito de carga (amzn-s3-demo-bucket2) y compruebe que puede cargar archivos.

Conclusión

Ha configurado correctamente el acceso selectivo al bucket de S3 para un solo AWS Transfer Family WebApp usuario. Esta configuración permite al usuario descargar contenido de un depósito y subirlo a otro, manteniendo la seguridad mediante funciones de IAM y S3 Access Grants.

Este enfoque se puede extender a varios usuarios mediante la creación de concesiones adicionales en S3 Access Grants para cada usuario, lo que permite un control pormenorizado de los permisos de acceso al bucket. Para obtener información sobre la configuración básica de la aplicación web, consulte [Tutorial: Cómo configurar una aplicación web básica de Transfer Family](#).

Configuración de un punto final de servidor SFTP, FTPS o FTP

En este tema se proporcionan detalles sobre la creación y el uso de puntos finales de AWS Transfer Family servidor que utilizan uno o varios de los protocolos SFTP, FTPS y FTP.

Temas

- [Opciones de proveedor de identidades](#)
- [AWS Transfer Family matriz de tipos de punto final](#)
- [Configuración de un punto final de servidor SFTP, FTPS o FTP](#)
- [Consideraciones sobre el Network Load Balancer para FTP y FTPS](#)
- [Transferencia de archivos a través de un punto de conexión mediante un cliente](#)
- [Administración de usuarios para puntos finales de servidor](#)
- [Uso de directorios lógicos para simplificar las estructuras de directorios de Transfer Family](#)
- [Acceda a sus sistemas de archivos FSx para NetApp ONTAP con Transfer Family](#)

Opciones de proveedor de identidades

AWS Transfer Family proporciona varios métodos para autenticar y administrar usuarios. En la siguiente tabla, se comparan los proveedores de identidad disponibles que puede usar con Transfer Family.

Action	AWS Transfer Family servicio gestionado	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
Protocolos admitidos	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
Key-based authentication	Sí	No	Sí	Sí
Autenticación de contraseña	No	Sí	Sí	Sí

Action	AWS Transfer Family servicio gestionado	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
AWS Identity and Access Management (IAM) y POSIX	Sí	Sí	Sí	Sí
Directorio de inicio lógico	Sí	Sí	Sí	Sí
Acceso parametrizado (basado en el nombre de usuario)	Sí	Sí	Sí	Sí
Estructura de acceso ad hoc	Sí	No	Sí	Sí
AWS WAF	No	No	Sí	No

Notas:

- IAM se usa para controlar el acceso al almacenamiento de respaldo de Amazon S3 y POSIX se usa para Amazon EFS.
- Ad hoc se refiere a la capacidad de enviar el perfil de usuario en tiempo de ejecución. Por ejemplo, puede colocar a los usuarios en sus directorios principales pasando el nombre de usuario como variable.
- Para obtener más información al respecto AWS WAF, consulte. [Agregue un cortafuegos de aplicaciones web](#)
- Hay una entrada de blog que describe el uso de una función Lambda integrada con Microsoft Entra ID (anteriormente Azure AD) como proveedor de identidad de Transfer Family. Para obtener más información, consulte [Autenticación AWS Transfer Family con Azure Active Directory](#) y. AWS Lambda

- Proporcionamos varias CloudFormation plantillas para ayudarlo a implementar rápidamente un servidor Transfer Family que utilice un proveedor de identidad personalizado. Para obtener más información, consulte [Plantillas de función de Lambda](#).

En los siguientes procedimientos, puede crear un SFTP-enabled servidor, FTPS-enabled un FTP-enabled servidor o un AS2-enabled servidor.

Paso siguiente

- [Crea un SFTP-enabled servidor](#)
- [Cree un FTPS-enabled servidor](#)
- [Cree un servidor FTP-enabled](#)
- [Configuración de AS2](#)

AWS Transfer Family matriz de tipos de punto final

Cuando cree un servidor de Transfer Family, seleccione el tipo de punto de conexión que va a utilizar. En la siguiente tabla se describen las características de cada tipo de punto de conexión.

Matriz de tipos de punto de conexión

Característica	Público	VPC: internet	VPC: interna	VPC_Endpoint (obsoleta)
Protocolos admitidos	SFTP	SFTP, FTPS, AS2	SFTP, FTP, FTPS, AS2	SFTP
Acceso	Desde Internet. Este tipo de punto de conexión no requiere ninguna configuración especial en la VPC.	A través de Internet y desde una VPC y VPC-connected entornos, como un centro de datos local a través Direct Connect de una VPN.	Desde una VPC y VPC-connected entornos, como un centro de datos local a través Direct Connect de una VPN.	Desde una VPC y VPC-connected entornos, como un centro de datos local a través Direct Connect de una VPN.

Característica	Público	VPC: internet	VPC: interna	VPC_Endpoint (obsoleta)
Direcciones IP estáticas	No puedes adjuntar una dirección IP estática. AWS proporciona direcciones IP que están sujetas a cambios.	Puede adjuntar direcciones IP elásticas al punto de conexión. Pueden ser direcciones IP propias de AWS o sus propias direcciones IP (Traer sus propias direcciones IP). Las direcciones IP elásticas adjuntas al punto de conexión no cambian. Las direcciones IP privadas adjuntas al servidor tampoco cambian.	Las direcciones IP privadas adjuntas al punto de conexión no cambian.	Las direcciones IP privadas adjuntas al punto de conexión no cambian.

Característica	Público	VPC: internet	VPC: interna	VPC_Endpoint (obsoleta)
Lista de direcciones IP de origen permitidas	Este tipo de punto de conexión no admite listas de permisos por direcciones IP de origen. El punto de conexión es de acceso público y escucha el tráfico a través del puerto 22.  Note Para VPC-hosted los puntos finales, los servidores SFTP Transfer Family pueden funcionar a través del puerto 22 (el	Para permitir el acceso mediante la dirección IP de origen, puede utilizar grupos de seguridad conectados a los puntos de conexión del servidor y las ACL de red conectadas a la subred en la que se encuentra el punto de conexión.	Para permitir el acceso mediante la dirección IP de origen, puede utilizar grupos de seguridad conectados a los puntos de conexión del servidor y la lista de control de acceso de la red (ACL de la red) conectadas a la subred en la que se encuentra el punto de conexión.	Para permitir el acceso mediante la dirección IP de origen, puede utilizar grupos de seguridad conectados a los puntos de conexión del servidor y las ACL de red conectadas a la subred en la que se encuentra el punto de conexión.

Característica	Público	VPC: internet	VPC: interna	VPC_Endpoint (obsoleta)
	predeterminado), 2222, 2223 o 22000.			
Lista de firewalls de clientes permitidos	Debe permitir el nombre DNS del servidor. Como las direcciones IP están sujetas a cambios, evite utilizarlas en la lista de direcciones IP permitidas por el firewall de su cliente.	Puede permitir el nombre DNS del servidor o las direcciones IP elásticas adjuntas al servidor.	Puede permitir las direcciones IP privadas o el nombre DNS de los puntos de conexión.	Puede permitir las direcciones IP privadas o el nombre DNS de los puntos de conexión.
Tipo de dirección IP	IPv4 (predeterminado) o de doble pila (IPv4 e IPv6)	Solo IPv4 (no se admite la doble pila)	IPv4 (predeterminado) o de doble pila (IPv4 e IPv6)	Solo IPv4 (no se admite la doble pila)

Note

El tipo de VPC_ENDPOINT puntos de conexión ahora está en desuso y no puede ser utilizado para crear nuevos servidores. En lugar de usarlo `EndpointType=VPC_ENDPOINT`, use el tipo de punto final de VPC (`EndpointType=VPC`), que puede usar como interno o orientado a Internet, como se describe en la tabla anterior.

- Para obtener más información sobre la obsolescencia, consulte. [Suspender el uso de VPC_ENDPOINT](#)

- Para obtener información sobre la administración de los permisos de punto final de la VPC, consulte. [Limitar el acceso a los terminales de VPC para los servidores Transfer Family](#)

Tenga en cuenta las siguientes opciones para aumentar la seguridad de su servidor AWS Transfer Family :

- Utilice un punto de enlace de VPC con acceso interno, de modo que solo puedan acceder al servidor los clientes de su VPC o VPC-connected entornos, como un centro de datos local a través de una VPN. Direct Connect
- Para permitir que los clientes accedan al punto de conexión a través de Internet y proteger su servidor, utilice un punto de conexión de VPC con acceso a Internet. A continuación, modifique los grupos de seguridad de la VPC para permitir el tráfico únicamente desde determinadas direcciones IP que alojan los clientes de sus usuarios.
- Si necesita una autenticación basada en contraseñas y utiliza un proveedor de identidad personalizado en el servidor, se recomienda que su política de contraseñas impida que los usuarios creen contraseñas poco seguras y limite el número de intentos fallidos de inicio de sesión.
- AWS Transfer Family es un servicio gestionado, por lo que no proporciona acceso desde una consola. No puede acceder directamente al servidor SFTP subyacente para ejecutar comandos nativos del sistema operativo en los servidores de Transfer Family.
- Use un Equilibrador de carga de red frente a un punto de conexión de VPC con acceso interno. Cambie el puerto oyente del equilibrador de carga del puerto 22 a un puerto diferente. Esto puede reducir, pero no eliminar, el riesgo de que los escáneres de puertos y los bots inspeccionen el servidor, ya que el puerto 22 es el más utilizado para escanear. Para obtener más información, consulta la entrada del blog Los [balanceadores de carga de red ahora admiten grupos de seguridad](#).

 Note

Si usa un Network Load Balancer, los AWS Transfer Family CloudWatch registros muestran la dirección IP del NLB, en lugar de la dirección IP real del cliente.

Configuración de un punto final de servidor SFTP, FTPS o FTP

Puede crear un servidor de transferencia de archivos mediante el servicio. AWS Transfer Family. Están disponibles los siguientes protocolos de transferencia de archivos:

- Protocolo de File Transfer (SFTP) Secure Shell (SSH): File Transfer a través de SSH. Para obtener más información, consulte [the section called “Crea un SFTP-enabled servidor”](#).

Note

Proporcionamos un AWS CDK ejemplo para crear un servidor SFTP Transfer Family. El ejemplo usa TypeScript y está disponible GitHub [aquí](#).

- Protocolo seguro de File Transfer (FTPS): File Transfer con cifrado TLS. Para obtener más información, consulte [the section called “Crea un FTPS-enabled servidor”](#).
- Protocolo de File Transfer (FTP): File Transfer sin cifrar. Para obtener más información, consulte [the section called “Crea un FTP-enabled servidor”](#).
- Declaración de aplicabilidad 2 (AS2): File Transfer para transportar datos estructurados de empresa a empresa. Para obtener más información, consulte [the section called “Configurar AS2”](#). Para AS2, puede crear rápidamente una CloudFormation pila con fines de demostración. Este procedimiento se describe en [Uso de una plantilla para crear una pila AS2 de Transfer Family de demostración](#).

Puede crear un servidor con varios protocolos.

Note

Si tiene varios protocolos habilitados para el mismo punto de conexión del servidor y desea proporcionar acceso con el mismo nombre de usuario en varios protocolos, puede hacerlo siempre que las credenciales específicas del protocolo estén configuradas en su proveedor de identidad. En el caso del FTP, se recomienda mantener credenciales independientes de las de SFTP y FTPS. Esto se debe a que, a diferencia de SFTP y FTPS, el FTP transmite las credenciales en texto no cifrado. Al aislar las credenciales de FTP de las de SFTP o FTPS, si las credenciales de FTP se comparten o están expuestas, las cargas de trabajo que utilizan SFTP o FTPS permanecen seguras.

Al crear un servidor, se elige uno específico Región de AWS para realizar las solicitudes de operación de archivos de los usuarios que están asignados a ese servidor. Además de asignar al servidor uno o más protocolos, también se asigna uno de los siguientes tipos de proveedores de identidad:

- Servicio administrado mediante claves SSH. Para obtener más información, consulte [Trabajar con usuarios de servicios administrados](#).
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Este método le permite integrar los grupos de Microsoft Active Directory para proporcionar acceso a los servidores de Transfer Family. Para obtener más información, consulte [Uso AWS de Directory Service para Microsoft Active Directory](#).
- Un proveedor de identidades personalizado. Transfer Family ofrece varias opciones para usar un proveedor de identidad personalizado, tal y como se describe en el [Uso de proveedores de identidad personalizados](#) tema.

También puede asignar al servidor un tipo de punto de conexión (de acceso público o alojado en una VPC) y un nombre de host mediante el punto de conexión del servidor predeterminado, o un nombre de host personalizado mediante el servicio Amazon Route 53 o mediante un servicio de sistema de nombres de dominio (DNS) de su elección. El nombre de host de un servidor debe ser único en el Región de AWS lugar donde se creó.

Además, puede asignar una función de CloudWatch registro de Amazon para enviar eventos a sus CloudWatch registros, elegir una política de seguridad que contenga los algoritmos criptográficos que su servidor puede utilizar y añadir metadatos al servidor en forma de etiquetas que son pares clave-valor.

 Important

Los costos incurridos se calculan por los servidores instanciados y por la transferencia de datos. Para obtener información sobre los precios y Calculadora de precios de AWS para obtener una estimación del costo de usar Transfer Family, consulta [AWS Transfer Family los precios](#).

Crea un SFTP-enabled servidor

El protocolo de File Transfer (SFTP) Secure Shell (SSH) es un protocolo de red que se utiliza para la transferencia segura de datos a través de Internet. El protocolo es compatible con todas las funciones de seguridad y autenticación de SSH. Se utiliza ampliamente para intercambiar datos, incluida información confidencial, entre socios comerciales de diversos sectores, como los servicios financieros, sanitarios, el comercio minorista y la publicidad.

Tenga en cuenta lo siguiente

- Los servidores SFTP de Transfer Family funcionan a través del puerto 22. Para los VPC-hosted puntos finales, los servidores SFTP Transfer Family también pueden funcionar a través de los puertos 2222, 2223 o 22000. Para obtener más información, consulte [Creación de un servidor en una nube privada virtual \(VPC\)](#).
- Los puntos finales públicos no pueden restringir el tráfico a través de grupos de seguridad. Para usar grupos de seguridad con su servidor Transfer Family, debe alojar el punto final de su servidor en una nube privada virtual (VPC), como se describe en [Creación de un servidor en una nube privada virtual \(VPC\)](#)

Véase también

- Proporcionamos un AWS CDK ejemplo para crear un servidor SFTP Transfer Family. El ejemplo usa TypeScript y está disponible GitHub [aquí](#).
- Para ver un tutorial sobre cómo implementar un servidor Transfer Family dentro de una VPC, [consulta la lista de direcciones IP permitidas para proteger AWS Transfer Family](#) tus servidores.

Para crear un servidor SFTP-enabled

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/> y seleccione Servidores en el panel de navegación y, a continuación, elija Crear servidor.
2. En Elegir protocolos, seleccione SFTP y, a continuación, Siguiente.
3. En Elegir un proveedor de identidad, seleccione el proveedor de identidad que desee utilizar para administrar el acceso de los usuarios. Dispone de las opciones siguientes:
 - Servicio gestionado: se almacenan las identidades y claves de los usuarios AWS Transfer Family.

- AWS Directory Service for Microsoft Active Directory: proporcione un directorio Directory Service para acceder al punto de conexión. Si lo hace, puede utilizar las credenciales almacenadas en el Active Directory para autenticar a los usuarios. Para obtener más información sobre cómo trabajar con proveedores de AWS Managed Microsoft AD identidades, consulte [Uso AWS de Directory Service para Microsoft Active Directory](#).

 Note

- Cross-Account y no se admiten los directorios compartidos AWS Managed Microsoft AD.
 - Para configurar un servidor con Directory Service como proveedor de identidad, debe añadir algunos Directory Service permisos. Para obtener más información, consulte [Antes de empezar a usar AWS Directory Service for Microsoft Active Directory](#).
- Proveedor de identidad personalizado: seleccione cualquiera de las siguientes opciones:
 - Úselo AWS Lambda para conectar su proveedor de identidad: puede usar un proveedor de identidad existente, respaldado por una función Lambda. Proporcione el nombre de identificación de la función de Lambda. Para obtener más información, consulte [Se utiliza AWS Lambda para integrar su proveedor de identidad](#).
 - Utilice Amazon API Gateway para conectar su proveedor de identidades: puede crear un método de API Gateway respaldado por una función de Lambda para usarlo como proveedor de identidades. Proporcione una URL de Amazon API Gateway y un rol de invocación. Para obtener más información, consulte [Uso de Amazon API Gateway para integrar su proveedor de identidad](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

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

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

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

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

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

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

AWS Lambda function





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

☒ **Password OR public key**

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

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

Cancel Previous Next

4. Elija Siguiente.
5. En Elegir punto de conexión, haga lo siguiente:
 - a. En el tipo de punto de conexión, seleccione el tipo de punto de conexión de acceso público. Para ver un punto de conexión alojado en una VPC, consulte [Creación de un servidor en una nube privada virtual \(VPC\)](#).
 - b. Para el tipo de dirección IP, elija IPv4 (predeterminado) para garantizar la compatibilidad con versiones anteriores o Dual-stack para habilitar las conexiones IPv4 e IPv6 con su terminal.

 Note

Dual-stack El modo permite que su terminal Transfer Family se comuniquen con clientes habilitados para IPv4 e IPv6. Esto le permite realizar una transición gradual de sistemas basados en IPv4 a sistemas basados en IPv6 sin necesidad de cambiar todos a la vez.

- c. (Opcional) Para un nombre de host personalizado, seleccione Ninguno.

Obtendrá un nombre de servidor proporcionado por. AWS
Transfer Family El nombre de host del servidor tiene la forma
`serverId.server.transfer.regionId.amazonaws.com`.

En el caso de un nombre de host personalizado, debe especificar un alias personalizado para el punto de conexión del servidor. Para obtener más información sobre el uso de nombres de host personalizados, consulte [Uso de nombres de host personalizados](#).

- d. (Opcional) En el caso del dispositivo con FIPS activado, active la casilla de verificación del punto de conexión con FIPS activado para asegurarse de que el dispositivo de punto final cumpla con las normas federales de procesamiento de información (FIPS).

 Note

FIPS-enabled Los puntos finales solo están disponibles en las regiones de Norteamérica AWS . Para obtener una lista de las regiones disponibles, consulte los [puntos de conexión y cuotas de AWS Transfer Family](#) en Referencia general de AWS. Para obtener más información acerca del FIPS, consulte [Estándar federal de procesamiento de la información \(FIPS\) 140-2](#) .

- e. Elija Siguiente.
6. En la página Elegir dominio, elige el servicio AWS de almacenamiento que desees usar para almacenar tus datos y acceder a ellos a través del protocolo seleccionado:
- Seleccione Amazon S3 para almacenar sus archivos y acceder a ellos como objetos a través del protocolo seleccionado.
 - Seleccione Amazon EFS para almacenar los archivos del sistema de archivos de Amazon EFS y acceder a ellos a través del protocolo seleccionado.

Elija Siguiente.

7. En Configurar detalles adicionales, haga lo siguiente:

- a. Para el registro, especifique un grupo de registro de ya existente o cree uno nuevo (la opción predeterminada). Si elige un grupo de registros existente, debe seleccionar uno que esté asociado al suyo Cuenta de AWS.

Si elige Crear grupo de registros, la CloudWatch consola (<https://console.aws.amazon.com/cloudwatch/>) se abre en la página Crear grupo de registros. Para obtener más información, consulte [Crear un grupo de CloudWatch registros en Logs](#).

- b. (Opcional) Para los flujos de trabajo administrados, elija los ID de flujo de trabajo (y el rol correspondiente) que Transfer Family debe asumir al ejecutar el flujo de trabajo. Puede elegir un flujo de trabajo para ejecutarlo tras una carga completa y otro para ejecutarlo tras una carga parcial. Para obtener más información sobre el procesamiento de los archivos mediante flujos de trabajo administrados, consulte [AWS Transfer Family flujos de trabajo gestionados](#).

Managed workflows [Info](#)

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

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

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

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

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

[dropdown] [refresh]

- c. Para ver las opciones de algoritmos criptográficos, elija una política de seguridad que contenga los algoritmos criptográficos habilitados para su uso en el servidor. Nuestra política de seguridad más reciente es la predeterminada: para obtener más información, consulte [Políticas de seguridad para AWS Transfer Family servidores](#).
- d. (Opcional) Para la clave de host del servidor, introduzca una clave privada RSA, ED25519 o ECDSA que se va a utilizar para identificar el servidor cuando los clientes se conecten a él a través de SFTP. También, puede agregar una descripción para diferenciar entre varias claves de host.

Tras crear el servidor, puede añadir claves de host adicionales. Tener varias claves de host es útil si desea rotar las claves o si desea tener diferentes tipos de claves, como una clave RSA y también una clave ECDSA.

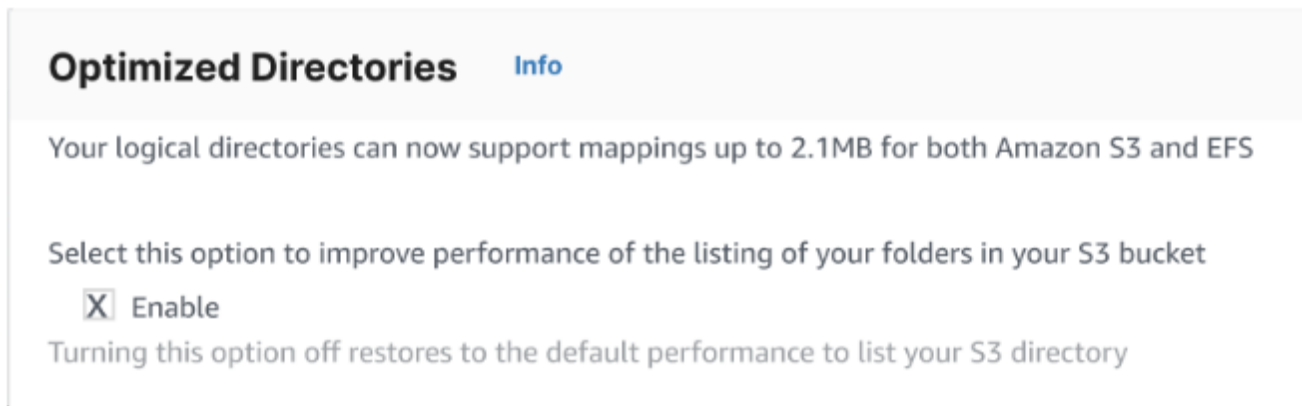
Note

La sección Server Host Key se usa solo para migrar usuarios desde un SFTP-enabled servidor existente.

- e. (Opcional) En el caso de las etiquetas, en Clave y valor, introduzca una o más etiquetas como pares de valores clave y, a continuación, seleccione Añadir etiqueta.
- f. Elija Siguiente.
- g. Puede optimizar el rendimiento de sus directorios de Amazon S3. Por ejemplo, supongamos que va a su directorio principal y tiene 10 000 subdirectorios. En otras palabras, su bucket de Amazon S3 tiene 10 000 carpetas. En este escenario, si ejecuta el comando `ls` (list), la

operación de lista tarda entre seis y ocho minutos. Sin embargo, si optimiza los directorios, esta operación solo tardará unos segundos.

Al crear el servidor mediante la consola, los directorios optimizados están habilitados de forma predeterminada. Si crea el servidor mediante la API, este comportamiento no está habilitado de forma predeterminada.



- h. (Opcional) Configure AWS Transfer Family los servidores para que muestren mensajes personalizados, como políticas organizativas o términos y condiciones, a sus usuarios finales. En Mostrar banner, en el cuadro de texto del banner de Pre-authentication visualización, introduzca el mensaje de texto que desee mostrar a los usuarios antes de que se autenticquen.
- i. (Opcional) Puede configurar las siguientes opciones adicionales.
 - SetStat opción: active esta opción para ignorar el error que se genera cuando un cliente intenta usarlo SETSTAT en un archivo que está cargando en un bucket de Amazon S3. Para obtener más información, consulte la SetStatOption documentación de [ProtocolDetails](#).
 - Reanudación de la sesión TLS: esta opción solo está disponible si ha habilitado el FTPS como uno de los protocolos de este servidor.
 - Passive IP: esta opción solo está disponible si ha habilitado el FTPS o FTP como uno de los protocolos de este servidor.

Additional configuration

SetStat option - *optional* [Info](#)

Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - *optional* [Info](#)

Choose how you want your server to process TLS session resumption requests

☒ Enforce

☐ Enable

☐ Disable

 To enable TLS session resumption, enable FTPS as one of the protocols selected in Step 1

Passive IP - *optional* [Info](#)

Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

 To enable Passive IP, enable FTP or FTPS as one of the protocols selected in Step 1

8. En Revisar y crear, revise sus opciones.

- Si desea editar alguno de ellos, seleccione Editar junto al paso.

Note

Debe revisar cada paso después del paso que eligió editar.

- Si no ha realizado cambios, seleccione Crear servidor para crear el suyo. Así llegará a la página Servers (Servidores), mostrada a continuación, donde ya aparece el nuevo servidor.

Pueden transcurrir algunos minutos antes de que el estado del nuevo servidor cambie a Online. En ese momento, el servidor podrá realizar operaciones con los archivos, pero primero tendrá que crear

un usuario. Para obtener más información sobre la creación de usuarios, consulte [Administración de usuarios para puntos finales de servidor](#).

Cree un FTPS-enabled servidor

El Protocolo de File Transfer a través de SSL (FTPS) es una extensión del FTP. Utilice los protocolos criptográficos de seguridad de la capa de transporte (TLS) y Secure Sockets Layer (SSL) para cifrar el tráfico. El FTPS permite el cifrado de las conexiones del canal de datos y de control de forma simultánea o independiente.

Note

Para obtener información importante sobre los balanceadores de carga de red, consulte [Evite colocar los NLB y los NAT delante de AWS Transfer Family servidores](#).

Para crear un servidor FTPS-enabled

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/> y seleccione Servidores en el panel de navegación y, a continuación, elija Crear servidor.
2. En Elegir protocolos, seleccione FTPS.

En el caso del certificado de servidor, elija un certificado almacenado en AWS Certificate Manager (ACM) que se utilizará para identificar el servidor cuando los clientes se conecten a él a través de FTPS y, a continuación, seleccione Siguiente.

Para solicitar un nuevo certificado público, consulte [Solicitar un certificado público](#) en la Guía del usuario de AWS Certificate Manager .

Para importar un certificado existente en ACM, consulte [Importación de certificados en ACM](#) en la Guía del usuario de AWS Certificate Manager .

Para solicitar un certificado privado para usar FTPS a través de direcciones IP privadas, consulte [Solicitar un certificado privado](#) en la Guía del usuario de AWS Certificate Manager .

Se admiten certificados con los siguientes algoritmos criptográficos y tamaños de clave:

- RSA de 2048 bits (RSA_2048)
- RSA de 4096 bits (RSA_4096)

- Curva elíptica principal de 256 bits (EC_prime256v1)
- Curva elíptica principal de 384 bits (EC_secp384r1)
- Curva elíptica principal de 521 bits (EC_secp521r1)

 Note

El certificado debe ser un certificado de SSL/TLS X.509 versión 3 válido con el FQDN o la dirección IP especificados y contener información sobre el emisor.

3. En Elegir un proveedor de identidad, seleccione el proveedor de identidad que desee utilizar para administrar el acceso de los usuarios. Dispone de las opciones siguientes:
- AWS Directory Service for Microsoft Active Directory— Usted proporciona un Directory Service directorio para acceder al punto final. Si lo hace, puede utilizar las credenciales almacenadas en el Active Directory para autenticar a los usuarios. Para obtener más información sobre cómo trabajar con proveedores de AWS Managed Microsoft AD identidad, consulte [Uso AWS de Directory Service para Microsoft Active Directory](#).

 Note

- Cross-Account y no se admiten los directorios compartidos AWS Managed Microsoft AD.
 - Para configurar un servidor con Directory Service como proveedor de identidad, debe añadir algunos Directory Service permisos. Para obtener más información, consulte [Antes de empezar a usar AWS Directory Service for Microsoft Active Directory](#).
- Proveedor de identidad personalizado: seleccione cualquiera de las siguientes opciones:
 - Úselo AWS Lambda para conectar su proveedor de identidad: puede usar un proveedor de identidad existente, respaldado por una función Lambda. Proporcione el nombre de identificación de la función de Lambda. Para obtener más información, consulte [Se utiliza AWS Lambda para integrar su proveedor de identidad](#).
 - Utilice Amazon API Gateway para conectar su proveedor de identidades: puede crear un método de API Gateway respaldado por una función de Lambda para usarlo como proveedor de identidades. Proporcione una URL de Amazon API Gateway y un rol de

invocación. Para obtener más información, consulte [Uso de Amazon API Gateway para integrar su proveedor de identidad](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory

Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity

Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. Elija Siguiente.
5. En Elegir punto de conexión, haga lo siguiente:

[i](#) Note

Los servidores FTPS para Transfer Family funcionan a través del puerto 21 (canal de control) y el rango de puertos 8192-8200 (canal de datos).

- a. En el tipo de punto de conexión, seleccione el tipo de punto de conexión alojado en la VPC para alojar el punto de conexión de su servidor. Para obtener más información acerca de cómo configurar un punto de conexión de la VPC, consulte [Creación de un servidor en una nube privada virtual \(VPC\)](#).

 Note

No se admiten los puntos de conexión de acceso público.

- b. (Opcional) En el caso del dispositivo con FIPS activado, active la casilla de verificación del punto de conexión con FIPS activado para asegurarse de que el dispositivo de punto final cumpla con las normas federales de procesamiento de información (FIPS).

 Note

FIPS-enabled Los puntos finales solo están disponibles en las regiones de Norteamérica AWS . Para obtener una lista de las regiones disponibles, consulte los [puntos de conexión y cuotas de AWS Transfer Family](#) en Referencia general de AWS. Para obtener más información acerca del FIPS, consulte [Estándar federal de procesamiento de la información \(FIPS\) 140-2](#) .

- c. Elija Siguiente.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

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

6. En la página Elegir dominio, elige el servicio AWS de almacenamiento que deseas usar para almacenar tus datos y acceder a ellos a través del protocolo seleccionado:
- Seleccione Amazon S3 para almacenar sus archivos y acceder a ellos como objetos a través del protocolo seleccionado.
 - Seleccione Amazon EFS para almacenar los archivos del sistema de archivos de Amazon EFS y acceder a ellos a través del protocolo seleccionado.

Elija Siguiente.

7. En Configurar detalles adicionales, haga lo siguiente:

- a. Para el registro, especifique un grupo de registro de ya existente o cree uno nuevo (la opción predeterminada).

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

Si selecciona Crear grupo de registros, la CloudWatch consola (<https://console.aws.amazon.com/cloudwatch/>) se abre en la página Crear grupo de registros. Para obtener más información, consulte [Crear un grupo de CloudWatch registros en Logs](#).

- b. (Opcional) Para los flujos de trabajo administrados, elija los ID de flujo de trabajo (y el rol correspondiente) que Transfer Family debe asumir al ejecutar el flujo de trabajo. Puede elegir un flujo de trabajo para ejecutarlo tras una carga completa y otro para ejecutarlo tras una carga parcial. Para obtener más información sobre el procesamiento de los archivos mediante flujos de trabajo administrados, consulte [AWS Transfer Family flujos de trabajo gestionados](#).

Managed workflows [Info](#)

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

w- ▼ ↻ [Create a new Workflow](#)

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

w- ▼ ↻ [Create a new Workflow](#)

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

▼ ↻

- c. Para ver las opciones de algoritmos criptográficos, elija una política de seguridad que contenga los algoritmos criptográficos habilitados para su uso en el servidor. Nuestra política de seguridad más reciente es la predeterminada: para obtener más información, consulte [Políticas de seguridad para AWS Transfer Family servidores](#).
- d. En el caso de la clave de host del servidor, manténgala en blanco.
- e. (Opcional) En el caso de las etiquetas, en Clave y valor, introduzca una o más etiquetas como pares de valores clave y, a continuación, seleccione Añadir etiqueta.
- f. Puede optimizar el rendimiento de sus directorios de Amazon S3. Por ejemplo, supongamos que va a su directorio principal y tiene 10 000 subdirectorios. En otras palabras, su bucket de Amazon S3 tiene 10 000 carpetas. En este escenario, si ejecuta el comando `ls` (list), la operación de lista tarda entre seis y ocho minutos. Sin embargo, si optimiza los directorios, esta operación solo tardará unos segundos.

Al crear el servidor mediante la consola, los directorios optimizados están habilitados de forma predeterminada. Si crea el servidor mediante la API, este comportamiento no está habilitado de forma predeterminada.

Optimized Directories [Info](#)

Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

- g. Elija Siguiente.
- h. (Opcional) Puede configurar AWS Transfer Family los servidores para que muestren mensajes personalizados, como políticas organizativas o términos y condiciones, a sus usuarios finales. También puede mostrar el mensaje del día (MOTD) personalizado a los usuarios que se hayan autenticado correctamente.

En el cuadro de texto del encabezado de Pre-authentication visualización, introduzca el mensaje de texto que desee mostrar a los usuarios antes de que se autenticuen y, en el Post-authentication cuadro de texto del encabezado, escriba el texto que desee mostrar a los usuarios una vez que se hayan autenticado correctamente.

- i. (Opcional) Puede configurar las siguientes opciones adicionales.
 - SetStat opción: active esta opción para ignorar el error que se genera cuando un cliente intenta usarlo SETSTAT en un archivo que está cargando en un bucket de Amazon S3. Para obtener más información, consulte la SetStatOption documentación del [ProtocolDetails](#)tema.
 - Reanudación de la sesión TLS: proporciona un mecanismo para reanudar o compartir una clave secreta negociada entre el control y la conexión de datos para una sesión de FTPS. Para obtener más información, consulte la TlsSessionResumptionMode documentación del [ProtocolDetails](#)tema.
 - IP pasiva: indica el modo pasivo para los protocolos FTP y FTPS. Escriba una sola dirección IPv4, como la dirección IP pública de un cortafuegos, un enrutador o un equilibrador de carga. Para obtener más información, consulte la PassiveIp documentación del [ProtocolDetails](#)tema.

Additional configuration

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

☐ Enable

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

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. En Revisar y crear, revise sus opciones.

- Si desea editar alguno de ellos, seleccione Editar junto al paso.

 Note

Debe revisar cada paso después del paso que eligió editar.

- Si no ha realizado cambios, seleccione Crear servidor para crear el suyo. Así llegará a la página Servers (Servidores), mostrada a continuación, donde ya aparece el nuevo servidor.

Pueden transcurrir algunos minutos antes de que el estado del nuevo servidor cambie a Online. En ese momento, el servidor ya puede realizar operaciones con archivos para los usuarios.

Próximos pasos: para el siguiente paso, continúe a [Uso de proveedores de identidad personalizados](#) para configurar los usuarios.

Cree un servidor FTP-enabled

El protocolo de File Transfer (FTP) es un protocolo de red que se utiliza para la transferencia de datos. El FTP utiliza un canal independiente para el control y la transferencia de datos. El canal de control está abierto hasta que finalice o se agote el tiempo de inactividad. El canal de datos estará activo mientras dure la transferencia. El FTP utiliza texto sin cifrar y no admite el cifrado del tráfico.

Note

Al habilitar el FTP, debe elegir la opción de acceso interno para el VPC-hosted punto final. Si necesita que su servidor haga que los datos atraviesen la red pública, debe utilizar protocolos seguros, como SFTP o FTPS.

Note

Para obtener información importante sobre los balanceadores de carga de red, consulte [Evite colocar los NLB y los NAT delante de AWS Transfer Family servidores](#)

Para crear un servidor FTP-enabled

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/> y seleccione Servidores en el panel de navegación y, a continuación, elija Crear servidor.
2. En Elegir protocolos, seleccione FTP y, a continuación, Siguiente.
3. En Elegir un proveedor de identidad, seleccione el proveedor de identidad que desee utilizar para administrar el acceso de los usuarios. Dispone de las opciones siguientes:
 - AWS Directory Service for Microsoft Active Directory— Usted proporciona un Directory Service directorio para acceder al punto final. Si lo hace, puede utilizar las credenciales almacenadas en el Active Directory para autenticar a los usuarios. Para obtener más información sobre cómo trabajar con proveedores de AWS Managed Microsoft AD identidad, consulte [Uso AWS de Directory Service para Microsoft Active Directory](#).

Note

- Cross-Account y no se admiten los directorios compartidos AWS Managed Microsoft AD.

- Para configurar un servidor con Directory Service como proveedor de identidad, debe añadir algunos Directory Service permisos. Para obtener más información, consulte [Antes de empezar a usar AWS Directory Service for Microsoft Active Directory](#).
- Proveedor de identidad personalizado: seleccione cualquiera de las siguientes opciones:
 - Úselo AWS Lambda para conectar su proveedor de identidad: puede usar un proveedor de identidad existente, respaldado por una función Lambda. Proporcione el nombre de identificación de la función de Lambda. Para obtener más información, consulte [Se utiliza AWS Lambda para integrar su proveedor de identidad](#).
 - Utilice Amazon API Gateway para conectar su proveedor de identidades: puede crear un método de API Gateway respaldado por una función de Lambda para usarlo como proveedor de identidades. Proporcione una URL de Amazon API Gateway y un rol de invocación. Para obtener más información, consulte [Uso de Amazon API Gateway para integrar su proveedor de identidad](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory

Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity

Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. Elija Siguiente.
5. En Elegir punto de conexión, haga lo siguiente:

[i](#) Note

Los servidores FTP para Transfer Family funcionan a través del puerto 21 (canal de control) y el rango de puertos 8192-8200 (canal de datos).

- a. En el tipo de punto de conexión, seleccione el punto de conexión alojado en la VPC para alojar el punto de conexión de su servidor. Para obtener más información acerca de cómo

configurar un punto de conexión de la VPC, consulte [Creación de un servidor en una nube privada virtual \(VPC\)](#).

 Note

No se admiten los puntos de conexión de acceso público.

- b. En el caso de FIPS activado, mantenga desactivada la casilla de verificación del punto de conexión con FIPS activado.

 Note

FIPS-enabled Los servidores FTP no admiten puntos finales.

- c. Elija Siguiente.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

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

6. En la página Elegir dominio, elija el servicio AWS de almacenamiento que desee usar para almacenar sus datos y acceder a ellos a través del protocolo seleccionado.
- Seleccione Amazon S3 para almacenar sus archivos y acceder a ellos como objetos a través del protocolo seleccionado.
 - Seleccione Amazon EFS para almacenar los archivos del sistema de archivos de Amazon EFS y acceder a ellos a través del protocolo seleccionado.

Elija Siguiente.

7. En Configurar detalles adicionales, haga lo siguiente:

- a. Para el registro, especifique un grupo de registro de ya existente o cree uno nuevo (la opción predeterminada).

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

Si selecciona Crear grupo de registros, la CloudWatch consola (<https://console.aws.amazon.com/cloudwatch/>) se abre en la página Crear grupo de registros. Para obtener más información, consulte [Crear un grupo de CloudWatch registros en Logs](#).

- b. (Opcional) Para los flujos de trabajo administrados, elija los ID de flujo de trabajo (y el rol correspondiente) que Transfer Family debe asumir al ejecutar el flujo de trabajo. Puede elegir un flujo de trabajo para ejecutarlo tras una carga completa y otro para ejecutarlo tras una carga parcial. Para obtener más información sobre el procesamiento de los archivos mediante flujos de trabajo administrados, consulte [AWS Transfer Family flujos de trabajo gestionados](#).

Managed workflows [Info](#)

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

w- [redacted] ▼ [Create a new Workflow](#)

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

w- [redacted] ▼ [Create a new Workflow](#)

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

[redacted] ▼

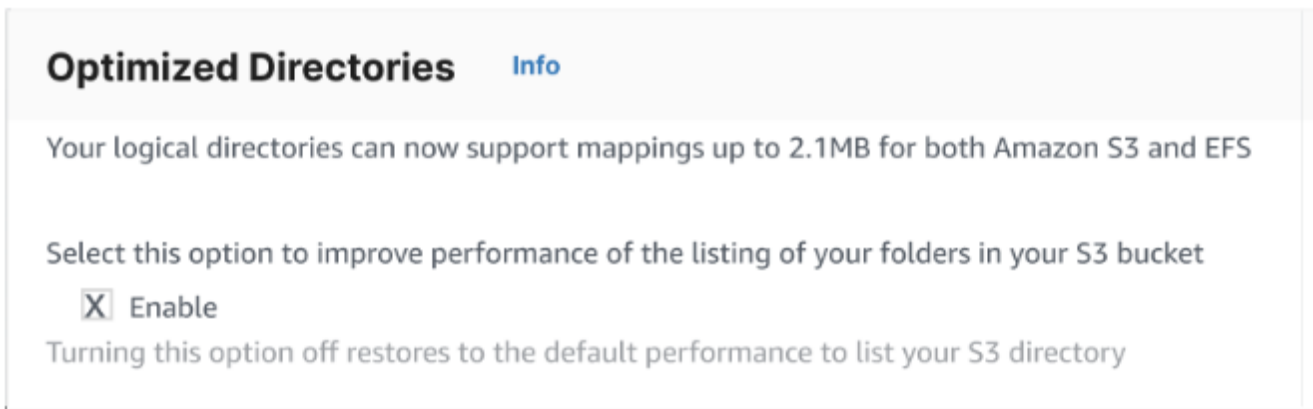
- c. Para ver las opciones de algoritmos criptográficos, elija una política de seguridad que contenga los algoritmos criptográficos habilitados para su uso en el servidor.

Note

Transfer Family asigna la política de seguridad más reciente a su servidor FTP. Sin embargo, dado que el protocolo FTP no utiliza ningún tipo de cifrado, los servidores FTP no utilizan ninguno de los algoritmos de política de seguridad. A menos que su servidor también utilice el protocolo FTPS o SFTP, la política de seguridad no se utilizará.

- d. En el caso de la clave de host del servidor, manténgala en blanco.
- e. (Opcional) En el caso de las etiquetas, en Clave y valor, introduzca una o más etiquetas como pares de valores clave y, a continuación, seleccione Añadir etiqueta.
- f. Puede optimizar el rendimiento de sus directorios de Amazon S3. Por ejemplo, supongamos que va a su directorio principal y tiene 10 000 subdirectorios. En otras palabras, su bucket de Amazon S3 tiene 10 000 carpetas. En este escenario, si ejecuta el comando `ls` (list), la operación de lista tarda entre seis y ocho minutos. Sin embargo, si optimiza los directorios, esta operación solo tardará unos segundos.

Al crear el servidor mediante la consola, los directorios optimizados están habilitados de forma predeterminada. Si crea el servidor mediante la API, este comportamiento no está habilitado de forma predeterminada.



- g. Elija Siguiente.
- h. (Opcional) Puede configurar AWS Transfer Family los servidores para que muestren mensajes personalizados, como políticas organizativas o términos y condiciones, a sus usuarios finales. También puede mostrar el mensaje del día (MOTD) personalizado a los usuarios que se hayan autenticado correctamente.

En el cuadro de texto del encabezado de Pre-authentication visualización, introduzca el mensaje de texto que desee mostrar a los usuarios antes de que se autenticuen y, en el Post-authentication cuadro de texto del encabezado, escriba el texto que desee mostrar a los usuarios una vez que se hayan autenticado correctamente.

- i. (Opcional) Puede configurar las siguientes opciones adicionales.
 - SetStat opción: active esta opción para ignorar el error que se genera cuando un cliente intenta usarlo SETSTAT en un archivo que está cargando en un bucket de Amazon S3. Para obtener más información, consulte la SetStatOption documentación del [ProtocolDetails](#)tema.
 - Reanudación de la sesión TLS: proporciona un mecanismo para reanudar o compartir una clave secreta negociada entre el control y la conexión de datos para una sesión de FTPS. Para obtener más información, consulte la TlsSessionResumptionMode documentación del [ProtocolDetails](#)tema.
 - IP pasiva: indica el modo pasivo para los protocolos FTP y FTPS. Escriba una sola dirección IPv4, como la dirección IP pública de un cortafuegos, un enrutador o un equilibrador de carga. Para obtener más información, consulte la PassiveIp documentación del [ProtocolDetails](#)tema.

Additional configuration

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

☐ Enable

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

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. En Revisar y crear, revise sus opciones.

- Si desea editar alguno de ellos, seleccione Editar junto al paso.

 Note

Debe revisar cada paso después del paso que eligió editar.

- Si no ha realizado cambios, seleccione Crear servidor para crear el suyo. Así llegará a la página Servers (Servidores), mostrada a continuación, donde ya aparece el nuevo servidor.

Pueden transcurrir algunos minutos antes de que el estado del nuevo servidor cambie a Online. En ese momento, el servidor ya puede realizar operaciones con archivos para los usuarios.

Próximos pasos: para el siguiente paso, continúe a [Uso de proveedores de identidad personalizados](#) para la configuración de los usuarios.

Creación de un servidor en una nube privada virtual (VPC)

Puede alojar el punto de conexión de su servidor dentro de una nube privada virtual (VPC) para utilizarla para transferir datos hacia y desde un bucket de Amazon S3 o un sistema de archivos Amazon EFS sin tener que recurrir a la Internet pública.

Note

Después del 19 de mayo de 2021, no podrás crear un servidor con `EndpointType=VPC_ENDPOINT` tu AWS cuenta si tu cuenta no lo ha hecho antes del 19 de mayo de 2021. Si ya creó servidores `EndpointType=VPC_ENDPOINT` en su AWS cuenta el 21 de febrero de 2021 o antes, no se verá afectado. Después de esta fecha, use `EndpointType=VPC`. Para obtener más información, consulte [the section called “Suspend the use of VPC_ENDPOINT”](#).

Si utiliza Amazon Virtual Private Cloud (Amazon VPC) para alojar sus AWS recursos, puede establecer una conexión privada entre la VPC y un servidor. Luego, puede usar este servidor para transferir datos a través de su cliente hacia y desde su bucket de Amazon S3 sin usar una dirección IP pública ni requerir una puerta de enlace de Internet.

Con Amazon VPC, puede lanzar AWS recursos en una red virtual personalizada. Puede utilizar una VPC para controlar la configuración de red, como el intervalo de direcciones IP, las subredes, las tablas de enrutamiento y las puertas de enlace de red. Para obtener más información acerca de VPCs, consulte [¿Qué es Amazon VPC?](#) en la Guía del usuario de Amazon VPC.

En las siguientes secciones puede encontrar instrucciones sobre cómo conectar su VPC a un servidor. A modo de resumen, puede hacerlo de la siguiente manera:

1. Configure un servidor mediante un punto de conexión de VPC.
2. Conéctese a su servidor mediante un cliente que se encuentre en su VPC a través del punto de conexión de VPC. De este modo, podrá transferir los datos almacenados en su bucket de Amazon S3 a través de su cliente mediante AWS Transfer Family. Puede realizar esta transferencia aunque la red esté desconectada de la Internet pública.
3. Además, si opta por hacer que el punto de conexión de su servidor esté orientado a Internet, puede asociar las direcciones IP elásticas a su punto de conexión. De este modo, los clientes ajenos a la VPC se conectarán al servidor. Puede usar grupos de seguridad de VPC para

controlar el acceso a los usuarios autenticados cuyas solicitudes se originan únicamente en las direcciones permitidas.

 Note

AWS Transfer Family admite puntos de conexión de doble pila, lo que permite que su servidor se comuniquen a través de IPv4 e IPv6. Para habilitar la compatibilidad con doble pila, selecciona la opción Habilitar el punto de enlace de doble pila de DNS al crear el punto de enlace de VPC. Tenga en cuenta que tanto la VPC como las subredes deben estar configuradas para admitir IPv6 antes de poder utilizar esta función. Dual-stack el soporte es especialmente útil cuando hay clientes que necesitan conectarse mediante cualquiera de los protocolos.

Para obtener información sobre los puntos finales de servidores de doble pila (IPv4 e IPv6), consulte. [Compatibilidad con IPv6 para servidores Transfer Family](#)

Temas

- [Cree un punto de conexión de servidor al que solo se pueda acceder desde su VPC](#)
- [Creación de un punto de conexión a Internet para el servidor](#)
- [Cambie el tipo de punto de conexión para su servidor](#)
- [Suspender el uso de VPC_ENDPOINT](#)
- [Limitar el acceso a los terminales de VPC para los servidores Transfer Family](#)
- [Funciones de red adicionales](#)
- [Actualización del tipo de punto final AWS Transfer Family del servidor de VPC_ENDPOINT a VPC](#)

Cree un punto de conexión de servidor al que solo se pueda acceder desde su VPC

En el siguiente procedimiento, se crea un punto de conexión de servidor al que solo puedan acceder los recursos de VPC.

Creación de un punto de conexión de servidor dentro de una VPC

1. Abra la AWS Transfer Family consola en. <https://console.aws.amazon.com/transfer/>
2. En el panel de navegación, seleccione Servidores y, a continuación, elija Crear servidor.

3. En Elegir protocolos, seleccione uno o más protocolos y, a continuación, elija Siguiente. Para obtener más información sobre protocolos, consulte [Paso 2: Crea un SFTP-enabled servidor](#).
4. En Elegir un proveedor de identidades, elija Servicio gestionado para almacenar las identidades y claves de los usuarios y AWS Transfer Family, a continuación, elija Siguiente.

En este procedimiento se utiliza la opción de administración por el servicio. Si elige Personalizado, debe indicar un punto de conexión de Amazon API Gateway y un rol de AWS Identity and Access Management (IAM) para el acceso a ese punto de conexión. Así puede integrar su servicio de directorio para la autenticación y autorización de sus usuarios. Para obtener más información acerca del uso de proveedores de identidad personalizados, consulte [Uso de proveedores de identidad personalizados](#).

5. En Elegir punto de conexión, haga lo siguiente:
 - a. En el tipo de punto de conexión, seleccione el tipo de punto de conexión alojado en la VPC para alojar el punto de conexión de su servidor.
 - b. En Access, seleccione Interno para que solo los clientes que utilicen las direcciones IP privadas del punto de conexión puedan acceder a su punto de conexión.

Para obtener más información sobre la opción de conexión a Internet, consulte [Creación de un punto de conexión a Internet para el servidor](#). Un servidor creado en una VPC sólo para acceso interno no admite nombres de host personalizados.

- c. Para la VPC, elija un ID de VPC existente o elija Crear una VPC para crear una nueva VPC.
 - d. En la sección Zonas de disponibilidad, elija hasta tres zonas de disponibilidad y subredes asociadas.
 - e. En la sección Grupos de seguridad, elija uno o varios ID de grupo de seguridad existentes o elija Crear un grupo de seguridad para crear un grupo de seguridad nuevo. Para obtener más información sobre los grupos de seguridad, consulte [Grupos de seguridad para su VPC](#) en la Guía del usuario de Amazon Virtual Private Cloud. Para crear un grupo de seguridad, consulte [Creación de un grupo de seguridad](#) en la Guía del usuario de Amazon Virtual Private Cloud.

 Note

Su VPC incluye automáticamente un grupo de seguridad predeterminado. Si no especifica un grupo o grupos de seguridad distinto al lanzar el servidor, se asociará el grupo de seguridad predeterminado a su servidor.

- Para las reglas de entrada del grupo de seguridad, puede configurar el tráfico SSH para que utilice los puertos 22, 2222, 22000 o cualquier combinación. El puerto 22 está configurado de forma predeterminada. Para usar el puerto 2222 o el puerto 22000, debe agregar una regla de entrada a su grupo de seguridad. Para el tipo, elija TCP personalizado y, a continuación, introduzca uno **2222** o **22000** varios puertos y, para el origen, introduzca el mismo rango de CIDR que tiene para la regla del puerto 22 de SSH.
- Para las reglas de entrada del grupo de seguridad, configure el tráfico FTP y FTPS para que utilice el rango de puertos para el canal de control y **21 8192-8200** para el canal de datos.

 Note

También puede usar el puerto 2223 para los clientes que requieren un ACK TCP «combinado» o la posibilidad de que el último paquete del protocolo de enlace tridireccional TCP también contenga datos.

Algunos programas de cliente pueden ser incompatibles con el puerto 2223: por ejemplo, un cliente que requiere que el servidor envíe la cadena de identificación de SFTP antes que el cliente.

[VPC](#) > [Security Groups](#) > [sg-\[redacted\]-default](#) > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- f. (Opcional) En el caso del dispositivo con FIPS activado, active la casilla de verificación del punto de conexión con FIPS activado para garantizar que el dispositivo de punto de conexión cumpla con las normas federales de procesamiento de la información (FIPS).

 Note

FIPS-enabled Los puntos finales solo están disponibles en las regiones de Norteamérica. AWS Para obtener una lista de las regiones disponibles, consulte los [puntos de conexión y cuotas de AWS Transfer Family](#) en Referencia general de AWS. Para obtener más información acerca del FIPS, consulte [Estándar federal de procesamiento de la información \(FIPS\) 140-2](#).

- g. Elija Siguiente.
6. En Configurar detalles adicionales, haga lo siguiente:
 - a. Para el CloudWatch registro, elige una de las siguientes opciones para permitir que Amazon CloudWatch registre la actividad de tus usuarios:
 - Cree un nuevo rol para permitir a Transfer Family crear automáticamente el rol de IAM, siempre y cuando tenga los permisos adecuados para crear un nuevo rol. El rol de IAM que se crea se llama `AWSTransferLoggingAccess`.
 - Elija Elegir un rol ya existente para seleccionar un rol de IAM de su cuenta. En Rol de registro, elija el rol. Este rol de IAM debe incluir una política de confianza con el servicio establecido en `transfer.amazonaws.com`.

Para obtener más información sobre el CloudWatch registro, consulte [Configura el rol de CloudWatch registro](#).

 Note

- No puede ver la actividad del usuario final en CloudWatch si no especifica una función de registro.
- Si no desea configurar un rol de CloudWatch registro, seleccione Elegir un rol existente, pero no seleccione un rol de registro.

- b. Para ver las opciones de algoritmos criptográficos, elija una política de seguridad que contenga los algoritmos criptográficos habilitados para su uso en el servidor.

 Note

De forma predeterminada, la política de TransferSecurityPolicy-2024-01 seguridad se adjunta a su servidor a menos que elija una diferente.

Para obtener más información sobre las políticas de seguridad, consulte [Políticas de seguridad para AWS Transfer Family servidores](#).

- c. (Opcional: esta sección es solo para migrar usuarios desde un SFTP-enabled servidor existente). En el caso de la clave de host del servidor, introduzca una clave privada RSA, ED25519 o ECDSA que se utilizará para identificar el servidor cuando los clientes se conecten a él a través de SFTP.
 - d. (Opcional) En el caso de las etiquetas, en Clave y valor, introduzca una o más etiquetas como pares de valores clave y, a continuación, seleccione Añadir etiqueta.
 - e. Elija Siguiente.
7. En Revisar y crear, revise sus opciones. Si:
- Si desea editar alguno de ellos, seleccione Editar junto al paso.

 Note

Deberás revisar cada paso después del paso que decidiste editar.

- Si no hay cambios, seleccione Crear servidor para crear su servidor. Así llegará a la página Servers (Servidores), mostrada a continuación, donde ya aparece el nuevo servidor.

Pueden transcurrir algunos minutos antes de que el estado del nuevo servidor cambie a Online. En ese momento, el servidor podrá realizar operaciones con los archivos, pero primero tendrá que crear un usuario. Para obtener más información sobre la creación de usuarios, consulte. [Administración de usuarios para puntos finales de servidor](#)

Creación de un punto de conexión a Internet para el servidor

En el siguiente procedimiento, se crea un punto de conexión de servidor. Solo los clientes cuyas direcciones IP de origen estén permitidas en el grupo de seguridad predeterminado de VPC pueden acceder a este punto de conexión a través de Internet. Además, al usar direcciones IP elásticas para

que su punto de conexión esté conectado a Internet, sus clientes pueden usar la dirección IP elástica para permitir el acceso a su punto de conexión en sus firewalls.

 Note

Solo se pueden usar SFTP y FTPS en un punto de conexión alojado en una VPC con acceso a Internet.

Creación de un punto de conexión de interfaz

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación, seleccione Servidores y, a continuación, elija Crear servidor.
3. En Elegir protocolos, seleccione uno o más protocolos y, a continuación, elija Siguiente. Para obtener más información sobre protocolos, consulte [Paso 2: Crea un SFTP-enabled servidor](#).
4. En Elegir un proveedor de identidades, elija Servicio gestionado para almacenar las identidades y claves de los usuarios y AWS Transfer Family, a continuación, elija Siguiente.

En este procedimiento se utiliza la opción de administración por el servicio. Si elige Personalizado, debe indicar un punto de conexión de Amazon API Gateway y un rol de AWS Identity and Access Management (IAM) para el acceso a ese punto de conexión. Así puede integrar su servicio de directorio para la autenticación y autorización de sus usuarios. Para obtener más información acerca del uso de proveedores de identidad personalizados, consulte [Uso de proveedores de identidad personalizados](#).

5. En Elegir punto de conexión, haga lo siguiente:
 - a. En el tipo de punto de conexión, seleccione el tipo de punto de conexión alojado en la VPC para alojar el punto de conexión de su servidor.
 - b. En Access, elija Internet Facing para que los clientes puedan acceder a su punto de conexión a través de Internet.

 Note

Si elige Internet Facing, puede elegir una dirección IP elástica existente en cada subred o subredes. O bien, puede ir a la consola de VPC (<https://console.aws.amazon.com/vpc/>) para asignar una o más direcciones IP elásticas

nuevas. Estas direcciones pueden ser de su propiedad AWS o de usted. No puede asociar direcciones IP elásticas que ya estén en uso con su punto de conexión.

- c. (Opcional) En Nombre de host personalizado, elija una de las siguientes opciones:

 Note

Los clientes AWS GovCloud (US) necesitan conectarse directamente a través de la dirección IP elástica o crear un registro de nombre de host en Commercial Route 53 que apunte a su EIP. Para obtener más información sobre el uso de Route 53 GovCloud para los puntos de conexión, consulte [Configuración de Amazon Route 53 con sus AWS GovCloud \(US\) recursos](#) en la Guía del AWS GovCloud (US) usuario.

- Alias DNS de Amazon Route 53: si el nombre de host que desea usar está registrado en Route 53. A continuación puede escribir el nombre de host.
- Otro DNS: si el nombre de host que desea usar está registrado en otro proveedor de DNS. A continuación puede escribir el nombre de host.
- Ninguno: para usar el punto de conexión del servidor y no usar un nombre de host personalizado. El nombre de host del servidor tiene la forma `server-id.server.transfer.region.amazonaws.com`.

 Note

En el caso de los clientes de None AWS GovCloud (US), no se crea un nombre de host en este formato.

Para obtener más información sobre el uso de nombres de host personalizados, consulte [Uso de nombres de host personalizados](#).

- d. Para la VPC, elija un ID de VPC existente o elija Crear una VPC para crear una nueva VPC.
- e. En la sección Zonas de disponibilidad, elija hasta tres zonas de disponibilidad y subredes asociadas. Para las direcciones IPv4, elija una dirección IP elástica para cada subred. Esta es la dirección IP que sus clientes pueden usar para permitir el acceso a su punto de conexión en sus firewalls.

Consejo: Debe usar una subred pública para sus zonas de disponibilidad o configurar primero una puerta de enlace a Internet si quiere usar una subred privada.

- f. En la sección Grupos de seguridad, elija uno o varios ID de grupo de seguridad existentes o elija Crear un grupo de seguridad para crear un grupo de seguridad nuevo. Para obtener más información sobre los grupos de seguridad, consulte [Grupos de seguridad para su VPC](#) en la Guía del usuario de Amazon Virtual Private Cloud. Para crear un grupo de seguridad, consulte [Creación de un grupo de seguridad](#) en la Guía del usuario de Amazon Virtual Private Cloud.

 Note

Su VPC incluye automáticamente un grupo de seguridad predeterminado. Si no especifica un grupo o grupos de seguridad distinto al lanzar el servidor, se asociará el grupo de seguridad predeterminado a su servidor.

- Para las reglas de entrada del grupo de seguridad, puede configurar el tráfico SSH para que utilice los puertos 22, 2222, 22000 o cualquier combinación. El puerto 22 está configurado de forma predeterminada. Para usar el puerto 2222 o el puerto 22000, debe agregar una regla de entrada a su grupo de seguridad. Para el tipo, elija TCP personalizado y, a continuación, introduzca uno **2222** o **22000** varios puertos y, para el origen, introduzca el mismo rango de CIDR que tiene para la regla del puerto 22 de SSH.
- Para las reglas de entrada del grupo de seguridad, configure el tráfico FTPS para que utilice el rango de puertos para el canal de control y **21 8192-8200** para el canal de datos.

 Note

También puede usar el puerto 2223 para los clientes que requieren un ACK TCP «combinado» o la posibilidad de que el paquete final del protocolo de enlace tridireccional TCP también contenga datos.

Algunos programas de cliente pueden ser incompatibles con el puerto 2223: por ejemplo, un cliente que requiere que el servidor envíe la cadena de identificación de SFTP antes que el cliente.

[VPC](#) > [Security Groups](#) > [sg-\[redacted\]-default](#) > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- g. (Opcional) En el caso del dispositivo con FIPS activado, active la casilla de verificación del punto de conexión con FIPS activado para garantizar que el dispositivo de punto de conexión cumpla con las normas federales de procesamiento de la información (FIPS).

 Note

FIPS-enabled Los puntos finales solo están disponibles en las regiones de Norteamérica. AWS Para obtener una lista de las regiones disponibles, consulte los [puntos de conexión y cuotas de AWS Transfer Family](#) en Referencia general de AWS. Para obtener más información acerca del FIPS, consulte [Estándar federal de procesamiento de la información \(FIPS\) 140-2](#).

- h. Elija Siguiente.
6. En Configurar detalles adicionales, haga lo siguiente:
 - a. Para el CloudWatch registro, elige una de las siguientes opciones para permitir que Amazon CloudWatch registre la actividad de tus usuarios:
 - Cree un nuevo rol para permitir a Transfer Family crear automáticamente el rol de IAM, siempre y cuando tenga los permisos adecuados para crear un nuevo rol. El rol de IAM que se crea se llama `AWSTransferLoggingAccess`.
 - Elija Elegir un rol ya existente para seleccionar un rol de IAM de su cuenta. En Rol de registro, elija el rol. Este rol de IAM debe incluir una política de confianza con el servicio establecido en `transfer.amazonaws.com`.

Para obtener más información sobre el CloudWatch registro, consulte [Configura el rol de CloudWatch registro](#).

 Note

- No puede ver la actividad del usuario final en CloudWatch si no especifica una función de registro.
- Si no desea configurar un rol de CloudWatch registro, seleccione Elegir un rol existente, pero no seleccione un rol de registro.

- b. Para ver las opciones de algoritmos criptográficos, elija una política de seguridad que contenga los algoritmos criptográficos habilitados para su uso en el servidor.

Note

De forma predeterminada, la política de `TransferSecurityPolicy-2024-01` seguridad se adjunta a su servidor a menos que elija una diferente.

Para obtener más información sobre las políticas de seguridad, consulte [Políticas de seguridad para AWS Transfer Family servidores](#).

- c. (Opcional: esta sección es solo para migrar usuarios desde un SFTP-enabled servidor existente). En el caso de la clave de host del servidor, introduzca una clave privada RSA, ED25519 o ECDSA que se utilizará para identificar el servidor cuando los clientes se conecten a él a través de SFTP.
- d. (Opcional) En el caso de las etiquetas, en Clave y valor, introduzca una o más etiquetas como pares de valores clave y, a continuación, seleccione Añadir etiqueta.
- e. Elija Siguiente.
- f. (Opcional) Para los flujos de trabajo administrados, elija los ID de flujo de trabajo (y el rol correspondiente) que Transfer Family debe asumir al ejecutar el flujo de trabajo. Puede elegir un flujo de trabajo para ejecutarlo tras una carga completa y otro para ejecutarlo tras una carga parcial. Para obtener más información sobre el procesamiento de los archivos mediante flujos de trabajo administrados, consulte [AWS Transfer Family flujos de trabajo gestionados](#).

Managed workflows [Info](#)

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

W- [dropdown] [refresh] [Create a new Workflow]

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

W- [dropdown] [refresh] [Create a new Workflow]

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

[dropdown] [refresh]

7. En Revisar y crear, revise sus opciones. Si:

- Si desea editar alguno de ellos, seleccione Editar junto al paso.

 Note

Deberás revisar cada paso después del paso que decidiste editar.

- Si no hay cambios, seleccione Crear servidor para crear su servidor. Así llegará a la página Servers (Servidores), mostrada a continuación, donde ya aparece el nuevo servidor.

Puede elegir el ID del servidor para ver la configuración detallada del servidor que acaba de crear. Una vez rellena la columna Dirección IPv4 pública, las direcciones IP elásticas que proporcionó se asociarán correctamente al punto de conexión del servidor.

 Note

Cuando el servidor de una VPC está en línea, solo se pueden modificar las subredes y solo a través de la API. [UpdateServer](#) Debe [detener el servidor](#) para añadir o cambiar las direcciones IP elásticas del punto de conexión del servidor.

Cambie el tipo de punto de conexión para su servidor

Si ya tiene un servidor existente que es accesible a través de Internet (es decir, tiene un tipo de punto de conexión público), puede cambiar su punto de conexión a un punto de conexión de VPC.

 Note

Si tiene un servidor existente en una VPC que se muestra como VPC_ENDPOINT, le recomendamos que lo modifique al nuevo tipo de punto de conexión de VPC. Con este nuevo tipo de punto de conexión, ya no necesita usar un Equilibrador de carga de red (NLB) para asociar direcciones IP elásticas al punto de conexión de su servidor. Además, puede utilizar grupos de seguridad de VPC para restringir el acceso al punto de conexión de su servidor. Sin embargo, puede seguir utilizando el tipo de VPC_ENDPOINT punto de conexión según sea necesario.

En el siguiente procedimiento, se asume que tiene un servidor que utiliza el tipo de punto de conexión público actual o el VPC_ENDPOINT tipo anterior.

Cambio del tipo de punto de conexión para su servidor

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación, seleccione Servers (Servidores).
3. Seleccione la casilla de verificación del servidor para el que desee cambiar el tipo de punto de conexión.

Important

Debe detener el servidor para poder cambiar el punto de conexión.

4. En Acciones, seleccione Detener.
5. En el cuadro de diálogo de confirmación que aparece, seleccione Detener para confirmar que desea detener el servidor.

Note

Antes de continuar con el siguiente paso, en Detalles del punto de conexión, espere a que el estado del servidor cambie a Desconectado; esto puede tardar un par de minutos. Puede que tenga que elegir Actualizar en la página de Servidores para ver el cambio de estado.

No podrá realizar ningún cambio hasta que el servidor esté desconectado.

6. En detalles de punto de conexión, elija Editar.
7. En Editar la configuración del punto de conexión, haga lo siguiente:
 - a. En Tipo de punto de conexión, seleccione VPC.
 - b. En Acceso, elija una de las siguientes opciones:
 - Interno para que solo los clientes que utilicen las direcciones IP privadas del punto de conexión puedan acceder a su punto de conexión.
 - Con conexión a Internet para que los clientes puedan acceder a su punto de conexión a través de la Internet pública.

Note

Si elige Internet Facing, puede elegir una dirección IP elástica existente en cada subred o subredes. O bien, puede ir a la consola de VPC (<https://>

console.aws.amazon.com/vpc/) para asignar una o más direcciones IP elásticas nuevas. Estas direcciones pueden ser de su propiedad AWS o de usted. No puede asociar direcciones IP elásticas que ya estén en uso con su punto de conexión.

- c. (Opcional solo para el acceso a Internet) Para un nombre de host personalizado, elija una de las siguientes opciones:
- Alias DNS de Amazon Route 53: si el nombre de host que desea usar está registrado en Route 53. A continuación puede escribir el nombre de host.
 - Otro DNS: si el nombre de host que desea usar está registrado en otro proveedor de DNS. A continuación puede escribir el nombre de host.
 - Ninguno: para usar el punto de conexión del servidor y no usar un nombre de host personalizado. El nombre de host del servidor tiene la forma `serverId.server.transfer.regionId.amazonaws.com`.

Para obtener más información sobre el uso de nombres de host personalizados, consulte [Uso de nombres de host personalizados](#).

- d. Para la VPC, elija un ID de VPC existente o elija Crear una VPC para crear una nueva VPC.
- e. En la sección Zonas de disponibilidad, seleccione hasta tres zonas de disponibilidad y las subredes asociadas. Si elige la opción Orientada a Internet, elija también una dirección IP elástica para cada subred.

 Note

Si desea un máximo de tres zonas de disponibilidad, pero no hay suficientes disponibles, créelas en la consola de VPC () <https://console.aws.amazon.com/vpc/>. Si modifica las subredes o las direcciones IP elásticas, el servidor tarda unos minutos en actualizarse. No puede guardar los cambios hasta que se complete la actualización del servidor.

- f. Seleccione Save.
8. En Acciones, seleccione Iniciar y espere a que el estado del servidor cambie a En línea; esto puede tardar un par de minutos.

 Note

Si ha cambiado un tipo de punto de conexión público a un tipo de punto de conexión de VPC, observe que el tipo de punto de conexión de su servidor ha cambiado a VPC.

El grupo de seguridad predeterminado se debe adjuntar al punto de conexión. Para cambiar o añadir grupos de seguridad adicionales, consulte [Creación de grupos de seguridad](#).

Suspender el uso de VPC_ENDPOINT

AWS Transfer Family ha dejado de poder crear servidores con `EndpointType=VPC_ENDPOINT` AWS cuentas nuevas. A partir del 19 de mayo de 2021, AWS las cuentas que no posean AWS Transfer Family servidores con un tipo de terminal no `VPC_ENDPOINT` podrán crear servidores nuevos con ellos `EndpointType=VPC_ENDPOINT`. Si ya posee servidores que utilizan el tipo de `VPC_ENDPOINT` punto de conexión, le recomendamos que comience a `EndpointType=VPC` utilizarlos lo antes posible. Para obtener más información, [consulte Actualizar el tipo de punto final AWS Transfer Family del servidor de VPC_ENDPOINT a VPC](#).

Lanzamos el nuevo tipo de VPC punto de conexión a principios de 2020. Para obtener más información, consulte [AWS Transfer Family para ver si SFTP admite grupos de seguridad de VPC y direcciones IP elásticas](#). Este nuevo punto de conexión tiene más funciones y es más rentable, y no tiene ningún coste. PrivateLink Para obtener más información, consulte [Precios de AWS PrivateLink](#).

Este tipo de punto de conexión es funcionalmente equivalente al tipo de punto de conexión anterior (`VPC_ENDPOINT`). Puede adjuntar direcciones IP elásticas directamente al punto de conexión para que esté orientado a Internet y utilizar grupos de seguridad para filtrar la IP de origen. Para obtener más información, consulte la entrada de blog sobre el [uso de direcciones IP permitidas AWS Transfer Family para proteger sus servidores SFTP](#).

También puede alojar este punto de conexión en un entorno de VPC compartido. Para obtener más información, consulte [AWS Transfer Family ahora es compatible con entornos de VPC de servicios compartidos](#).

Además de SFTP, puede usar la `EndpointType VPC` para habilitar FTPS y FTP. No tenemos previsto añadir estas funciones y FTPS/FTP soporte a `EndpointType=VPC_ENDPOINT`. También hemos eliminado este tipo de punto final como opción de la AWS Transfer Family consola.

Puede cambiar el tipo de punto final de su servidor mediante la consola Transfer Family AWS CLI, la API, los SDK o CloudFormation. Para cambiar el tipo de punto de conexión de su servidor, consulte [Actualización del tipo de punto final AWS Transfer Family del servidor de VPC_ENDPOINT a VPC](#).

Si tienes alguna duda, ponte en contacto con AWS Support nuestro equipo de AWS cuentas.

 Note

No tenemos previsto añadir estas funciones ni compatibilidad con FTPS o FTP a `EndpointType = VPC_ENDPOINT`. Ya no lo ofrecemos como opción en la consola AWS Transfer Family .

Si tiene más preguntas, puede ponerse en contacto con nosotros o con su equipo de cuentas. AWS Support

Limitar el acceso a los terminales de VPC para los servidores Transfer Family

Al crear un AWS Transfer Family servidor con un tipo de punto de enlace de VPC, los usuarios y principales de IAM necesitan permisos para crear y eliminar puntos de enlace de VPC. Sin embargo, las políticas de seguridad de su organización pueden restringir estos permisos. Puedes usar las políticas de IAM para permitir la creación y eliminación de terminales de VPC específicamente para Transfer Family y, al mismo tiempo, mantener las restricciones para otros servicios.

 Important

La siguiente política de IAM permite a los usuarios crear y eliminar puntos finales de VPC solo para los servidores Transfer Family y, al mismo tiempo, deniega estas operaciones para otros servicios:

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateVpcEndpoint",
    "ec2>DeleteVpcEndpoints"
  ],
  "Resource": ["*"],
  "Condition": {
    "ForAnyValue:StringNotLike": {
```

```

        "ec2:VpceServiceName": [
            "com.amazonaws.INPUT-YOUR-REGION.transfer.server.*"
        ],
        "StringNotLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/INPUT-YOUR-ROLE"
            ]
        }
    }
}

```

INPUT-YOUR-REGION Sustitúyalos por tu AWS región (por ejemplo **us-east-1**) y *INPUT-YOUR-ROLE* por el rol de IAM al que quieras conceder estos permisos.

Funciones de red adicionales

AWS Transfer Family proporciona varias funciones de red avanzadas que mejoran la seguridad y la flexibilidad cuando se utilizan configuraciones de VPC:

- Soporte para entornos de VPC compartidos: puede alojar su terminal de servidor Transfer Family en un entorno de VPC compartido. Para obtener más información, consulte [Uso de puntos de enlace alojados en VPC compartidas con](#). AWS Transfer Family
- Autenticación y seguridad: puede utilizar un firewall de aplicaciones AWS web para proteger su punto final de Amazon API Gateway. Para obtener más información, consulte [Protección AWS Transfer Family con AWS Web Application Firewall y Amazon API Gateway](#).

Actualización del tipo de punto final AWS Transfer Family del servidor de VPC_ENDPOINT a VPC

Puedes usar la Consola de administración de AWS API Transfer Family o la API Transfer Family para actualizar el servidor EndpointType de VPC_ENDPOINT a VPC. CloudFormation En las siguientes secciones se proporcionan procedimientos detallados y ejemplos para usar cada uno de estos métodos para actualizar un tipo de punto de conexión de servidor. Si tiene servidores en varias AWS regiones y en varias AWS cuentas, puede usar el script de ejemplo que se proporciona en la siguiente sección, con las modificaciones, para identificar los servidores mediante el VPC_ENDPOINT tipo que necesitará actualizar.

Temas

- [Identificar los servidores mediante el tipo de VPC_ENDPOINT punto de conexión](#)
- [Actualización del tipo de punto final del servidor mediante el Consola de administración de AWS](#)
- [Actualización del tipo de punto final del servidor mediante CloudFormation](#)
- [Actualización del servidor EndpointType mediante la API](#)

Identificar los servidores mediante el tipo de **VPC_ENDPOINT** punto de conexión

Puede identificar qué servidores utilizan VPC_ENDPOINT mediante Consola de administración de AWS.

Identificación de los servidores que utilizan el punto de conexión **VPC_ENDPOINT** mediante la consola

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. Seleccione Servidores en el panel de navegación para ver la lista de servidores de su cuenta en esa región.
3. Ordene la lista de servidores por tipo de punto de conexión para ver todos los servidores que utilizan VPC_ENDPOINT.

Para identificar los servidores que se utilizan **VPC_ENDPOINT** en varias AWS regiones y cuentas

Si tiene servidores en varias AWS regiones y en varias AWS cuentas, puede utilizar el siguiente script de ejemplo, con modificaciones, para identificar los servidores mediante el tipo de VPC_ENDPOINT punto final. El script de ejemplo utiliza las operaciones de la [ListServers](#) API Amazon EC2 [DescribeRegions](#) y Transfer Family. Si tiene varias cuentas de AWS , puede recorrerlas utilizando un rol de IAM con acceso de auditor de solo lectura si se autentica mediante perfiles de sesión ante su proveedor de identidad.

1. A continuación se muestra un ejemplo simple.

```
import boto3

profile = input("Enter the name of the AWS account you'll be working in: ")
session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2")

regions = ec2.describe_regions()
```

```
for region in regions['Regions']:
    region_name = region['RegionName']
    if region_name=='ap-northeast-3': #https://github.com/boto/boto3/issues/1943
        continue
    transfer = session.client("transfer", region_name=region_name)
    servers = transfer.list_servers()
    for server in servers['Servers']:
        if server['EndpointType']=='VPC_ENDPOINT':
            print(server['ServerId'], region_name)
```

2. Una vez que tenga la lista de servidores que desea actualizar, puede utilizar uno de los métodos descritos en las siguientes secciones para actualizar EndpointType a VPC.

Actualización del tipo de punto final del servidor mediante el Consola de administración de AWS

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación, seleccione Servers (Servidores).
3. Seleccione la casilla de verificación del servidor para el que desee cambiar el tipo de punto de conexión.

Important

Debe detener el servidor para poder cambiar el punto de conexión.

4. En Acciones, seleccione Detener.
5. En el cuadro de diálogo de confirmación que aparece, seleccione Detener para confirmar que desea detener el servidor.

Note

Antes de continuar con el siguiente paso, espere a que el estado del servidor cambie a Desconectado; esto puede tardar un par de minutos. Puede que tenga que elegir Actualizar en la página de Servidores para ver el cambio de estado.

6. Cuando el estado cambie a Sin conexión, seleccione el servidor para que aparezca la página de detalles del servidor.
7. En la sección Detalles del punto de conexión, elija Editar.

8. Elija VPC alojada como tipo de punto de conexión.
9. Seleccione Save.
10. En Acciones, seleccione Iniciar y espere a que el estado del servidor cambie a En línea; esto puede tardar un par de minutos.

Actualización del tipo de punto final del servidor mediante CloudFormation

En esta sección se describe CloudFormation cómo actualizar el servidor EndpointType aVPC. Utilice este procedimiento para los servidores Transfer Family que haya desplegado mediante CloudFormation. En este ejemplo, la plantilla original CloudFormation utilizada para implementar el servidor de Transfer Family se muestra de la siguiente manera:

```
AWS::Template::FormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC_ENDPOINT endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
      EndpointDetails:
        VpcEndpointId: !Ref VPCEndpoint
      EndpointType: VPC_ENDPOINT
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
  VPCEndpoint:
    Type: AWS::EC2::VPCEndpoint
    Properties:
      ServiceName: com.amazonaws.us-east-1.transfer.server
      SecurityGroupIds:
        - !Ref SecurityGroupId
      SubnetIds:
        - !Select [0, !Ref SubnetIds]
        - !Select [1, !Ref SubnetIds]
```

```

- !Select [2, !Ref SubnetIds]
VpcEndpointType: Interface
VpcId: !Ref VpcId

```

La plantilla se actualiza con los siguientes cambios:

- EndpointType cambió a VPC.
- Se ha eliminado el recurso `AWS::EC2::VPCEndpoint`.
- SecurityGroupId, SubnetIds y VpcId pasaron a la sección EndpointDetails del recurso `AWS::Transfer::Server`,
- Se ha eliminado VpcEndpointId propiedad de EndpointDetails.

La plantilla actualizada es el siguiente:

```

AWS TemplateFormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
      EndpointDetails:
        SecurityGroupIds:
          - !Ref SecurityGroupId
        SubnetIds:
          - !Select [0, !Ref SubnetIds]
          - !Select [1, !Ref SubnetIds]
          - !Select [2, !Ref SubnetIds]
        VpcId: !Ref VpcId
      EndpointType: VPC
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP

```

Para actualizar el tipo de punto final de los servidores Transfer Family implementados mediante CloudFormation

1. Detenga el servidor que desea actualizar siguiendo estos pasos.
 - a. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
 - b. En el panel de navegación, seleccione Servers (Servidores).
 - c. Seleccione la casilla de verificación del servidor para el que desee cambiar el tipo de punto de conexión.



Important

Debe detener el servidor para poder cambiar el punto de conexión.

- d. En Acciones, seleccione Detener.
 - e. En el cuadro de diálogo de confirmación que aparece, seleccione Detener para confirmar que desea detener el servidor.



Note

Antes de continuar con el siguiente paso, espere a que el estado del servidor cambie a Desconectado; esto puede tardar un par de minutos. Puede que tenga que elegir Actualizar en la página de Servidores para ver el cambio de estado.

2. Actualiza la CloudFormation pila
 - a. Abre la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
 - b. Seleccione la pila de que se va a utilizar para crear el servidor de Transfer Family.
 - c. Elija Actualizar.
 - d. Elija Reemplazar la plantilla actual
 - e. Cargue la nueva plantilla. CloudFormation Los conjuntos de cambios le ayudan a comprender cómo afectarán los cambios en las plantillas a los recursos en ejecución antes de implementarlos. En este ejemplo, se modificará el recurso del servidor de transferencia y se eliminará el recurso VPCEndpoint. El servidor de tipo punto de conexión de VPC crea un punto de conexión de VPC en su nombre y reemplaza el recurso original VPCEndpoint.

Tras cargar la nueva plantilla, el conjunto de cambios será el siguiente:

Change set preview				
Changes (2)				
Search changes				
Action	Logical ID	Physical ID	Resource type	Replacement
Modify	TransferServer	arn:aws:transfer:us-east-1:364810874344:server/s-6a7d04e12d494ec98	AWS::Transfer::Server	Conditional
Remove	VPCEndpoint	vpce-04e685f8702849573 ↗	AWS::EC2::VPCEndpoint	-

- f. Actualice la pila.
3. Cuando se complete la actualización de la pila, diríjase a la consola de administración de Transfer Family en <https://console.aws.amazon.com/transfer/>.
4. Reinicie el servidor. Elija el servidor en el que realizó la actualización y CloudFormation, a continuación, seleccione Iniciar en el menú Acciones.

Actualización del servidor EndpointType mediante la API

Puede usar el comando [describe-server](#) AWS CLI o el comando API [UpdateServer](#). El siguiente script de ejemplo detiene el servidor Transfer Family, lo actualiza EndpointType, elimina el VPC_ENDPOINT e inicia el servidor.

```
import boto3
import time

profile = input("Enter the name of the AWS account you'll be working in: ")
region_name = input("Enter the AWS Region you're working in: ")
server_id = input("Enter the AWS Transfer Server Id: ")

session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2", region_name=region_name)
transfer = session.client("transfer", region_name=region_name)

group_ids=[]

transfer_description = transfer.describe_server(ServerId=server_id)
```

```

if transfer_description['Server']['EndpointType']=='VPC_ENDPOINT':
    transfer_vpc_endpoint = transfer_description['Server']['EndpointDetails']
['VpcEndpointId']
    transfer_vpc_endpoint_descriptions =
ec2.describe_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
    for transfer_vpc_endpoint_description in
transfer_vpc_endpoint_descriptions['VpcEndpoints']:
        subnet_ids=transfer_vpc_endpoint_description['SubnetIds']
        group_id_list=transfer_vpc_endpoint_description['Groups']
        vpc_id=transfer_vpc_endpoint_description['VpcId']
        for group_id in group_id_list:
            group_ids.append(group_id['GroupId'])
    if transfer_description['Server']['State']=='ONLINE':
        transfer_stop = transfer.stop_server(ServerId=server_id)
        print(transfer_stop)
        time.sleep(300) #safe
        transfer_update =
transfer.update_server(ServerId=server_id,EndpointType='VPC',EndpointDetails={'SecurityGroupId
        print(transfer_update)
        time.sleep(10)
        transfer_start = transfer.start_server(ServerId=server_id)
        print(transfer_start)
        delete_vpc_endpoint =
ec2.delete_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])

```

Uso de nombres de host personalizados

El nombre de host del servidor es el nombre de host que los usuarios introducen en su cliente SFTP para conectar con su servidor. Puedes usar un dominio personalizado que hayas registrado como nombre de host de tu servidor cuando trabajes con él. AWS Transfer Family Por ejemplo, podría usar un nombre de host personalizado similar a este: `mysftpserver.mysubdomain.domain.com`.

Para redirigir el tráfico desde el dominio personalizado registrado al punto de conexión del servidor, puede utilizar Amazon Route 53 o cualquier proveedor del sistema de nombres de dominio (DNS). Route 53 es el servicio DNS que admite AWS Transfer Family de forma nativa.

Temas

- [Utilice Amazon Route 53 como proveedor de DNS](#)
- [Uso de otros proveedores de DNS](#)
- [Nombres de host personalizados para servidores no creados por consolas](#)

En la consola, puede elegir una de estas opciones para configurar un nombre de host personalizado:

- **Alias DNS de Amazon Route 53:** si el nombre de host que desea usar está registrado en Route 53. A continuación puede escribir el nombre de host.
- **Otro DNS:** si el nombre de host que desea usar está registrado en otro proveedor de DNS. A continuación puede escribir el nombre de host.
- **Ninguno:** para usar el punto de conexión del servidor y no usar un nombre de host personalizado.

Esta opción se establece al crear un nuevo servidor o editar la configuración de un servidor existente. Para obtener más información sobre cómo crear un nuevo servidor, consulte [Paso 2: Crea un SFTP-enabled servidor](#). Para obtener más información sobre cómo editar la configuración de un servidor existente, consulte [Editar detalles del servidor](#).

Para obtener más información sobre cómo usar su propio dominio como nombre de host del servidor y cómo se AWS Transfer Family usa Route 53, consulte las siguientes secciones.

Utilice Amazon Route 53 como proveedor de DNS

Al crear un servidor, puede utilizar Amazon Route 53 como proveedor de DNS. Antes de usar un dominio con Route 53, debe registrar el dominio. Para obtener más información, consulte [Funcionamiento del registro de un dominio](#) en la Guía para desarrolladores de Amazon Route 53.

Cuando utiliza Route 53 para proporcionar el enrutamiento de DNS a su servidor, AWS Transfer Family utiliza el nombre de host personalizado que ingresó para extraer su zona alojada. Cuando se AWS Transfer Family extrae una zona alojada, pueden ocurrir tres cosas:

1. Si eres nuevo en Route 53 y no tienes una zona alojada, AWS Transfer Family agrega una nueva zona alojada y un CNAME registro. El valor de este registro CNAME es el nombre de host del punto de conexión correspondiente a su servidor. Un CNAME es un nombre de dominio alternativo.
2. Si tiene una zona alojada en Route 53 sin ningún registro CNAME, AWS Transfer Family añade un registro CNAME a la zona alojada.
3. Si el servicio detecta que ya existe un registro CNAME en la zona alojada, aparecerá un error que indica que ya existe un registro CNAME. En este caso, cambie el valor del registro CNAME por el nombre de host de su servidor.

Para obtener más información acerca de las zonas alojadas en Route 53, consulte [Zona Alojada](#) en la Guía para desarrolladores de Amazon Route 53.

Uso de otros proveedores de DNS

Al crear un servidor, también puede utilizar proveedores de DNS diferentes a Amazon Route 53. Si utiliza un proveedor de DNS alternativo, asegúrese de que el tráfico de su dominio se dirija al punto de conexión de su servidor .

Para ello, establezca como dominio el nombre de host del punto de conexión correspondiente al servidor.

- En el caso de los puntos finales IPv4, el nombre de host tiene el siguiente aspecto en la consola:

`serverid.server.transfer.region.amazonaws.com`

- En el caso de los puntos finales de doble pila, el nombre de host tiene el siguiente aspecto en la consola:

`serverid.transfer-server.region.on.aws`

Note

Si su servidor tiene un punto final de VPC, el formato del nombre de host es diferente al descrito anteriormente. Para encontrar su punto de conexión de VPC, seleccione la VPC en la página de detalles del servidor y, a continuación, seleccione el ID del punto de conexión de VPC en el panel de control de la VPC. El punto de conexión es el primer nombre de DNS de los que aparecen en la lista.

Nombres de host personalizados para servidores no creados por consolas

Al crear un servidor mediante AWS Cloud Development Kit (AWS CDK) CloudFormation, o mediante la CLI, debe agregar una etiqueta si desea que ese servidor tenga un nombre de host personalizado. Al crear un servidor de Transfer Family mediante la consola, el etiquetado se realiza automáticamente.

Note

También necesita crear un registro DNS para redirigir el tráfico de su dominio al punto de conexión del servidor. Para obtener más información, consulte [Trabajar con registros](#) en la Guía para desarrolladores de Amazon Route 53.

Usa las siguientes claves para su nombre de host personalizado:

- Añada `transfer:customHostname` para mostrar el nombre de host personalizado en la consola.
- Si utiliza Route 53 como proveedor de DNS, agregue `transfer:route53HostedZoneId`. Esta etiqueta vincula el nombre de host personalizado a su ID de zona alojada de Route 53.

Para agregar el nombre de host personalizado, ejecute el siguiente comando CLI.

```
aws transfer tag-resource --arn arn:aws:transfer:region:Cuenta de AWS:server/server-ID
--tags Key=transfer:customHostname,Value="custom-host-name"
```

Por ejemplo:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:customHostname,Value="abc.example.com"
```

Si usa Route 53, ejecute el siguiente comando para vincular su nombre de host personalizado a su identificador de zona alojada de Route 53.

```
aws transfer tag-resource --arn server-ARN:server/server-ID --tags
Key=transfer:route53HostedZoneId,Value=HOSTED-ZONE-ID
```

Por ejemplo:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:route53HostedZoneId,Value=ABCDE1111222233334444
```

Asumiendo los valores de ejemplo del comando anterior, ejecute los siguientes comandos para ver las etiquetas:

```
aws transfer list-tags-for-resource --arn arn:aws:transfer:us-
east-1:111122223333:server/s-1234567890abcdef0
```

```
"Tags": [
  {
    "Key": "transfer:route53HostedZoneId",
    "Value": "/hostedzone/ABCDE1111222233334444"
  },
```

```
{
  "Key": "transfer:customHostname",
  "Value": "abc.example.com"
}
```

Note

Sus zonas alojadas públicas y sus identificadores están disponibles en Amazon Route 53. Inicie sesión en la consola de Route 53 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/route53/>.

Consideraciones sobre el Network Load Balancer para FTP y FTPS

Aunque recomendamos evitar los balanceadores de carga de red delante de AWS Transfer Family los servidores, si su implementación de FTP o FTPS requiere una NLB o NAT en la ruta de comunicación del cliente, siga estas recomendaciones:

- En el caso de un NLB, utilice el puerto 21 para las comprobaciones de estado, en lugar de los puertos 8192-8200.
- Para el AWS Transfer Family servidor, habilite la reanudación de la sesión TLS mediante la configuración. `TlsSessionResumptionMode = ENFORCED`

Note

Este es el modo recomendado, ya que proporciona una seguridad mejorada:

- Requiere que los clientes utilicen la reanudación de la sesión TLS para las conexiones posteriores.
- Ofrece garantías de seguridad más sólidas al garantizar la coherencia de los parámetros de cifrado.
- Ayuda a prevenir posibles ataques de degradación.
- Mantiene el cumplimiento de los estándares de seguridad a la vez que optimiza el rendimiento.

- Si es posible, deje de usar un NLB para aprovechar al máximo los límites de AWS Transfer Family rendimiento y conexión.

Para obtener más información sobre las alternativas de NLB, póngase en contacto con el equipo de gestión de AWS Transfer Family productos a través de AWS Support. Para obtener más información sobre cómo mejorar su postura de seguridad, consulte la entrada del blog [Seis consejos para mejorar la seguridad de su AWS Transfer Family servidor](#).

La guía de seguridad para los NLB se encuentra en [Evite colocar los NLB y los NAT delante de AWS Transfer Family servidores](#).

Transferencia de archivos a través de un punto de conexión mediante un cliente

Los archivos se transfieren a través del AWS Transfer Family servicio especificando la operación de transferencia en un cliente. AWS Transfer Family admite los siguientes clientes:

- Admitimos la versión 3 del protocolo SFTP.
- OpenSSH (macOS y Linux)

Note

Este cliente solo funciona con servidores que estén habilitados para el Protocolo de File Transfer (SFTP) Secure Shell (SSH).

- WinSCP (solo Microsoft Windows)
- Cyberduck (Windows, macOS y Linux)
- FileZilla (Windows, macOS y Linux)

Las limitaciones siguientes se aplican a cada cliente:

- El protocolo SCP no es compatible porque se considera inseguro. Puede utilizar el comando scp OpenSSH tal y como se describe en [Uso del comando scp](#)
- El número máximo de sesiones SFTP simultáneas y multiplexadas por conexión es de 10.
- Para las conexiones inactivas, el valor de tiempo de espera es de 1800 segundos (30 minutos) para todos los protocolos (). SFTP/FTP/FTPS Si no hay actividad después de este período, es posible que el cliente se desconecte. Para las conexiones que no responden:
 - El SFTP tiene un tiempo de espera de 300 segundos (5 minutos) cuando un cliente deja de responder por completo.

- El FTPS y el FTP tienen un tiempo de espera por inactividad de aproximadamente 10 minutos, que es gestionado por la biblioteca subyacente.
- Amazon S3 y Amazon EFS (debido al protocolo NFSv4) requieren que los nombres de archivo estén codificados. UTF-8 El uso de una codificación diferente puede provocar resultados inesperados. Para Amazon S3, consulte las [directrices de nomenclatura de claves de objetos](#).
- En el caso del Protocolo de File Transfer a través de SSL (FTPS), solo se admite el modo explícito. El modo implícito no es compatible.
- Para el Protocolo de File Transfer (FTP) y el FTPS, solo se admite el modo pasivo.
- Para FTP y FTPS, solo se admite el modo STREAM.
- Para FTP y FTPS, solo se admite el modo. Image/Binary
- Para FTP y FTPS, TLS: PROT C (desprotegido) El TLS para la conexión de datos es el valor predeterminado, pero el protocolo FTPS no admite PROT C. AWS Transfer Family Por lo tanto, en el caso del FTPS, es necesario emitir el PROT P para que se acepte la operación de datos.
- Si utiliza Amazon S3 para el almacenamiento de su servidor y si su cliente incluye la opción de utilizar varias conexiones para una sola transferencia, asegúrese de inhabilitarla. De lo contrario, las cargas de archivos grandes pueden fallar de forma impredecible. Tenga en cuenta que si utiliza Amazon EFS como servidor de almacenamiento, EFS admite varias conexiones para una sola transferencia.

La siguiente es una lista de los comandos disponibles para FTP y FTPS:

Comandos disponibles					
LABOR	HAZAÑA	MAYORÍA	PASS	RETR	STOR
AUTH	LANG	MKD	PASV	RMD	STOU
TAZA	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PUERTO	RINTO	SISTEMA
DELE	MFMT	NO	PWD	SIZE	TYPE
EPSV	MLSD	OPTA	QUIT	STAT	USER

Note

No es compatible con la APPE.

En el caso de SFTP, los usuarios que utilizan el directorio de inicio lógico en servidores que utilizan Amazon Elastic File System (Amazon EFS) no admiten actualmente las siguientes operaciones.

Comandos SFTP incompatibles			
SSH_FXP_R EADLINK	SSH_FXP_SYMLINK	SSH_FXP_STAT cuando el archivo solicitado es un enlace simbólico	SSH_FXP_R EALPATH cuando la ruta solicitada a contiene algún componente de enlace simbólico

Generación de un par de claves público-privadas

Para poder transferir un archivo, debe disponer de un par de claves público-privadas. Si no ha generado previamente un par de claves, consulte [Genere claves SSH para los usuarios administrados por el servicio](#).

Temas

- [Comandos disponibles SFTP/FTPS/FTP](#)
- [Encuentre su punto de conexión de Amazon VPC](#)
- [Evite errores setstat](#)
- [Uso de OpenSSH](#)
- [Utilice WinSCP](#)
- [Uso de Cyberduck](#)
- [Uso FileZilla](#)
- [Utilice un cliente Perl](#)
- [Utilice LFTP](#)
- [Procesamiento de carga posterior](#)
- [Mensajes SFTP](#)

Comandos disponibles SFTP/FTPS/FTP

En la siguiente tabla se describen los comandos disponibles para los protocolos SFTP, FTPS y FTP.
AWS Transfer Family

Note

En la tabla se mencionan los archivos y directorios de Amazon S3, que solo admite buckets y objetos: no hay jerarquía. Sin embargo, puede usar prefijos en los nombres de las claves de los objetos para dar a entender una jerarquía y organizar los datos de forma similar a las carpetas. Este comportamiento se describe en [Trabajar con metadatos de objetos](#) de la Guía del usuario de Amazon Simple Storage Service.

SFTP/FTPS/FTP Comandos

Comando	Amazon S3	Amazon EFS
cd	Soportado	compatible
chgrp	No compatible	Compatible (solo root o owner)
chmod	No compatible	Compatible (solo root)
chmtime	No compatible	compatible
chown	No compatible	Compatible (solo root)
get	compatible	Compatible (incluida la resolución de enlaces simbólicos)
ln -s	No compatible	Soportado
ls/dir	Soportado	Soportado
mkdir	Soportado	Soportado
put	Soportado	Soportado

Comando	Amazon S3	Amazon EFS
<code>pwd</code>	Soportado	compatible
<code>rename</code>	Solo se admite para archivos  Note No se admite el cambio de nombre que sobrescriba un archivo existente.	compatible  Note No se admite el cambio de nombre que sobrescriba un archivo o directorio existente.
<code>rm</code>	Soportado	compatible
<code>rmdir</code>	Compatible (solo directorios vacíos)	Soportado
<code>version</code>	Soportado	compatible

Encuentre su punto de conexión de Amazon VPC

Si el tipo de punto de conexión de su servidor de Transfer Family es VPC, no es fácil identificar el punto de conexión que se va a utilizar para transferir archivos. En este caso, utilice el siguiente procedimiento para encontrar su punto de conexión de Amazon VPC.

Para encontrar su punto de conexión de Amazon VPC

1. Diríjase a la página de detalles de su servidor.
2. En el panel de detalles del punto de conexión, seleccione la VPC.

Endpoint details

Edit

Status	Online	Custom hostname	-
Endpoint type	VPC (vpce- [redacted] [link icon])	Endpoint	-
VPC	vpc- [redacted]	Access	Info
FIPS Enabled	No	Internal	

3. En el panel de control de Amazon VPC, seleccione el ID del punto de conexión de VPC.
4. En la lista de nombres de DNS, el punto de conexión de su servidor es el primero de la lista.

VPC > Endpoints > vpce-[redacted]

vpce-[redacted] Actions

Details

Endpoint ID	Status	Creation time	Endpoint type
vpce-[redacted]	Available	Monday, April 4, 2022 at 10:51:31 EDT	Interface
VPC ID	Status message	Service name	Private DNS names enabled
vpc-[redacted] (no-name-specified)	-	com.amazonaws.us-east-2.transfer.server.c-0002	No
DNS record IP type	IP address type	DNS names	
ipv4	ipv4	vpce-[redacted]	
		[redacted]	
		[redacted].us-east-	
		2 [redacted]	
		- [redacted]	
		[redacted]	
		[redacted].us-east-	

Evite errores `setstat`

Al cargar el archivo, algunos clientes de transferencia de archivos SFTP pueden usar comandos como SETSTAT para intentar cambiar los atributos de los archivos remotos, lo que incluye la marca temporal y los permisos. Sin embargo, estos comandos no son compatibles con los sistemas de almacenamiento de objetos, como Amazon S3. Debido a esta incompatibilidad, la carga de archivos desde estos clientes puede provocar errores incluso si el archivo se carga correctamente.

- Cuando utilice la API `CreateServer` o `UpdateServer`, utilice la opción `SetStatOption` de `ProtocolDetails` para ignorar el error que se genera cuando el cliente intenta utilizar SETSTAT en un archivo que está cargando en un bucket de S3.
- Establezca el valor en `ENABLE_NO_OP` para hacer que el servidor de Transfer Family ignore el comando SETSTAT y cargue los archivos sin necesidad de realizar ningún cambio en el cliente SFTP.
- Tenga en cuenta que, si bien la `SetStatOption ENABLE_NO_OP` configuración ignora el error, genera una entrada de registro en CloudWatch los registros para que pueda determinar cuándo el cliente realiza una llamada a SETSTAT.

Para ver los detalles de la API de esta opción, consulte [ProtocolDetails](#)

Uso de OpenSSH

Esta sección contiene instrucciones para transferir archivos desde la línea de comandos mediante OpenSSH.

Note

Este cliente solo funciona con un SFTP-enabled servidor.

Temas

- [Con OpenSSH](#)
- [Uso del comando scp](#)

Con OpenSSH

Para transferir archivos AWS Transfer Family mediante la utilidad de línea de comandos OpenSSH

1. En Linux, macOS o Windows abra un terminal de comandos.
2. En el símbolo del sistema, escriba el comando siguiente:

```
sftp -i transfer-key sftp_user@service_endpoint
```

En el comando anterior, *sftp_user* es el nombre de usuario y *transfer-key* es la clave privada de SSH. Aquí *service_endpoint* se muestra el punto final del servidor, tal y como se muestra en la AWS Transfer Family consola del servidor seleccionado.

Note

Este comando usa la configuración que se encuentra en el `ssh_config` archivo predeterminado. A menos que haya editado este archivo anteriormente, SFTP usa el puerto 22. Puede especificar un puerto diferente (por ejemplo, 2222) añadiendo un `-P` indicador al comando, de la siguiente manera.

```
sftp -P 2222 -i transfer-key sftp_user@service_endpoint
```

Como alternativa, si siempre quiere usar el puerto 2222 o el puerto 22000, puede actualizar el puerto predeterminado en el `ssh_config` archivo.

Debe aparecer el símbolo del sistema `sftp`.

3. (Opcional) Para ver el directorio de inicio del usuario, introduzca el siguiente comando en la línea de comandos `sftp`:

```
pwd
```

4. Para cargar un archivo desde su sistema de archivos al servidor de Transfer Family, utilice el comando `put`. Por ejemplo, para cargar `hello.txt` (suponiendo que el archivo esté en el directorio actual del sistema de archivos), ejecute el siguiente comando en la línea de comandos `sftp`:

```
put hello.txt
```

Aparecerá un mensaje similar al siguiente para indicar que la transferencia está en curso o que se ha completado.

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

```
hello.txt 100% 127 0.1KB/s 00:00
```

Note

Desde que se crea el servidor, pueden transcurrir algunos minutos hasta que el servicio DNS del entorno pueda resolver el nombre de host de su punto de conexión.

Uso del comando **scp**

Transfer Family no es compatible con el protocolo SCP. Sin embargo, puede usar el comando `scp` OpenSSH si necesita esta funcionalidad.

La recomendación para usar SCP sobre SFTP es usar OpenSSH versión 9.0 o posterior. En la versión 9 y posteriores de OpenSSH, `scp` el comando utiliza de forma predeterminada el protocolo SFTP para las transferencias de archivos en lugar del protocolo SCP heredado.

Important

Asegúrese de que su servidor Transfer Family esté configurado para usar el acceso al directorio optimizado para S3.

Utilice WinSCP

Siga las instrucciones indicadas a continuación para transferir archivos desde la línea de comandos mediante WinSCP.

Note

Si utiliza WinSCP 5.19, puede conectarse directamente a Amazon S3 con sus credenciales AWS y archivos. `upload/download` Para obtener más información, consulte [Conexión al servicio Amazon S3](#).

Para transferir archivos AWS Transfer Family mediante WinSCP

1. Abra el cliente WinSCP.
2. En el cuadro de diálogo de inicio de sesión, en Protocolo de archivos, elija un protocolo: SFTP o FTP.

Si eligió FTP, elija una de las siguientes opciones para el cifrado:

- Sin cifrado para FTP
 - TLS/SSL Cifrado explícito para FTPS
3. ParaNombre del host, escriba el punto de conexión del servidor. El punto de conexión del servidor se encuentra en la página de Detalles del servidor. Para obtener más información, consulte [Vea los detalles de los servidores SFTP, FTPS y FTP](#).

Si el servidor usa un punto de conexión de VPC, consulte [Encuentre su punto de conexión de Amazon VPC](#).

4. En el número de puerto, introduzca lo siguiente:
 - **22** para SFTP
 - **21** para FTP/FTPS
5. En Nombre de usuario, introduzca el nombre del usuario que creó para su proveedor de identidad específico.

Consejo: El nombre de usuario debe ser uno de los usuarios que creó o configuró para su proveedor de identidad. AWS Transfer Family proporciona los siguientes proveedores de identidad:

- [Trabajar con usuarios de servicios administrados](#)
 - [Uso AWS de Directory Service para Microsoft Active Directory](#)
 - [Uso de proveedores de identidad personalizados](#)
6. Seleccione Avanzado para abrir el cuadro de diálogo Configuración avanzada del sitio. En la sección SSH, elija Autenticación.
 7. Busque y elija el archivo de clave privada de SSH en su sistema de archivos.

Si WinSCP le ofrece convertir la clave privada de SSH al formato PPK, elija Aceptar.

8. Elija Aceptar para volver al cuadro de diálogo Iniciar sesión y allí elija Guardar.

9. En el cuadro de diálogo Guardar sitio, elija Aceptar para completar la configuración de la conexión.
10. En el cuadro de diálogo de inicio de sesión, elija Herramientas y, a continuación, Preferencias.
11. En el cuadro de diálogo de preferencias, casilla de Transfer, elija Endurance.

En la opción Habilitar la transferencia resume/transfer a un nombre de archivo temporal, seleccione Inhabilitar.

 Important

Si dejas esta opción habilitada, aumentarán los costos de carga y disminuirán considerablemente su rendimiento. También puede provocar errores al cargar archivos de gran tamaño.

12. En Transferir, seleccione Fondo y desactive la casilla Usar varias conexiones para una sola transferencia.

Consejo: Si dejas esta opción seleccionada, las cargas de archivos grandes pueden fallar de forma impredecible. Por ejemplo, se pueden crear cargas multiparte huérfanas que conlleven gastos de Amazon S3. También puede producirse una corrupción silenciosa de los datos.

13. Ejecute la transferencia de archivos.

Puede utilizar la técnica de arrastrar y soltar para copiar archivos entre las ventanas de destino y origen. Puede usar los iconos de la barra de herramientas para cargar, descargar, eliminar, editar o modificar las propiedades de los archivos en WinSCP.

 Note

Esta nota no se aplica si utiliza Amazon EFS para el almacenamiento.

Los comandos que intentan cambiar los atributos de los archivos remotos, incluidas las marcas de tiempo, no son compatibles con los sistemas de almacenamiento de objetos como Amazon S3. Por lo tanto, si utiliza Amazon S3 como almacenamiento, asegúrese de deshabilitar la configuración de la marca de tiempo de WinSCP (o utilice `SetStatOption` como se describe en [Evite errores setstat](#)) antes de realizar transferencias de archivos. Para ello, en el cuadro de diálogo Preajustes de transferencia de WinSCP, desactive la opción de subida Establecer permisos y la opción común Mantener fecha.

Uso de Cyberduck

Siga las instrucciones indicadas a continuación para transferir archivos desde la línea de comandos mediante Cyberduck.

Para transferir archivos AWS Transfer Family mediante Cyberduck

1. Abra el cliente de [Cyberduck](#).
2. Elija Abrir conexión.
3. En el cuadro de diálogo Abrir conexión, elija un protocolo: SFTP (protocolo de transferencia de archivos SSH), FTP-SSL (AUTH TLS explícito) o FTP (protocolo de transferencia de archivos).
4. En Servidor, escriba el punto de conexión del servidor. El punto de conexión del servidor se encuentra en la página de Detalles del servidor. Para obtener más información, consulte [Vea los detalles de los servidores SFTP, FTPS y FTP](#).

Si el servidor usa un punto de conexión de VPC, consulte [Encuentre su punto de conexión de Amazon VPC](#).

5. En el número de puerto, introduzca lo siguiente:
 - **22** para SFTP
 - **21** para FTP/FTPS
6. En Usuario, escriba el nombre del usuario que creó en [Administración de usuarios para puntos finales de servidor](#).
7. Si selecciona SFTP, para la clave privada SSH, elija o introduzca la clave privada SSH.
8. Elija Conectar.
9. Ejecute la transferencia de archivos.

En función del lugar donde se encuentren los archivos, elija entre las acciones siguientes:

- En el directorio local (el origen), seleccione los archivos que desea transferir, arrástrelos y suéltelos en el directorio de Amazon S3 (el destino).
- En el directorio de Amazon S3 (el origen), seleccione los archivos que desea transferir, arrástrelos y suéltelos en el directorio local (el destino).

Uso FileZilla

Siga las instrucciones que aparecen a continuación para transferir archivos utilizando FileZilla.

FileZilla Para configurar una transferencia de archivos

1. Abra el FileZilla cliente.
2. Elija Archivo y, a continuación, Administrador del sitio.
3. En el cuadro de diálogo del administrador del sitio, elija Nuevo sitio.
4. En la pestaña General, en Protocolo, elija un protocolo: SFTP o FTP.

Si eligió FTP, elija una de las siguientes opciones para el cifrado:

- Utilice únicamente FTP simple (inseguro): para FTP
 - Utilice FTP explícito sobre TLS, si está disponible: para FTPS
5. En el campo Nombre de host, introduzca el protocolo que está utilizando, seguido del punto de conexión del servidor. El punto de conexión del servidor se encuentra en la página de Detalles del servidor. Para obtener más información, consulte [Vea los detalles de los servidores SFTP, FTPS y FTP](#).
 - Si utiliza SFTP, introduzca: `sftp://hostname`
 - Si utiliza FTPS, introduzca: `ftps://hostname`

Asegúrese de *hostname* reemplazarlo por el punto final del servidor actual.

Si el servidor usa un punto de conexión de VPC, consulte [Encuentre su punto de conexión de Amazon VPC](#).

6. En el número de puerto, introduzca lo siguiente:
 - **22** para SFTP
 - **21** para FTP/FTPS
7. Si selecciona SFTP, en Tipo de inicio de sesión, elija Archivo clave.

En Archivo de claves, elija o introduzca la clave privada SSH.

8. En Usuario, escriba el nombre del usuario que creó en [Administración de usuarios para puntos finales de servidor](#).
9. Elija Conectar.

10. Ejecute la transferencia de archivos.

Note

Si interrumpe una transferencia de archivos en curso, AWS Transfer Family podría escribir un objeto parcial en su bucket de Amazon S3. Si interrumpe una carga, compruebe que el tamaño del archivo en el bucket de Amazon S3 coincide con el tamaño del objeto original antes de continuar.

Utilice un cliente Perl

Si usa el cliente `Net::SFTP::Foreign` perl, debe configurar `elqueue_size`. 1 Por ejemplo:

```
my $sftp = Net::SFTP::Foreign->new('user@s-12345.server.transfer.us-east-2.amazonaws.com', queue_size => 1);
```

Note

Esta solución alternativa es necesaria para las revisiones de `Net::SFTP::Foreign` anteriores a [1.92.02](#).

Utilice LFTP

LFTP es un cliente FTP gratuito que permite a los usuarios realizar transferencias de archivos a través de la interfaz de línea de comandos desde la mayoría de las máquinas Linux.

En el caso de las descargas de archivos de gran tamaño, LFTP tiene un problema conocido con paquetes desordenados, que provoca un error en la transferencia de archivos.

Procesamiento de carga posterior

Puede ver la información de procesamiento posterior a la carga, incluidos los metadatos de los objetos de Amazon S3 y las notificaciones de eventos.

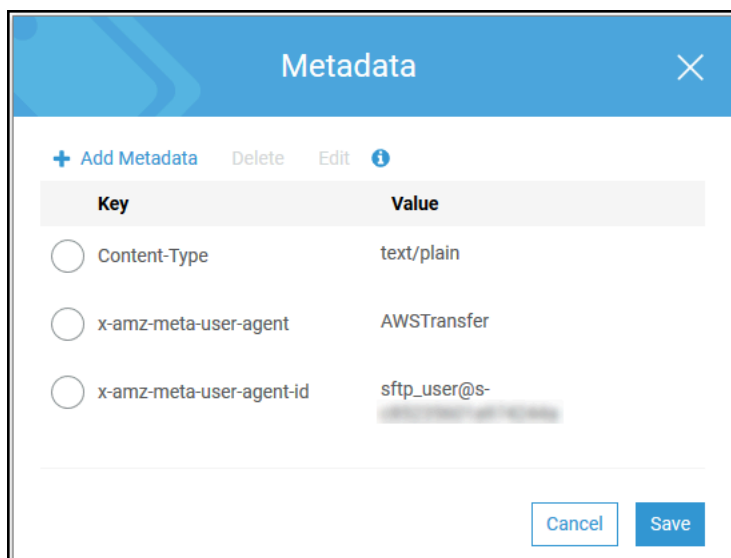
Temas

- [Metadatos de objeto de Amazon S3](#)

- [Notificaciones de eventos de Amazon S3](#)

Metadatos de objeto de Amazon S3

Como parte de los metadatos de su objeto, verá una clave llamada `x-amz-meta-user-agent` cuyo valor es `AWSTransfer` y `x-amz-meta-user-agent-id` cuyo valor es `username@server-id`. `username` es el usuario de Transfer Family que cargó el archivo y `server-id` es el servidor utilizado para la carga. Se puede acceder a esta información mediante la [HeadObject](#) operación en el objeto S3 dentro de la función Lambda.



The screenshot shows the 'Metadata' window in the AWS console. It has a blue header with a close button. Below the header are buttons for '+ Add Metadata', 'Delete', 'Edit', and an information icon. A table with two columns, 'Key' and 'Value', lists the following metadata:

Key	Value
☐ Content-Type	text/plain
☐ x-amz-meta-user-agent	AWSTransfer
☐ x-amz-meta-user-agent-id	sftp_user@s-

At the bottom right of the window are 'Cancel' and 'Save' buttons.

Notificaciones de eventos de Amazon S3

Cuando se carga un objeto en su bucket de S3 mediante Transfer Family, `RoleSessionName` aparece en el campo Solicitante de la [estructura de notificaciones de eventos de S3](#) como `[AWS:Role Unique Identifier]/username.sessionid@server-id`. Por ejemplo, el siguiente es el contenido de un ejemplo de campo Requester (Solicitante) de un registro de acceso de S3 para un archivo que se copió en el bucket de S3.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

En el campo Requester (Solicitante) de arriba, se muestra el rol de IAM al que se llamó `IamRoleName`. Para obtener más información sobre cómo configurar las notificaciones de eventos S3, consulte [Configuración de notificaciones de eventos de Amazon S3](#) en la Guía para desarrolladores de Amazon Simple Storage Service. Para obtener más información sobre los

identificadores únicos de rol AWS Identity and Access Management (IAM), consulte [Identificadores únicos en la Guía](#) del AWS Identity and Access Management usuario.

Mensajes SFTP

En esta sección se describen los mensajes del lado del cliente que puede recibir durante o después de las transferencias de archivos SFTP cuando utiliza un servidor Transfer Family. Para obtener más información sobre cualquier evento de SFTP, consulta los registros de tu cliente de SFTP. Puede usar esa información para solucionar cualquier error o enviar esa información a su equipo de red para que lo ayude a identificar el problema.

Mensajes SFTP del lado del cliente

Actividad	Description (Descripción)
AUTH_FAILURE	El usuario falló en la autenticación. Esto puede deberse a cualquier tipo de error provocado por un proveedor de identidades personalizado o por un usuario gestionado por un servicio. Los detalles del evento ayudan a aclarar la causa raíz del error.
CLOSE	Indica que un archivo o directorio abierto se ha cerrado correctamente.
CONNECTED/DISCONNECTED	Indica que la conexión y las desconexiones se han realizado correctamente.
CREATE_SYMLINK	Se creó un enlace simbólico (con éxito o sin éxito).
DELETE	Se ha eliminado un archivo (correctamente o sin éxito).
ERROR	Un error general e inesperado. La descripción asociada contiene información que puede ayudarle a usted o a sus administradores de red a identificar el problema específico.

Actividad	Description (Descripción)
EXIT_REASON	Se emite cuando un error inesperado provoca la finalización de la sesión de SFTP. El mensaje asociado al evento describe la causa.
MKDIR	Se creó un directorio (con éxito o sin éxito).
OPEN	Se ha abierto un archivo para su lectura o escritura (correctamente o sin éxito)
PARTIAL_CLOSE	El cliente se desconectó del servidor mientras un archivo aún estaba abierto y no se recibió ningún mensaje de CIERRE. Transfer Family almacena la parte recibida del archivo (que de hecho podría ser el archivo completo) y emite el evento PARTIAL_CLOSE para alertar al cliente sobre el problema. La integración de los flujos de trabajo también recibe un onPartialClose evento para gestionar el archivo de forma adecuada.
RENAME	Se ha cambiado el nombre de un archivo (correctamente o sin éxito)
RMDIR	Se ha eliminado un directorio (correctamente o sin éxito)

Actividad	Description (Descripción)
SETSTAT	Los atributos de un archivo se modifican (correctamente o sin éxito).  Note Transfer Family no es compatible con SETSTAT si utiliza Amazon S3 como almacenamiento. En Evite errores setstat esta sección se proporcionan detalles sobre cómo evitar SetStat errores desactivando la configuración. Esto evita que reciba un <code>unfail unsupported error</code> : en su lugar, recibirá <code>success but do nothing</code> un mensaje.
TLS_RESUME_FAILURE	El servidor está configurado para forzar la reanudación de la sesión TLS y el cliente no la admite.

Administración de usuarios para puntos finales de servidor

En las siguientes secciones, encontrará información sobre cómo añadir usuarios mediante AWS Transfer Family un proveedor de identidades personalizado AWS Directory Service for Microsoft Active Directory o personalizado.

Como parte de las propiedades de cada usuario se almacena también su clave pública de Secure Shell (SSH). Es necesario hacerlo para la autenticación basada en claves. La clave privada se almacenará localmente en el equipo de su usuario. Cuando el usuario envía una solicitud de autenticación a su servidor mediante un cliente, su servidor confirma que el usuario tiene acceso a la clave SSH privada asociada. A continuación, el servidor autentica correctamente al usuario.

 Note

Para la implementación y la administración automatizadas de usuarios con varias claves SSH, consulte. [Módulos Transfer Family Terraform](#)

Además debe especificar el directorio de inicio o de destino del usuario y asignar un rol de AWS Identity and Access Management (IAM) al usuario. Opcionalmente puede indicar una política de sesión para restringir el acceso de los usuarios únicamente al directorio de inicio del bucket de Amazon S3.

 Important

AWS Transfer Family impide que los nombres de usuario que tengan 1 o 2 caracteres se autenticuen en los servidores SFTP. Además, también bloqueamos el nombre de usuario root.

La razón de esto se debe al gran volumen de intentos de inicio de sesión maliciosos por parte de los escáneres de contraseñas.

Amazon EFS frente a Amazon S3

Características de cada opción de almacenamiento:

- Para limitar el acceso: Amazon S3 soporta políticas de sesión; Amazon EFS soporta identificadores de usuario, grupo y grupo secundario POSIX
- Ambos public/private admiten claves
- Ambos son compatibles con los directorios principales
- Ambos admiten directorios lógicos

 Note

En el caso de Amazon S3, la mayor parte del soporte para los directorios lógicos se realiza mediante API/CLI. Puede utilizar la casilla de verificación Restringido de la consola para bloquear a un usuario en su directorio de inicio, pero no puede especificar una estructura de directorios virtuales.

Directorios lógico

Si especifica valores de directorio lógico para el usuario, el parámetro que utilice depende del tipo de usuario.

- Para los usuarios administrados por el servicio, introduzca los valores del directorio lógico en `HomeDirectoryMappings`.
- Para los usuarios de proveedores de identidad personalizados, proporcione los valores del directorio lógico en `HomeDirectoryDetails`.

AWS Transfer Family admite la especificación de un `HomeDirectory` valor cuando se utiliza el `LOGICAL HomeDirectoryType`. Esto se aplica a los usuarios gestionados por el servicio, al acceso a Active Directory y a las implementaciones de proveedores de identidad personalizados cuando `HomeDirectoryDetails` se proporcionan en la respuesta.

Important

Al especificar a `HomeDirectory` con `LOGICAL HomeDirectoryType`, el valor debe asignarse a una de las asignaciones de directorios lógicos. El servicio lo valida tanto durante la creación del usuario como durante las actualizaciones para evitar configuraciones que no funcionen.

Comportamiento predeterminado

De forma predeterminada, si no se especifica, `HomeDirectory` se establece en «/» para el modo LÓGICO. Este comportamiento no ha cambiado y sigue siendo compatible con las definiciones de usuario existentes.

- Asegúrese de asignarlo `HomeDirectory` a una entrada y no a un objetivo. Para obtener más información, consulte [Reglas para el uso de directorios lógicos](#).
- Para obtener más información sobre la estructura de un directorio virtual, consulte [Estructura de directorio virtual](#).

Consideraciones sobre el proveedor de identidad personalizado

Al usar un proveedor de identidad personalizado, ahora puede especificar un `HomeDirectory` en la respuesta mientras usa `LOGICAL HomeDirectoryType`. La llamada a la `TestIdentityProvider` API

generará resultados correctos cuando el IDP personalizado especifique un HomeDirectory en modo LÓGICO.

Ejemplo de respuesta de IDP personalizada con HomeDirectory y LOGICAL: HomeDirectoryType

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-user-role",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectory": "/marketing",
  "HomeDirectoryDetails": "[{\"Entry\": \"\\\\\", \"Target\": \"\\\\/bucket/home\\\\\"}, {\"Entry\": \"\\\\/marketing\\\\\", \"Target\": \"\\\\/marketing-bucket/campaigns\\\\\"}]\""}
}
```

Cuotas de grupo de Active Directory

AWS Transfer Family tiene un límite predeterminado de 100 grupos de Active Directory por servidor. Si su caso de uso requiere más de 100 grupos, considere la posibilidad de utilizar una solución de proveedor de identidad personalizada, tal como se describe en [Simplifique la autenticación de Active Directory con un proveedor de identidad personalizado para AWS Transfer Family](#).

Este límite se aplica a los servidores que utilizan los siguientes proveedores de identidad:

- AWS Directory Service para Microsoft Active Directory
- AWS Directory Service para los servicios de dominio Entra ID

Si necesita solicitar un aumento del límite de servicio, consulte [Servicio de AWS las cuotas](#) en Referencia general de AWS. Si su caso de uso requiere más de 100 grupos, considere la posibilidad de utilizar una solución de proveedor de identidad personalizada, tal como se describe en [Simplifique la autenticación de Active Directory con un proveedor de identidad personalizado para AWS Transfer Family](#).

Para obtener información sobre la solución de problemas relacionados con los límites de grupos de Active Directory, consulte [Se han superado los límites de grupos de Active Directory](#).

Temas

- Trabajar con usuarios de servicios administrados
- Uso de proveedores de identidad personalizados
- Uso AWS de Directory Service para Microsoft Active Directory

- [Uso AWS de Directory Service para los servicios de dominio Entra ID](#)

Trabajar con usuarios de servicios administrados

Puede añadir usuarios administrados por el servicio Amazon S3 o Amazon EFS a su servidor, en función de la configuración del Dominio del servidor. Para obtener más información, consulte [Configuración de un punto final de servidor SFTP, FTPS o FTP](#).

Cuando utilice la modalidad con identidad administrada por el servicio, debe añadir los usuarios al servidor con protocolo habilitado de transferencia de archivos. Al hacerlo, cada nombre de usuario debe ser único en el servidor.

[Para añadir un usuario gestionado por el servicio mediante programación, consulta el ejemplo de la API. CreateUser](#)

Note

Para los usuarios gestionados por el servicio, hay un límite de 2000 entradas de directorio lógico. Para obtener información sobre el uso de directorios lógicos, consulte. [Uso de directorios lógicos para simplificar las estructuras de directorios de Transfer Family](#)

Temas

- [Añadir usuarios administrados por el servicio Amazon S3](#)
- [Añadir usuarios administrados por el servicio Amazon EFS](#)
- [Administración de usuarios administrados por servicios](#)

Añadir usuarios administrados por el servicio Amazon S3

Note

Si desea configurar un depósito de Amazon S3 multicuenta, siga los pasos que se mencionan en este artículo del Knowledge Center: [¿Cómo configuro mi AWS Transfer Family servidor para que utilice un depósito de Amazon Simple Storage Service que está en otra AWS cuenta?](#) .

Cómo añadir un usuario administrado por el servicio Amazon S3 a su servidor

1. Abra la AWS Transfer Family consola en y <https://console.aws.amazon.com/transfer/>, a continuación, seleccione Servidores en el panel de navegación.
2. En la página Servidores, seleccione la casilla de verificación situada junto al servidor al que desee añadir el usuario.
3. Seleccione Agregar usuario.
4. En la sección Configuración de usuario, en Nombre de usuario, introduzca el nombre de usuario. Este nombre de usuario debe tener un mínimo de 3 y un máximo de 100 caracteres. Puede utilizar los siguientes caracteres en el nombre de usuario: a-z, 0—9 A-Z, guión bajo '_', guión '-', punto '.' y signo '@'. El nombre de usuario no puede empezar con un guión '-', punto '.' o con el signo '@'.
5. En Acceso, elija el rol de IAM que creó anteriormente y que proporciona acceso a su bucket de Amazon S3.

Se trata del rol de IAM que creó siguiendo el procedimiento descrito en [Creación de una política y un rol de IAM](#). Ese rol de IAM incluye una política de IAM que proporciona acceso al bucket de Amazon S3. También incluye una relación de confianza con el AWS Transfer Family servicio, definida en otra política de IAM. Si necesita un control de acceso detallado para sus usuarios, consulte la entrada del blog [Mejore el control de acceso a los datos con Amazon AWS Transfer Family S3](#).

6. (Opcional) En Política, seleccione una de las siguientes opciones:
 - Ninguna
 - Políticas existentes
 - Seleccione una política de IAM: le permite elegir una política de sesión existente. Elija Ver para ver un objeto JSON que contiene los detalles de la política.
 - Auto-generate política basada en la carpeta de inicio: genera una política de sesión para usted. Elija Ver para ver un objeto JSON que contiene los detalles de la política.

Note

Si elige una Auto-generate política basada en la carpeta principal, no seleccione Restringido para este usuario.

Para obtener más información sobre las políticas de sesión [Creación de una política y un rol de IAM](#)[Creación de una política de sesión para un bucket de Amazon S3](#), consulte [o Enfoques de gestión dinámica de permisos](#).

7. En el directorio principal, elija el bucket de Amazon S3 para almacenar los datos que se van a transferir AWS Transfer Family. Especifique la ruta al directorio home al que llega el usuario cuando inicia sesión con su cliente.

Si deja este parámetro en blanco, se usará el directorio root del bucket de su Amazon S3. En ese caso, asegúrese de que el rol de IAM proporciona acceso al directorio root.

 Note

Le recomendamos que elija una ruta de directorio que contenga el nombre de usuario correspondiente, pues le permitirá usar con eficacia una política de sesión. La política de sesión limita el acceso de cada usuario a su directorio home en el bucket de Amazon S3.

8. (Opcional) En Restringido, seleccione la casilla de verificación para que los usuarios no puedan acceder a nada que esté fuera de esa carpeta y no puedan ver el nombre de la carpeta o el bucket de Amazon S3.

 Note

Asignar al usuario un directorio de inicio y restringirlo a ese directorio de inicio debería ser suficiente para bloquear el acceso del usuario a la carpeta designada. Si necesita aplicar más controles, utilice una política de sesión.

Si selecciona Restringido para este usuario, no podrá seleccionar la Auto-generate política en función de la carpeta de inicio, ya que la carpeta de inicio no es un valor definido para los usuarios restringidos.

9. En Clave pública de SSH, escriba el componente de clave pública del par de claves de SSH.

El servicio validará la clave antes de permitirle añadir un nuevo usuario.

 Note

Para obtener instrucciones sobre el modo de generar un par de claves de SSH, consulte [Genere claves SSH para los usuarios administrados por el servicio](#).

10. (Opcional) En Clave y Valor, escriba una o varias etiquetas como pares clave-valor y seleccione Agregar etiqueta.
11. Seleccione Add (Añadir) para agregar el nuevo usuario al servidor que haya elegido.

El nuevo usuario aparecerá en la sección Usuarios de la página Detalles del servidor.

Próximos pasos: para el siguiente paso, continúe con [Transferencia de archivos a través de un punto de conexión mediante un cliente](#).

Añadir usuarios administrados por el servicio Amazon EFS

Amazon EFS utiliza el modelo de permisos de archivos de la Interfaz de sistema operativo portátil (POSIX) para representar la propiedad de los archivos.

- Para obtener más información sobre la propiedad de los archivos de Amazon EFS, consulte [Propiedad de los archivos de Amazon EFS](#).
- Para obtener más información sobre la configuración de directorios para los usuarios de EFS, consulte [Configuración de los usuarios de Amazon EFS para Transfer Family](#).

Cómo añadir un usuario administrado por el servicio Amazon EFS a su servidor

1. Abra la AWS Transfer Family consola en y <https://console.aws.amazon.com/transfer/>, a continuación, seleccione Servidores en el panel de navegación.
2. En la página Servidores, seleccione el servidor Amazon EFS al que desee añadir un usuario.
3. Seleccione Añadir usuario para mostrar la página Añadir usuario.
4. En la sección Configuración de usuario, aplique los siguientes ajustes.
 - a. El Nombre de usuario, debe tener un mínimo de 3 y un máximo de 100 caracteres. Puede utilizar los siguientes caracteres en el nombre de usuario: a—z, 0—9 A-Z, guión bajo '_', guión '-', punto '.', y en el signo «@». El nombre de usuario no puede comenzar por un guion (-), un punto (.), ni una arroba (@).

- b. Para el Identificador de usuario y el Identificador de grupo, tenga en cuenta lo siguiente:
- Para el primer usuario que cree, le recomendamos que introduzca un valor de **0** tanto para el Identificador de grupo como para el Identificador de usuario. Esto otorga al usuario privilegios de administrador para Amazon EFS.
 - Para usuarios adicionales, introduzca el ID de usuario POSIX y el ID de grupo del usuario. Estos identificadores se utilizan para todas las operaciones de Amazon Elastic File System realizadas por el usuario.
 - Para el Identificador de usuario y el Identificador de grupo, no utilice ceros a la izquierda. Por ejemplo, **12345** es aceptable, pero **012345** no lo es.
- c. (Opcional) Para los Identificadores de grupo secundarios, introduzca uno o más ID de grupo POSIX adicionales para cada usuario, separados por comas.
- d. En Acceso, elija el rol de IAM que:
- Otorga al usuario acceso únicamente a los recursos de Amazon EFS (sistemas de archivos) a los que desea que accedan.
 - Define qué operaciones del sistema de archivos puede y no puede realizar el usuario.

Le recomendamos que utilice el rol de IAM para la selección del sistema de archivos Amazon EFS con acceso y read/write permisos de montaje. Por ejemplo, la combinación de las dos políticas AWS administradas siguientes, si bien es bastante permisiva, otorga los permisos necesarios al usuario:

- AmazonElasticFileSystemClientFullAccess
- AWSTransferConsoleFullAccess

Para obtener más información, consulte la publicación del blog de [Soporte de AWS Transfer Family para Amazon Elastic File System](#).

- e. Para el Directorio de inicio, haga lo siguiente:
- Elija el sistema de archivos Amazon EFS que desee utilizar para almacenar los datos que desee transferir con AWS Transfer Family.
 - Decida si desea establecer el directorio de inicio como Restringido. Si se establece el directorio de inicio en Restringido, se producen los siguientes efectos:

- Los usuarios de Amazon EFS no pueden acceder a ningún archivo o directorio fuera de esa carpeta.
- Los usuarios de Amazon EFS no pueden ver el nombre del sistema de archivos de Amazon EFS (fs-xxxxxxx).

 Note

Al seleccionar la opción Restringido, los enlaces simbólicos no se resuelven para los usuarios de Amazon EFS.

- (Opcional) Introduzca la ruta al directorio de inicio en el que desea que estén los usuarios cuando inicien sesión con su cliente.

Si no especifica un directorio de inicio, se utilizará el directorio raíz del sistema de archivos Amazon EFS. En ese caso, asegúrese de que su rol de IAM proporciona acceso a este directorio raíz.

5. En Clave pública de SSH, escriba el componente de clave pública del par de claves de SSH.

El servicio validará la clave antes de permitirle añadir un nuevo usuario.

 Note

Para obtener instrucciones sobre el modo de generar un par de claves de SSH, consulte [Genere claves SSH para los usuarios administrados por el servicio](#).

6. (Opcional) Introduzca cualquier etiqueta para el usuario. En Clave y Valor, escriba una o varias etiquetas como pares clave-valor y seleccione Agregar etiqueta.
7. Seleccione Add (Añadir) para agregar el nuevo usuario al servidor que haya elegido.

El nuevo usuario aparecerá en la sección Usuarios de la página Detalles del servidor.

Problemas que pueden surgir al usar SFTP por primera vez en su servidor de Transfer Family:

- Si ejecutas el comando `sftp` y no aparece el mensaje, es posible que aparezca el siguiente mensaje:

```
Couldn't canonicalize: Permission denied
```

Need `pwd`

En este caso, debe aumentar los permisos de política del rol de usuario. Puede añadir una política AWS gestionada, como. `AmazonElasticFileSystemClientFullAccess`

- Si lo introduce `pwd` cuando se le `sftp` solicita ver el directorio principal del usuario, es posible que aparezca el siguiente mensaje, donde `USER-HOME-DIRECTORY` se encuentra el directorio principal del usuario de SFTP:

```
remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
```

En este caso, debería poder navegar hasta el directorio de inicio (`cd ..`) y crear el directorio de inicio del usuario (`mkdir username`).

Próximos pasos: para el siguiente paso, continúe con [Transferencia de archivos a través de un punto de conexión mediante un cliente](#).

Administración de usuarios administrados por servicios

En esta sección, puede encontrar información sobre cómo ver una lista de usuarios, cómo editar los detalles de los usuarios y cómo agregar una clave pública SSH.

- [Ver una lista de usuarios](#)
- [Ver o editar los detalles del usuario](#)
- [Eliminar un usuario](#)
- [Añadir clave pública SSH](#)
- [Eliminar la clave pública SSH](#)

Cómo encontrar una lista de sus usuarios

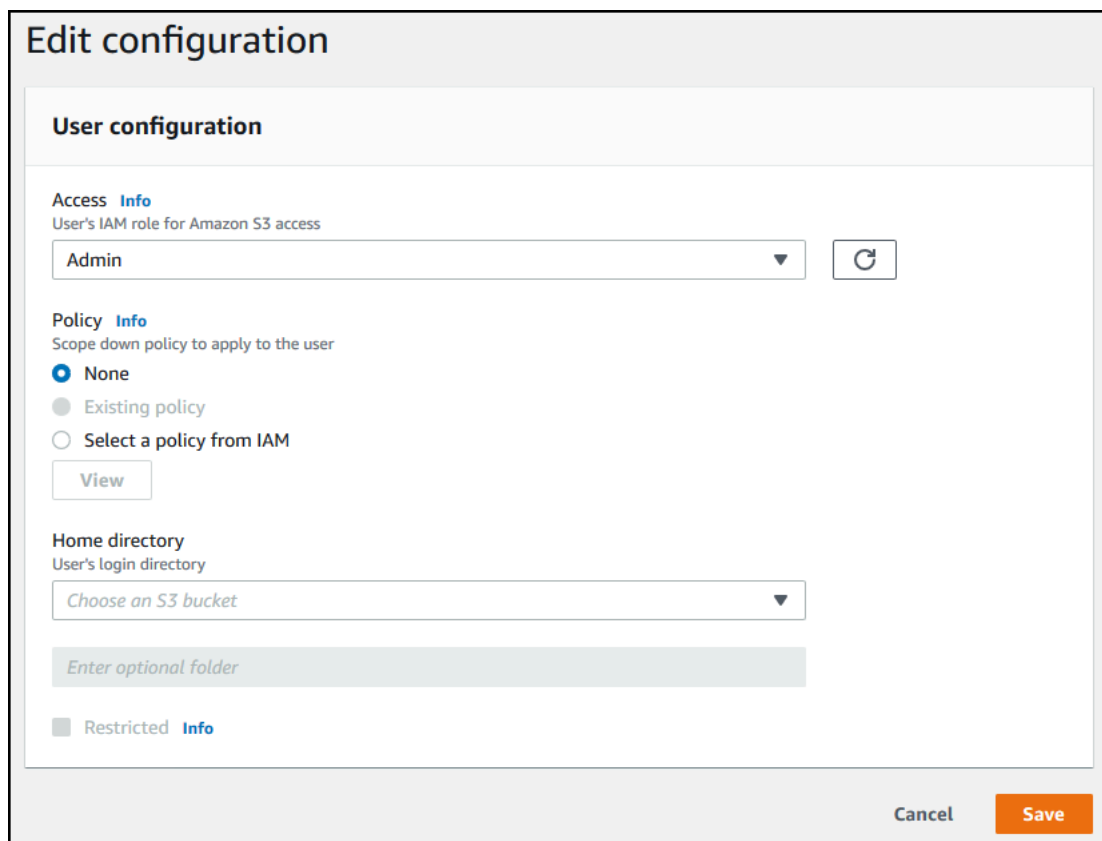
1. Abre la AWS Transfer Family consola en. <https://console.aws.amazon.com/transfer/>
2. Seleccione Servidores en el panel de navegación para mostrar la página Servidores.
3. Elija el identificador en la columna ID de servidor para ver la página Detalles del servidor.
4. En Usuarios, consulte una lista de usuarios.

Visualización o edición de los detalles del usuario

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. Seleccione Servidores en el panel de navegación para mostrar la página Servidores.
3. Elija el identificador en la columna ID de servidor para ver la página Detalles del servidor.
4. En Usuarios, elija un nombre de usuario para ver la página de Detalles del usuario.

Puede cambiar las propiedades del usuario en esta página seleccionando Editar.

5. En la página de Detalles del usuario, seleccione Editar junto a Configuración del usuario.



6. En la página Editar configuración, en Acceso, elija el rol de IAM que creó anteriormente y que proporciona acceso a su bucket de Amazon S3.

Se trata del rol de IAM que creó siguiendo el procedimiento descrito en [Creación de una política y un rol de IAM](#). Ese rol de IAM incluye una política de IAM que proporciona acceso al bucket de Amazon S3. También incluye una relación de confianza con el AWS Transfer Family servicio, definida en otra política de IAM.

7. (Opcional) Para la política, seleccione una de las siguientes opciones:
 - Ninguna

- Políticas existentes
- Seleccione una política de IAM para elegir una política existente. Elija Ver para ver un objeto JSON que contiene los detalles de la política.

Para obtener más información sobre las políticas de sesiones, consulte [Creación de una política y un rol de IAM](#). Para obtener más información sobre la creación de una política de sesión, consulte [Creación de una política de sesión para un bucket de Amazon S3](#).

8. En el directorio principal, elija el bucket de Amazon S3 para almacenar los datos que se van a transferir AWS Transfer Family. Especifique la ruta al directorio home al que llega el usuario cuando inicia sesión con su cliente.

Si deja este parámetro en blanco, se usará el directorio root del bucket de su Amazon S3. En ese caso, asegúrese de que el rol de IAM proporciona acceso al directorio root.

 Note

Le recomendamos que elija una ruta de directorio que contenga el nombre de usuario correspondiente, pues le permitirá usar con eficacia una política de sesión. La política de sesión limita el acceso de cada usuario a su directorio home en el bucket de Amazon S3.

9. (Opcional) En Restringido, seleccione la casilla de verificación para que los usuarios no puedan acceder a nada que esté fuera de esa carpeta y no puedan ver el nombre de la carpeta o el bucket de Amazon S3.

 Note

Al asignar al usuario un directorio de inicio y restringirlo a ese directorio de inicio, esto debería ser suficiente para bloquear el acceso del usuario a la carpeta designada. Utilice una política de sesión cuando necesite aplicar más controles.

10. Seleccione Save (Guardar) para guardar los cambios.

Cómo eliminar un usuario

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. Seleccione Servidores en el panel de navegación para mostrar la página Servidores.

3. Elija el identificador en la columna ID de servidor para ver la página Detalles del servidor.
4. En Usuarios, elija un nombre de usuario para ver la página de Detalles del usuario.
5. En la página de Detalles del usuario, seleccione Eliminar a la derecha del nombre de usuario.
6. En la ventana de diálogo de confirmación que aparece, escriba la palabra **delete**, y luego seleccione Eliminar para confirmar que desea eliminar al usuario.

El usuario se elimina de la lista de usuarios.

Para añadir una clave pública SSH para un usuario

1. Abre la AWS Transfer Family consola en. <https://console.aws.amazon.com/transfer/>
2. En el panel de navegación, seleccione Servers (Servidores).
3. Elija el identificador en la columna ID de servidor para ver la página Detalles del servidor.
4. En Usuarios, elija un nombre de usuario para ver la página de Detalles del usuario.
5. Seleccione Add SSH public key (Añadir clave pública de SSH) para añadir una nueva clave SSH pública a un usuario.

 Note

Las claves SSH las usan solo los servidores que están habilitados para el Protocolo de File Transfer (SFTP) Secure Shell (SSH). Para obtener más información sobre el modo de generar un par de claves SSH, consulte [Genere claves SSH para los usuarios administrados por el servicio](#).

6. En SSH public key (Clave pública de SSH), escriba el componente de clave pública del par de claves de SSH.

El servicio validará la clave antes de permitirle añadir un nuevo usuario. El formato de la clave SSH es `ssh-rsa string`. Para generar un par de claves de SSH, consulte [Genere claves SSH para los usuarios administrados por el servicio](#).

7. Seleccione Añadir clave.

Para eliminar una clave pública SSH de un usuario

1. Abre la AWS Transfer Family consola en. <https://console.aws.amazon.com/transfer/>
2. En el panel de navegación, seleccione Servers (Servidores).

3. Elija el identificador en la columna ID de servidor para ver la página Detalles del servidor.
4. En Usuarios, elija un nombre de usuario para ver la página de Detalles del usuario.
5. Para eliminar una clave pública, selecciona la casilla de verificación de su clave SSH y selecciona Eliminar.

Uso de proveedores de identidad personalizados

AWS Transfer Family ofrece varias opciones para que los proveedores de identidad personalizados autenticuen y autoricen a los usuarios a transferir archivos de forma segura. Estos son los enfoques principales:

- [Solución de proveedor de identidad personalizada](#)—En este tema se describe la solución de proveedor de identidad personalizado Transfer Family, mediante un conjunto de herramientas alojado en GitHub

Note

Para la mayoría de los casos de uso, esta es la opción recomendada. En concreto, si necesita admitir más de 100 grupos de Active Directory, la solución de proveedor de identidades personalizado ofrece una alternativa escalable sin limitaciones de grupo. Esta solución se describe en la entrada del blog titulada [Simplifique la autenticación de Active Directory con un proveedor de identidad personalizado para AWS Transfer Family](#).

- [Uso de Amazon API Gateway para integrar su proveedor de identidad](#)—En este tema se describe cómo utilizar una AWS Lambda función para respaldar un método de Amazon API Gateway.

Puede proporcionar una interfaz RESTful con un único método de Amazon API Gateway. Transfer Family utiliza este método para conectarse con su proveedor de identidad, que autentica y autoriza a los usuarios a acceder a Amazon S3 o Amazon EFS. Utilice esta opción si necesita una API RESTful para integrar su proveedor de identidad o si desea utilizarla para aprovechar sus capacidades AWS WAF para el bloqueo geográfico o las solicitudes de limitación de velocidad. Para obtener más información, consulte [Uso de Amazon API Gateway para integrar su proveedor de identidad](#).

- [Enfoques de gestión dinámica de permisos](#)—En este tema se describen los enfoques para gestionar los permisos de los usuarios de forma dinámica mediante políticas de sesión.

Para autenticar a sus usuarios, puede utilizar su proveedor de identidades actual con AWS Transfer Family. El proveedor de identidad se integra mediante una función de AWS Lambda que autentica y autoriza a los usuarios a acceder a Amazon S3 o Amazon Elastic File System (Amazon EFS). Para obtener más información, consulte [Se utiliza AWS Lambda para integrar su proveedor de identidad](#). También puede acceder a los CloudWatch gráficos para obtener métricas como el número de archivos y bytes transferidos en la consola de AWS Transfer Family administración, lo que le ofrece un panel único para supervisar las transferencias de archivos mediante un panel centralizado.

- Transfer Family ofrece una entrada de blog y un taller que lo guiarán a través de la creación de una solución de transferencia de archivos. Esta solución aprovecha los SFTP/FTPS puntos de AWS Transfer Family enlace gestionados y Amazon Cognito y DynamoDB para la gestión de usuarios.

La entrada del blog está disponible en [Uso de Amazon Cognito como proveedor de identidad con Amazon AWS Transfer Family S3](#). Puede ver los detalles del taller [aquí](#).

Note

En el caso de los proveedores de identidad personalizados, el nombre de usuario debe tener un mínimo de 3 y un máximo de 100 caracteres. Puede utilizar los siguientes caracteres en el nombre de usuario: a—z, 0—9 A-Z, guión bajo '_', guión '-', punto '.' y signo '@'. El nombre de usuario no puede empezar con un guión '-', punto '.' o con el signo '@'.

Al implementar un proveedor de identidad personalizado, tenga en cuenta las siguientes prácticas recomendadas:

- Implemente la solución en la misma Cuenta de AWS región que sus servidores Transfer Family.
- Implemente el principio de privilegios mínimos al configurar las funciones y políticas de IAM.
- Utilice funciones como la lista de direcciones IP permitidas y el registro estandarizado para mejorar la seguridad.
- Pruebe minuciosamente su proveedor de identidad personalizado en un entorno que no sea de producción antes del despliegue.

Temas

- [Solución de proveedor de identidad personalizada](#)
- [Se utiliza AWS Lambda para integrar su proveedor de identidad](#)
- [Uso de Amazon API Gateway para integrar su proveedor de identidad](#)
- [Uso de varios métodos de autenticación](#)
- [Compatibilidad con IPv6 para proveedores de identidad personalizados](#)

Solución de proveedor de identidad personalizada

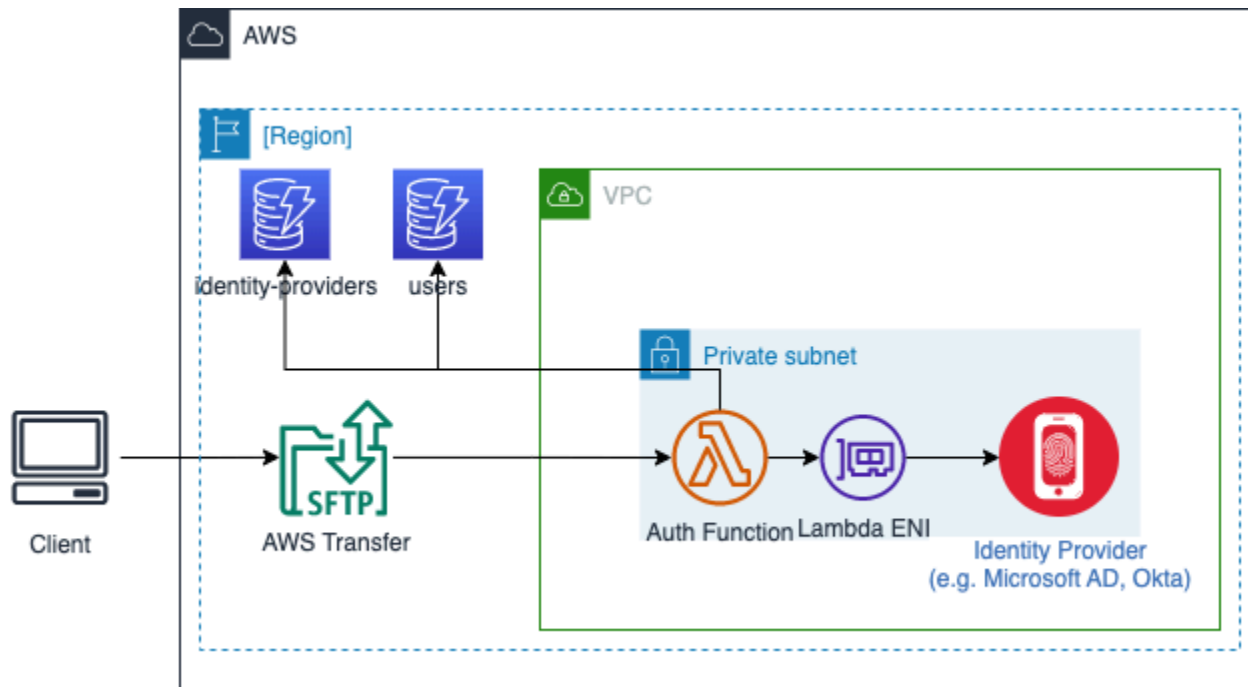
La solución de proveedor de identidad AWS Transfer Family personalizado es una solución modular de proveedor de identidad personalizado que resuelve muchos casos de uso comunes de autenticación y autorización que tienen las empresas al implementar el servicio. Esta solución proporciona una base reutilizable para implementar proveedores de identidad personalizados con una configuración de sesión granular por usuario y separa la lógica de autenticación y autorización, lo que ofrece una base flexible y fácil de mantener para varios casos de uso.

Con la solución de proveedor de identidad AWS Transfer Family personalizado, puede abordar los casos de uso más comunes de autenticación y autorización empresarial. Esta solución modular ofrece:

- Una base reutilizable para implementar proveedores de identidad personalizados
- Configuración granular de sesión por usuario
- Lógica de autenticación y autorización separadas

Detalles de implementación del kit de herramientas de identidad personalizado

La solución proporciona una base flexible y fácil de mantener para varios casos de uso. Para empezar, revise el kit de herramientas en y <https://github.com/aws-samples/toolkit-for-aws-transfer-family>, a continuación, siga las instrucciones de implementación de la sección [Primeros pasos](#).



Note

Si anteriormente ha utilizado plantillas y ejemplos de proveedores de identidad personalizados, considere la posibilidad de adoptar esta solución en su lugar. En el futuro, los módulos específicos del proveedor se estandarizarán en esta solución. El mantenimiento continuo y las mejoras en las funciones se aplicarán a esta solución.

Esta solución contiene patrones estándar para implementar un proveedor personalizado que tenga en cuenta detalles como el registro y dónde almacenar los metadatos adicionales de la sesión necesarios AWS Transfer Family, como el `HomeDirectoryDetails` parámetro. Esta solución proporciona una base reutilizable para implementar proveedores de identidad personalizados con una configuración de sesión granular por usuario y desvincula la lógica de autenticación del proveedor de identidades de la lógica reutilizable que crea una configuración que se devuelve a Transfer Family para completar la autenticación y establecer los ajustes de la sesión.

El código y los recursos de apoyo de esta solución están disponibles en. <https://github.com/aws-samples/toolkit-for-aws-transfer-family>

El kit de herramientas contiene las siguientes funciones:

- Una [AWS Serverless Application Model](#) plantilla que proporciona los recursos necesarios. Si lo desea, implemente y configure Amazon API Gateway para incorporarlo AWS WAF, tal y como se

describe en la entrada del blog [AWS Transfer Family Securing with AWS Web Application Firewall y Amazon API Gateway](#).

- Un esquema de [Amazon DynamoDB](#) para almacenar los metadatos de configuración sobre los proveedores de identidad, incluidos los ajustes de sesión de usuario, `HomeDirectoryDetails` como `Role`, y. `Policy`
- Un enfoque modular que le permite añadir nuevos proveedores de identidad a la solución en el futuro, en forma de módulos.
- Recuperación de atributos: si lo desea, recupere los atributos del rol de IAM y del perfil POSIX (UID y GID) de los proveedores de identidad compatibles, como AD, LDAP y Okta.
- Soporte para varios proveedores de identidad conectados a un único servidor de Transfer Family y varios servidores de Transfer Family mediante la misma implementación de la solución.
- Built-in Verificación de las listas de direcciones IP permitidas, como las listas de direcciones IP permitidas, que se pueden configurar opcionalmente por usuario o por proveedor de identidad.
- Registro detallado con nivel de registro configurable y soporte de rastreo para facilitar la resolución de problemas.

Antes de empezar a implementar la solución de proveedor de identidad personalizado, debe disponer de los siguientes recursos. AWS

- Una Amazon Virtual Private Cloud (VPC) con subredes privadas, con conectividad a Internet a través de una puerta de enlace NAT o un punto de enlace de puerta de enlace de DynamoDB.
- Los permisos de IAM adecuados para realizar las siguientes tareas:
 - Implemente la `custom-idp.yaml` CloudFormation plantilla,
 - Crear AWS CodePipeline proyectos
 - Crea AWS CodeBuild proyectos
 - Cree funciones y políticas de IAM

 Important

Debe implementar la solución en el mismo lugar Región de AWS que contiene Cuenta de AWS los servidores Transfer Family de destino.

Proveedores de identidades compatibles

La siguiente lista contiene detalles de los proveedores de identidad compatibles con la solución de proveedor de identidad personalizado.

Proveedor	Flujos de contraseñas	Flujos de claves públicas	Multi-factor	Recuperación de atributos	Details
Active Directory y LDAP	Sí	Sí	No	Sí	La verificación del usuario se puede realizar como parte del flujo de autenticación de clave pública.
Argon2 (hash local)	Sí	No	No	No	Los hashes de Argon2 se almacenan en el registro de usuario para los casos de uso de autenticación basada en contraseñas «locales».
Amazon Cognito	Sí	No	Sí*	No	Time-based One-Time Solo para la autenticación multifactorial basada en

Proveedor	Flujos de contraseñas	Flujos de claves públicas	Multi-factor	Recuperación de atributos	Details
					contraseñas (TOTP). * No se admite el SMS-based MFA.
Ingresar ID (anteriormente Azure AD)	Sí	No	No	No	
Okta	Sí	Sí	Sí*	Sí	TOTP-based Solo MFA.
Clave pública	No	Sí	No	No	Las claves públicas se almacenan en el registro de usuario de DynamoDB.
Secrets Manager	Sí	Sí	No	No	

Se utiliza AWS Lambda para integrar su proveedor de identidad

En este tema se describe cómo crear una AWS Lambda función que se conecte a su proveedor de identidades personalizado. Puede usar cualquier proveedor de identidad personalizado, como Okta, Secrets Manager o un almacén de datos personalizado que incluya lógica de autorización y autenticación. OneLogin

En la mayoría de los casos de uso, la forma recomendada de configurar un proveedor de identidades personalizado es utilizar el [Solución de proveedor de identidad personalizada](#).

 Note

Antes de crear un servidor de Transfer Family que utilice Lambda como proveedor de identidades, debe crear la función. Para ver una función de Lambda de ejemplo, consulte [Ejemplo de función de Lambda](#). O bien, puede implementar una CloudFormation pila que utilice uno de los [Plantillas de función de Lambda](#). Además, asegúrese de que la función de Lambda utilice una política basada en recursos que confíe en Transfer Family. Para ver una política de ejemplo, consulte [Política basada en recursos de Lambda](#).

1. Abra la [consola de AWS Transfer Family](#).
2. Seleccione Crear servidor para abrir la página Crear servidor. En Elegir un proveedor de identidad, elija un proveedor de identidad personalizado, como se muestra en la siguiente captura de pantalla.

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

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

Cancel

Previous

Next

Note

La selección de métodos de autenticación solo está disponible si habilita SFTP como uno de los protocolos del servidor de Transfer Family.

3. Asegúrese de que esté seleccionado el valor predeterminado, Usar AWS Lambda para conectar su proveedor de identidad.
4. Para la AWS Lambda función, seleccione el nombre de su Función de Lambda.

5. Rellene las casillas restantes y, a continuación, seleccione Crear servidor. Para obtener más información sobre los pasos restantes para crear un servidor, consulte [Configuración de un punto final de servidor SFTP, FTPS o FTP](#).

Política basada en recursos de Lambda

Debe tener una política que haga referencia al servidor de Transfer Family y a los ARN Lambda. Por ejemplo, puede usar la siguiente política con la función de Lambda que se conecta a su proveedor de identidad. La política es un JSON de escape en forma de cadena.

```
"Policy":
"{\"Version\":\"2012-10-17\",
  \"Id\":\"default\",
  \"Statement\":[
    {\"Sid\":\"AllowTransferInvocation\",
      \"Effect\":\"Allow\",
      \"Principal\":{\"Service\":\"transfer.amazonaws.com\"},
      \"Action\":\"lambda:InvokeFunction\",
      \"Resource\":\"arn:aws:lambda:region:123456789012:function:my-lambda-auth-function\",
      \"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
        \"arn:aws:transfer:region:123456789012:server/server-id\"}}}}
  ]}"
```

Note

En el ejemplo de política anterior, sustituya cada *user input placeholder* una por su propia información.

Estructura de mensaje de evento

La estructura de los mensajes de eventos del servidor SFTP enviados a la función de Lambda del autorizador para un IDP personalizado es la siguiente.

```
{
  "username": "value",
  "password": "value",
  "protocol": "SFTP",
```

```
"serverId": "s-abcd123456",  
"sourceIp": "192.168.0.100"  
}
```

Siendo username y password los valores de las credenciales de inicio de sesión que se envían al servidor.

Por ejemplo, introduzca el siguiente comando para la conexión:

```
sftp bobusa@server_hostname
```

Se le pedirá que escriba su contraseña:

```
Enter password:  
mysecretpassword
```

Puede comprobarlo desde la función de Lambda al imprimir el evento pasado desde la función de Lambda. Debería parecerse a lo que sigue.

```
{  
  "username": "bobusa",  
  "password": "mysecretpassword",  
  "protocol": "SFTP",  
  "serverId": "s-abcd123456",  
  "sourceIp": "192.168.0.100"  
}
```

La estructura de eventos es similar para FTP y FTPS: la única diferencia es que esos valores se utilizan para el parámetro protocol y no para SFTP.

funciones de Lambda para autenticación

Para implementar diferentes estrategias de autenticación, edite la función de Lambda. Para ayudarte a satisfacer las necesidades de tu aplicación, puedes implementar una CloudFormation pila. Para obtener más información sobre Lambda, consulte la [Guía para AWS Lambda desarrolladores o Cómo crear](#) funciones [Lambda](#) con. Node.js

Temas

- [Valores de Lambda válidos](#)
- [Ejemplo de función de Lambda](#)

- [Prueba de su configuración](#)
- [Plantillas de función de Lambda](#)

Valores de Lambda válidos

En la siguiente tabla se describen los detalles de los valores que Transfer Family acepta para las funciones de Lambda que se utilizan para los proveedores de identidades personalizados.

Valor	Description (Descripción)	Obligatorio
Role	Especifica el nombre de recurso de Amazon (ARN) del rol de IAM que controla el acceso de sus usuarios a su bucket de Amazon S3 o al sistema de archivos EFS. Las políticas asociadas a este rol determinarán el nivel de acceso que quiere ofrecer a los usuarios cuando se transfieran archivos dentro y fuera de su bucket de Amazon S3 o del sistema de archivos de Amazon EFS. El rol de IAM también debe contener una relación de confianza que permita que el servidor pueda obtener acceso a los recursos cuando atienda las solicitudes de transferencia de los usuarios. Para obtener más información sobre cómo establecer una relación de confianza, consulte Para establecer una relación de confianza.	Obligatorio

Valor	Description (Descripción)	Obligatorio
PosixProfile	La identidad POSIX completa, incluido el ID de usuario (Uid), el ID de grupo (Gid) y cualquier ID de grupo secundario (Secondary Gids) que controla el acceso de los usuarios a los sistemas de archivos de Amazon EFS. Los permisos POSIX establecidos en los archivos y directorios del sistema de archivos determinan el nivel de acceso que obtienen los usuarios al transferir archivos dentro y fuera de los sistemas de archivos de Amazon EFS.	Se requiere para el almacenamiento de respaldo de Amazon EFS
PublicKeys	Una lista de valores de clave pública de SSH que son válidos para este usuario. Una lista vacía implica que no se trata de un inicio de sesión válido. No debe devolverse durante la autenticación de la contraseña.	Opcional

Valor	Description (Descripción)	Obligatorio
Policy	Una política de sesión para el usuario, de modo que pueda usar el mismo rol de IAM en varios usuarios. Esta política reduce el ámbito de acceso del usuario a partes de su bucket de Amazon S3. Para obtener más información sobre el uso de políticas de sesión con proveedores de identidades personalizados, consulte los ejemplos de políticas de sesión de este tema.	Opcional

Valor	Description (Descripción)	Obligatorio
HomeDirectoryType	El tipo de directorio de destino (carpeta) que quiere utilizar como directorio de inicio de los usuarios cuando inicien sesión en el servidor. • Si lo establece en PATH, el usuario verá las rutas absolutas de bucket de Amazon S3 o de EFS como en sus clientes de protocolo de file transfer. • Si lo configura en LOGICAL, deberá proporcionar asignaciones en las HomeDirectoryDetails para hacer que las rutas de acceso de Amazon S3 o de Amazon EFS sean visibles para sus usuarios.	Opcional
HomeDirectoryDetails	Los mapeos de directorio lógico que especifican qué rutas de acceso y claves de Amazon S3 deben ser visibles para el usuario y cómo desea hacerlas visibles. Deberá especificar el par Entry y Target, donde Entry muestra cómo se hace visible la ruta y Target es la ruta de Amazon S3 o de Amazon EFS real.	Obligatorio si HomeDirectoryType tiene un valor de LOGICAL

Valor	Description (Descripción)	Obligatorio
HomeDirectory	Directorio de destino de un usuario cuando inicia sesión en el servidor a través del cliente. El formato depende del backend de almacenamiento: • Para Amazon S3: / bucket-name/user-home-directory Ejemplo: /amzn-s3-demo-bucket/users/john • Para Amazon EFS: / fs-12345/user-home-directory Ejemplo: /fs-faa1a123/users/john  Important El nombre del bucket o el ID del sistema de archivos Amazon EFS deben incluirse en la ruta. Si se omite esta información, se producirán errores de tipo «Archivo no encontrado» durante las transferencias de archivos.	Opcional

 Note

`HomeDirectoryDetails` es una representación de cadenas de un mapa de JSON. Esto contrasta con `PosixProfile`, que es un objeto de mapa JSON real, y `PublicKeys`, que es una matriz JSON de cadenas. Consulte los ejemplos de código para ver los detalles específicos del idioma.

 HomeDirectory Requisitos de formato

Cuando utilice el `HomeDirectory` parámetro, asegúrese de incluir el formato de ruta completo:

- Para el almacenamiento en Amazon S3: incluya siempre el nombre del bucket en el formato `/bucket-name/path`
- Para el almacenamiento en Amazon EFS: incluya siempre el ID del sistema de archivos en el formato `/fs-12345/path`

Una causa común de los errores de «Archivo no encontrado» es omitir el nombre del bucket o el ID del sistema de archivos EFS en la `HomeDirectory` ruta. Si `HomeDirectory` se establece solo `/` sin el identificador de almacenamiento, la autenticación se realizará correctamente, pero las operaciones con los archivos fallarán.

Ejemplo de función de Lambda

En esta sección se presentan algunos ejemplos de funciones de Lambda, tanto en Nodejs como en Python.

 Note

En estos ejemplos, el usuario, el rol, el perfil POSIX, la contraseña y los detalles del directorio de inicio son todos ejemplos y deben reemplazarse por sus valores reales.

Logical home directory, NodeJS

La siguiente función de ejemplo de Nodejs proporciona los detalles de un usuario que tiene un [directorio de inicio lógico](#).

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
  check the value of the server ID, only that it is provided.
  if (event.serverId !== "" && event.username == 'example-user') {
    var homeDirectoryDetails = [
      {
        Entry: "/",
        Target: "/fs-faa1a123"
      }
    ];
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
      authenticated if and only if the Role field is not blank
      PosixProfile: {"Gid": 65534, "Uid": 65534}, // Required for EFS access, but
      not needed for S3
      HomeDirectoryDetails: JSON.stringify(homeDirectoryDetails),
      HomeDirectoryType: "LOGICAL",
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
      // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
      authentication failure
      response = {};
    }
  } else {
    // Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {};
  }
}
```

```

    }
    callback(null, response);
};

```

Path-based home directory, NodeJS

La siguiente función de ejemplo de Nodejs proporciona los detalles de un usuario que tiene un directorio de inicio basado en rutas.

```

// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
    console.log("Username:", event.username, "ServerId: ", event.serverId);

    var response;
    // Check if the username presented for authentication is correct. This doesn't
    check the value of the server ID, only that it is provided.
    // There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
    (e.g., "127.0.0.1") to further restrict logins.
    if (event.serverId !== "" && event.username == 'example-user') {
        response = {
            Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
            authenticated if and only if the Role field is not blank
            Policy: '', // Optional, JSON stringified blob to further restrict this user's
            permissions
            // HomeDirectory format depends on your storage backend:
            // For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
            users/john')
            // For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
            HomeDirectory: '/my-transfer-bucket/users/example-user' // S3 example -
            replace with your bucket name
            // HomeDirectory: '/fs-faa1a123/users/example-user' // EFS example - uncomment
            for EFS
        };

        // Check if password is provided
        if (!event.password) {
            // If no password provided, return the user's SSH public key
            response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
            // Check if password is correct
        } else if (event.password !== 'Password1234') {

```



```
// Return HTTP status 200 but with no role in the response to indicate
authentication failure
    response = {};
}
} else {
    // Return HTTP status 200 but with no role in the response to indicate
authentication failure
    response = {};
}
callback(null, response);
};
```

Logical home directory, Python

La siguiente función de ejemplo de Python proporciona los detalles de un usuario que tiene un [directorio de inicio lógico](#).

```
# GetUserConfig Python Lambda with LOGICAL HomeDirectoryDetails
import json

def lambda_handler(event, context):
    print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

    response = {}

    # Check if the username presented for authentication is correct. This doesn't
    check the value of the server ID, only that it is provided.
    if event['serverId'] != '' and event['username'] == 'example-user':
        homeDirectoryDetails = [
            {
                'Entry': '/',
                'Target': '/fs-faa1a123'
            }
        ]
        response = {
            'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
            be authenticated if and only if the Role field is not blank
            'PosixProfile': {"Gid": 65534, "Uid": 65534}, # Required for EFS access, but
            not needed for S3
            'HomeDirectoryDetails': json.dumps(homeDirectoryDetails),
            'HomeDirectoryType': "LOGICAL"
        }
    }
```

```

# Check if password is provided
if event.get('password', '') == '':
    # If no password provided, return the user's SSH public key
    response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
# Check if password is correct
elif event['password'] != 'Password1234':
    # Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {}
else:
    # Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {}

return response

```

Path-based home directory, Python

La siguiente función de ejemplo de Python proporciona los detalles de un usuario que tiene un directorio de inicio basado en rutas.

```

# GetUserConfig Python Lambda with PATH HomeDirectory

def lambda_handler(event, context):
    print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

    response = {}

    # Check if the username presented for authentication is correct. This doesn't
    check the value of the server ID, only that it is provided.
    # There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
    (e.g., "127.0.0.1") to further restrict logins.
    if event['serverId'] != '' and event['username'] == 'example-user':
        response = {
            'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
            be authenticated if and only if the Role field is not blank
            'Policy': '', # Optional, JSON stringified blob to further restrict this
            user's permissions
            # HomeDirectory format depends on your storage backend:
            # For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
            users/john')
            # For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')

```

```

    'HomeDirectory': '/my-transfer-bucket/users/example-user', # S3 example -
    replace with your bucket name
    # 'HomeDirectory': '/fs-faa1a123/users/example-user', # EFS example -
    uncomment for EFS
    'HomeDirectoryType': "PATH" # Not strictly required, defaults to PATH
  }

  # Check if password is provided
  if event.get('password', '') == '':
    # If no password provided, return the user's SSH public key
    response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
    # Check if password is correct
    elif event['password'] != 'Password1234':
      # Return HTTP status 200 but with no role in the response to indicate
      authentication failure
      response = {}
    else:
      # Return HTTP status 200 but with no role in the response to indicate
      authentication failure
      response = {}

  return response

```

Prueba de su configuración

Tras crear el proveedor de identidad personalizado, debe probar la configuración.

Console

Para probar la configuración mediante la AWS Transfer Family consola

1. Abra la [consola de AWS Transfer Family](#).
2. En la página Servidores, elija su nuevo servidor, elija Acciones y, a continuación, elija Probar.
3. Introduzca el texto del nombre de usuario y la contraseña que estableció al implementar la CloudFormation pila. Si ha mantenido las opciones predeterminadas, el nombre de usuario es myuser y la contraseña es MySuperSecretPassword.
4. Elija el protocolo del servidor e introduzca la dirección IP de la IP de origen, si la configuró al implementar la CloudFormation pila.

CLI

Para probar la configuración mediante la AWS CLI

1. Ejecute el comando [test-identity-provider](#). Sustituya cada *user input placeholder* por su propia información, tal y como se describe en los pasos siguientes.

```
aws transfer test-identity-provider --server-id s-1234abcd5678efgh --user-
name myuser --user-password MySuperSecretPassword --server-protocol FTP --
source-ip 127.0.0.1
```

2. Introduzca el identificador del servidor.
3. Introduzca el nombre de usuario y la contraseña que estableció al implementar la CloudFormation pila. Si ha mantenido las opciones predeterminadas, el nombre de usuario es myuser y la contraseña es MySuperSecretPassword.
4. Introduzca el protocolo del servidor y la dirección IP de origen, si los configuró al implementar la CloudFormation pila.

Si la autenticación del usuario se realiza correctamente, la prueba devuelve una respuesta HTTP de StatusCode: 200, una cadena vacía de Message: "" (que, de lo contrario, contendría el motivo del error) y un campo Response.

Note

En el ejemplo de respuesta que aparece a continuación, el campo Response es un objeto JSON que se ha “encadenado” (convertido en una cadena JSON plana que se puede utilizar dentro de un programa) y contiene los detalles de los roles y permisos del usuario.

```
{
  "Response": "{\\\"Policy\\\":\\\"{\\\"Version\\\":\\\"2012-10-17\\\",\\\"Statement\\\":
[\\\"Sid\\\":\\\"ReadAndListAllBuckets\\\",\\\"Effect\\\":\\\"Allow\\\",\\\"Action\\
\\\":[\\\"s3:ListAllMybuckets\\\",\\\"s3:GetBucketLocation\\\",\\\"s3:ListBucket\\\",\\
\\\"s3:GetObjectVersion\\\",\\\"s3:GetObjectVersion\\\"],\\\"Resource\\\":\\\"*\\\"]}\\\",
\\\"Role\\\":\\\"arn:aws:iam::000000000000:role/MyUserS3AccessRole\\\",\\\"HomeDirectory\\\":\\\"/
\\\"}\\\",
  \"StatusCode\": 200,
  \"Message\": \"\"
}
```

Plantillas de función de Lambda

Puede implementar una CloudFormation pila que utilice una función Lambda para la autenticación. Proporcionamos varias plantillas que autentican y autorizan a sus usuarios mediante credenciales de inicio de sesión. Puede modificar estas plantillas o AWS Lambda códigos para personalizar aún más el acceso de los usuarios.

Note

Puede crear un FIPS-enabled AWS Transfer Family servidor CloudFormation especificando una política FIPS-enabled de seguridad en la plantilla. Las políticas de seguridad disponibles se describen en [Políticas de seguridad para AWS Transfer Family servidores](#)

Para crear una CloudFormation pila para utilizarla en la autenticación

1. Abra la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
2. Siga las instrucciones para implementar una CloudFormation pila a partir de una plantilla existente en [Seleccionar una plantilla de pila](#) en la Guía del AWS CloudFormation usuario.
3. Utilice una de las siguientes plantillas para crear una función de Lambda que se utilizará para la autenticación en Transfer Family.

- [Plantilla de pila clásica \(Amazon Cognito\)](#)

Una plantilla básica para crear una AWS Lambda para usarla como proveedor de identidad personalizado en AWS Transfer Family. Se autentica con Amazon Cognito para la autenticación basada en contraseñas y las claves públicas se devuelven desde un bucket de Amazon S3 si se utiliza la autenticación basada en claves públicas. Tras la implementación, puede modificar el código de la función de Lambda para hacer algo diferente.

- [AWS Secrets Manager plantilla de pila](#)

Plantilla básica que se utiliza AWS Lambda con un AWS Transfer Family servidor para integrar Secrets Manager como proveedor de identidad. Se autentica con una entrada AWS Secrets Manager de ese formato `aws/transfer/server-id/username`. Además, el secreto debe contener los pares clave-valor de todas las propiedades de usuario devueltas a Transfer Family. Tras la implementación, puede modificar el código de la función de Lambda para hacer algo diferente.

- Plantilla de [pila Okta: plantilla](#) básica que se utiliza AWS Lambda con un AWS Transfer Family servidor para integrar Okta como proveedor de identidad personalizado.
- [Okta-mfa plantilla de pila](#): plantilla básica que se utiliza AWS Lambda con un AWS Transfer Family servidor para integrar Okta, con autenticación multifactor, como proveedor de identidad personalizado.
- [Plantilla de Azure Active Directory](#): los detalles de esta pila se describen en la entrada del blog [Autenticarse AWS Transfer Family con Azure Active Directory](#) y. AWS Lambda

Una vez implementada la pila, puede ver los detalles sobre ella en la pestaña Salidas de la CloudFormation consola.

Implementar una de estas pilas es la forma más sencilla de integrar un proveedor de identidades personalizado en el flujo de trabajo de Transfer Family.

Uso de Amazon API Gateway para integrar su proveedor de identidad

En este tema se describe cómo utilizar una AWS Lambda función para respaldar un método de API Gateway. Utilice esta opción si necesita una API RESTful para integrar su proveedor de identidad o si desea AWS WAF utilizarla para aprovechar sus capacidades para el bloqueo geográfico o las solicitudes de limitación de velocidad.

En la mayoría de los casos de uso, la forma recomendada de configurar un proveedor de identidades personalizado es utilizar el. [Solución de proveedor de identidad personalizada](#)

Limitaciones si utiliza una API Gateway para integrar su proveedor de identidad

- Esta configuración no admite dominios personalizados.
- Esta configuración no admite una URL de API Gateway privada.

Si necesita alguna de estas opciones, puede usar Lambda como proveedor de identidades, sin API Gateway. Para obtener más información, consulte [Se utiliza AWS Lambda para integrar su proveedor de identidad](#).

Autenticación mediante un método de API Gateway

Puede crear un método API Gateway para usarlo como proveedor de identidad para Transfer Family. Este enfoque proporciona una forma muy segura de crear y proporcionar API. Con API Gateway, puede crear un punto final HTTPS para que todas las operaciones de API entrantes se transmitan

con mayor seguridad. Para obtener más información sobre el servicio API Gateway, consulte la [Guía para desarrolladores de API Gateway](#).

API Gateway ofrece un método de autorización denominado `AWS_IAM`, que le proporciona la misma autenticación basada en AWS Identity and Access Management (IAM) que se AWS utiliza internamente. Si habilita la autenticación con `AWS_IAM`, solo las personas que llaman con permisos explícitos para llamar a una API pueden acceder al método API Gateway de esa API.

Para usar su método API Gateway como proveedor de identidad personalizado para Transfer Family, habilita IAM para su método API Gateway. Como parte de este proceso, usted proporciona un rol de IAM con permisos para que Transfer Family utilice su puerta de enlace.

 Note

Para mejorar la seguridad, puede configurar un firewall de aplicaciones web. AWS WAF es un firewall de aplicaciones web que permite monitorizar las solicitudes HTTP y HTTPS que se reenvían a una Amazon API Gateway. Para obtener más información, consulte [Agregue un cortafuegos de aplicaciones web](#).

 No habilite el almacenamiento en caché de API Gateway

No habilite el almacenamiento en caché para tu método API Gateway cuando lo utilices como proveedor de identidad personalizado para Transfer Family. El almacenamiento en caché es inapropiado e inválido para las solicitudes de autenticación porque:

- Cada solicitud de autenticación es única y requiere una respuesta en tiempo real, no una respuesta en caché
- El almacenamiento en caché no ofrece ningún beneficio, ya que Transfer Family nunca envía solicitudes duplicadas o repetidas a la API Gateway.
- Al habilitar el almacenamiento en caché, la API Gateway responderá con datos no coincidentes, lo que provocará que las respuestas a las solicitudes de autenticación no sean válidas

Uso del método API Gateway para la autenticación personalizada con Transfer Family

1. Crea una CloudFormation pila. Para ello:

 Note

Las plantillas de pila se han actualizado para usar BASE64-encoded contraseñas: para obtener más información, consulte [Mejoras en las plantillas CloudFormation](#).

- a. Abra la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
- b. Siga las instrucciones para implementar una CloudFormation pila a partir de una plantilla existente en [Seleccionar una plantilla de pila](#) en la Guía del AWS CloudFormation usuario.
- c. Use una de las siguientes plantillas básicas para crear un método API Gateway respaldado por la API de AWS Lambda para usarlo como proveedor de identidad personalizado en Transfer Family.

- [Plantilla de pila básica](#)

De forma predeterminada, el método API Gateway se utiliza como proveedor de identidad personalizado para autenticar a un único usuario en un único servidor mediante una clave o contraseña SSH (Secure Shell) codificada de forma rígida. Tras la implementación, puede modificar el código de la función de Lambda para hacer algo diferente.

- [AWS Secrets Manager plantilla de pila](#)

De forma predeterminada, el método API Gateway se autentica con una entrada de este formato de `aws/transfer/server-id/username` en Secrets Manager. Además, el secreto debe contener los pares clave-valor de todas las propiedades de usuario devueltas a Transfer Family. Tras la implementación, puede modificar el código de la función de Lambda para hacer algo diferente. Para obtener más información, consulte la entrada del blog [Habilitar la autenticación por contraseña para su AWS Transfer Family uso AWS Secrets Manager](#).

- [Plantilla de pila Okta](#)

Su método API Gateway se integra con Okta como proveedor de identidad personalizado en Transfer Family. Para obtener más información, consulte la publicación de blog sobre el [Uso de Okta como proveedor de identidad con AWS Transfer Family](#).

Implementar una de estas pilas es la forma más sencilla de integrar un proveedor de identidades personalizado en el flujo de trabajo de Transfer Family. Cada pila utiliza la función de Lambda

para admitir su método de API basado en API Gateway. A continuación, puede usar su método de API como proveedor de identidad personalizado en Transfer Family. De forma predeterminada, la función de Lambda autentica a un único usuario llamado `myuser` con una contraseña de `MySuperSecretPassword`. Tras la implementación, puede editar estas credenciales o actualizar el código de la función de Lambda para hacer algo diferente.

 Important

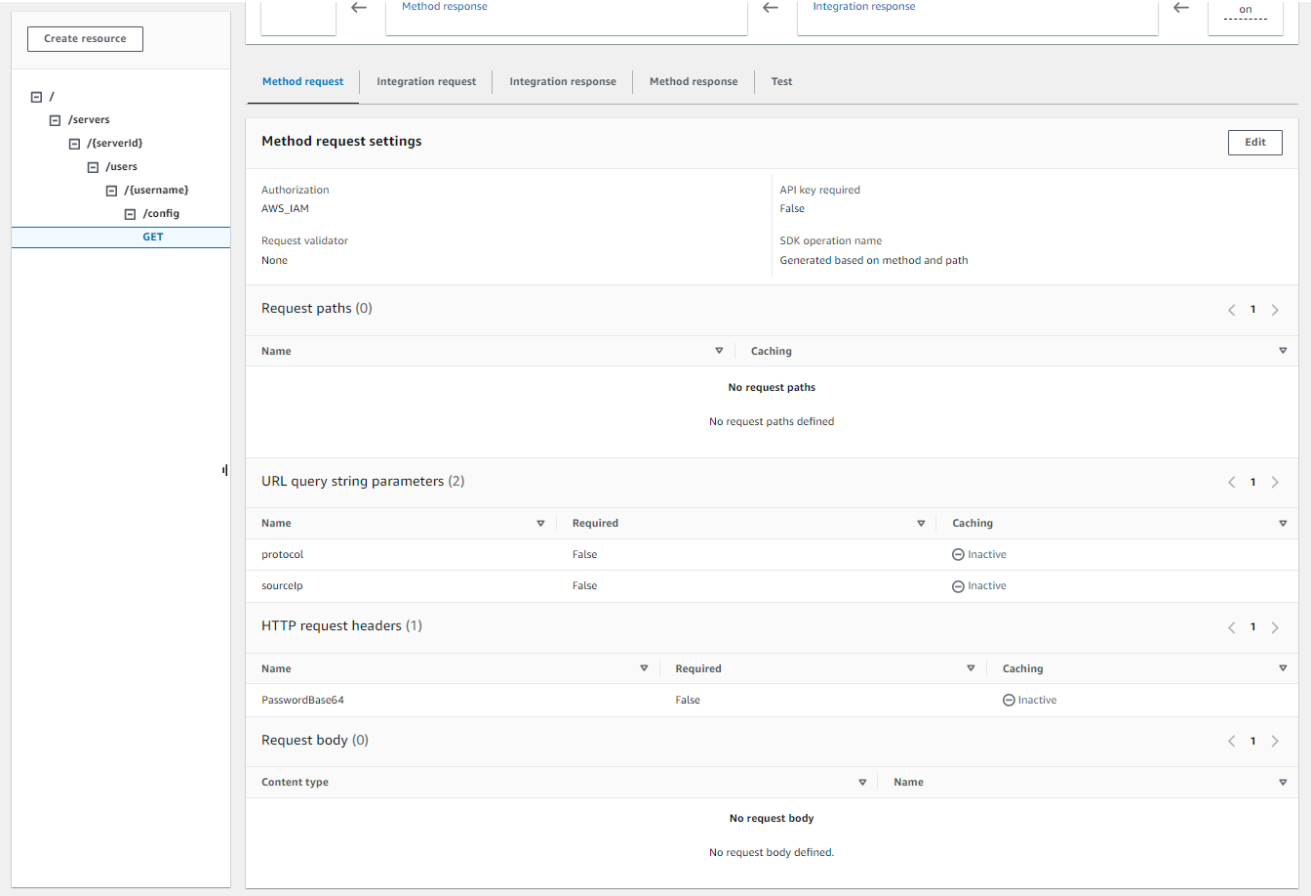
Le recomendamos que edite las credenciales de usuario y contraseña predeterminadas.

Una vez desplegada la pila, puede ver sus detalles en la pestaña Salidas de la CloudFormation consola. Estos detalles incluyen el nombre de recurso de Amazon (ARN) de la pila, el ARN del rol de IAM que creó la pila y la URL de su nueva puerta de enlace.

 Note

Si utiliza la opción de proveedor de identidad personalizado para habilitar la autenticación basada en contraseñas para sus usuarios y habilita el registro de solicitudes y respuestas que proporciona API Gateway, API Gateway registra las contraseñas de sus usuarios en sus Amazon Logs. CloudWatch No recomendamos utilizar este modo de inicio en entornos de producción. Para obtener más información, consulte [Configurar el registro de CloudWatch API en API Gateway](#) en la Guía para desarrolladores de API Gateway.

2. Compruebe la configuración del método API Gateway para su servidor. Para ello:
 - a. Abra la consola de API Gateway en <https://console.aws.amazon.com/apigateway/>.
 - b. Elija la API de plantilla básica Transfer Custom Identity Provider que generó la CloudFormation plantilla. Puede que tengas que seleccionar tu región para ver las pasarelas.
 - c. En el panel Recursos, selecciona GET. La siguiente captura de pantalla muestra la configuración correcta del método.



En este punto, su API Gateway está lista para ser implementada.

3. Para Acciones, elija Implementar API. Para la Etapa de implementación, elija prod y, a continuación, elija Implementar.

Una vez que el método API Gateway se haya implementado correctamente, consulta su rendimiento en Stages > Stage details, como se muestra en la siguiente captura de pantalla.



Note

Copie la dirección URL de invocación que aparece en la parte superior de la pantalla. Puede que lo necesites para el siguiente paso.

The screenshot displays the AWS Transfer Family console interface. At the top, the breadcrumb navigation shows 'API Gateway > APIs > Transfer Custom Identity Provider basic template API > Stages'. The main heading is 'Stages'. On the left, a sidebar lists the stage 'prod'. The main content area is divided into several sections:

- Stage details** (with an 'Edit' button):
 - Stage name: prod
 - API cache: ☒ Inactive
 - Rate: 10000
 - Burst: 5000
 - Web ACL: -
 - Client certificate: -
 - Invoke URL**: [https://\[redacted\].execute-api.us-east-1.amazonaws.com/prod](https://[redacted].execute-api.us-east-1.amazonaws.com/prod) (this field is highlighted with a red box in the image)
 - Active deployment: t8aqrn on December 12, 2023, 10:49 (UTC-05:00)
- Logs and tracing** (with an 'Edit' button):
 - CloudWatch logs: Error and info logs
 - Detailed metrics: ☒ Inactive
 - X-Ray tracing: ☒ Inactive
 - Custom access logging: ☒ Inactive
- Stage variables** (with tabs for 'Deployment history', 'Documentation history', 'Canary', and 'Tags'):
 - Stage variables (0/0)
 - Find resources input field
 - Table with columns 'Name' and 'Value' (currently empty)
 - Message: 'No variables associated with the stage.'
 - Manage variables button

4. Abra la AWS Transfer Family consola en. <https://console.aws.amazon.com/transfer/>
5. Se debería haber creado una Transfer Family para ti cuando creaste la pila. Si no es así, configure su servidor siguiendo estos pasos.
 - a. Seleccione Crear servidor para abrir la página Crear servidor. En Elija un proveedor de identidad, seleccione Personalizado y, a continuación, seleccione Usar Amazon API Gateway para conectarse con su proveedor de identidad, como se muestra en la siguiente captura de pantalla.

Choose an identity provider

Identity provider

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

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

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

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

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

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

Provide an Amazon API Gateway URL

Role
IAM role for the service to invoke your Amazon API Gateway URL

- b. En el cuadro de texto Proporcionar una URL de Amazon API Gateway, pegue la dirección URL de invocación del punto de conexión de API Gateway que creó en el paso 3 de este procedimiento.
- c. En Función, elige la función de IAM que creó la CloudFormation plantilla. Este rol permite a Transfer Family invocar su método de puerta de enlace de API.

El rol de invocación contiene el nombre de la CloudFormation pila que seleccionó para la pila que creó en el paso 1. Tiene el formato siguiente: *CloudFormation-stack-name-TransferIdentityProviderRole-ABC123DEF456GHI*.

- d. Rellene las casillas restantes y, a continuación, seleccione Crear servidor. Para obtener más información sobre los pasos restantes para crear un servidor, consulte [Configuración de un punto final de servidor SFTP, FTPS o FTP](#).

Implementación de su método de API Gateway

Para crear un proveedor de identidades personalizado para Transfer Family, el método API Gateway debe implementar un único método que tenga una ruta de recursos de `/servers/serverId/users/username/config`. Los valores de *serverId* y *username* proceden de la ruta de recurso RESTful. Además, añada `sourceIp` y `protocol` como Parámetros de cadena de consulta de URL en la Solicitud de método, como se muestra en la imagen siguiente.

Resources

Create resource

/

/servers

/servers/{serverId}

/servers/{serverId}/users

/servers/{serverId}/users/{username}

/servers/{serverId}/users/{username}/config

GET

API actions

Deploy API

/servers/{serverId}/users/{username}/config - GET - Method execution

Update documentation

Delete

ARN

arn:aws:execute-api:us-east-1:123456789012:us-east-1/servers/{serverId}/users/{username}/config

Resource ID

aw4ihv

Client

Method request

Integration request

Method response

Integration response

Lambda integration

Method request

Integration request

Integration response

Method response

Test

Method request settings

Edit

Authorization

AWS_IAM

API key required

False

Request validator

None

SDK operation name

Generated based on method and path

Request paths (0)

< 1 >

Name

Caching

No request paths

No request paths defined

URL query string parameters (2)

< 1 >

Name

Required

Caching

protocol

False

Inactive

sourceIp

False

Inactive

 Note

El nombre de usuario debe tener un mínimo de 3 y un máximo de 100 caracteres. Puede utilizar los siguientes caracteres en el nombre de usuario: a-z, 0—9 A-Z, guión bajo '_', guión '-', punto '.' y signo '@'. El nombre de usuario no puede empezar con un guión '-', punto '.' o con el signo '@'.

Proveedor de identidades personalizado

241

Si Transfer Family intenta autenticar una contraseña en nombre de un usuario, el servicio proporciona un campo de encabezado `Password:`. En ausencia de un encabezado de `Password:`, Transfer Family intenta la autenticación con clave pública para autenticar al usuario.

Si utiliza un proveedor de identidad para autenticar y autorizar a los usuarios finales, además de validar sus credenciales, puede permitir o denegar las solicitudes de acceso en función de las direcciones IP de los clientes utilizados por los usuarios finales. Puede usar esta característica para asegurarse de que solo se pueda acceder a los datos almacenados en sus buckets de S3 o en su sistema de archivos Amazon EFS a través de los protocolos compatibles desde las direcciones IP que haya especificado como confiables. Para habilitar esta característica, debe incluir `sourceIp` en la cadena de consulta.

Si tiene varios protocolos habilitados para su servidor y desea proporcionar acceso con el mismo nombre de usuario a través de varios protocolos, puede hacerlo siempre que las credenciales específicas de cada protocolo estén configuradas en su proveedor de identidad. Para habilitar esta característica, debe incluir el valor *protocol* en la ruta de recursos RESTful.

El método API Gateway siempre debe devolver el código de estado HTTP 200. Cualquier otro código de estado HTTP significa que se ha producido un error en el acceso a la API.

Ejemplo de respuesta de Amazon S3

El cuerpo de la respuesta de ejemplo es un documento JSON del siguiente formato para Amazon S3.

```
{
  "Role": "IAM role with configured S3 permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
    "ssh-rsa public-key2"
  ],
  "Policy": "STS Assume role session policy",
  "HomeDirectory": "/amzn-s3-demo-bucket/path/to/home/directory"
}
```

Note

La política es un JSON de escape en forma de cadena. Por ejemplo:

```
"Policy":
"{
```

```

{"Version": "2012-10-17",
 "Statement":
  [
    {"Condition":
      {"StringLike":
        {"s3:prefix":
          ["user/*", "user/"]}},
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Sid": "ListHomeDir",
      {"Resource": "arn:aws:s3:::*",
        "Action": ["s3:PutObject",
          "s3:GetObject",
          "s3:DeleteObjectVersion",
          "s3:DeleteObject",
          "s3:GetObjectVersion",
          "s3:GetObjectACL",
          "s3:PutObjectACL"],
        "Effect": "Allow",
        "Sid": "HomeDirObjectAccess"}]}
]
}

```

El siguiente ejemplo de respuesta muestra que un usuario tiene un tipo de directorio de inicio lógico.

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\", \"Target\": \"/amzn-s3-demo-bucket1\"}]",
  "PublicKeys": []
}

```

Ejemplo de respuesta de Amazon EFS

El cuerpo de la respuesta de ejemplo es un documento JSON del siguiente formato para Amazon EFS.

```

{
  "Role": "IAM role with configured EFS permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
  ]
}

```

```

    "ssh-rsa public-key2"
  ],
  "PosixProfile": {
    "Uid": "POSIX user ID",
    "Gid": "POSIX group ID",
    "SecondaryGids": [Optional list of secondary Group IDs],
  },
  "HomeDirectory": "/fs-id/path/to/home/directory"
}

```

El campo `Role` indica que la autenticación ha tenido éxito. Al realizar la autenticación con contraseña (cuando se proporciona un encabezado de `Password:`), no es necesario que proporcione las claves públicas de SSH. Si un usuario no se puede autenticar, por ejemplo, si la contraseña es incorrecta, su método debería devolver una respuesta de `Role` sin configurar. Un ejemplo de esta respuesta es un objeto JSON vacío.

El siguiente ejemplo de respuesta muestra un usuario que tiene un tipo de directorio de inicio lógico.

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\\\", \"Target\": \"/faa1a123\"}]",
  "PublicKeys": [""],
  "PosixProfile": {"Uid": 65534, "Gid": 65534}
}

```

Puede incluir políticas de usuario en la función de Lambda en formato JSON. Para obtener más información acerca de la configuración de usuario en Transfer Family, consulte [Administrar los controles de acceso](#).

Función de Lambda por defecto

Para implementar diferentes estrategias de autenticación, edite la función de Lambda que utiliza su puerta de enlace. Para ayudarle a satisfacer las necesidades de su aplicación, puede utilizar el siguiente ejemplo de funciones Lambda en Node.js. Para obtener más información sobre Lambda, consulte la [Guía para AWS Lambda desarrolladores o Cómo crear funciones Lambda](#) con Node.js.

El siguiente ejemplo de función de Lambda toma el nombre de usuario, la contraseña (si está realizando la autenticación con contraseña), el identificador del servidor, el protocolo y la dirección IP del cliente. Puede usar una combinación de estas entradas para buscar su proveedor de identidad y determinar si se debe aceptar el inicio de sesión.

 Note

Si tiene varios protocolos habilitados para su servidor y desea proporcionar acceso con el mismo nombre de usuario a través de varios protocolos, puede hacerlo siempre que las credenciales específicas del protocolo se hayan configurado en su proveedor de identidad. Para el Protocolo de File Transfer (FTP), se recomienda mantener credenciales separadas del Protocolo de File Transfer (SFTP) de Secure Shell (SSH) y el Protocolo de File Transfer a través de SSL (FTPS). Recomendamos mantener credenciales separadas para el FTP porque, a diferencia del SFTP y el FTPS, el FTP transmite las credenciales en texto no cifrado. Al aislar las credenciales de FTP de las de SFTP o FTPS, si las credenciales de FTP se comparten o están expuestas, las cargas de trabajo que utilizan SFTP o FTPS permanecen seguras.

Este rol de ejemplo devuelve el rol y los detalles del directorio de inicio lógico, junto con las claves públicas (si realiza la autenticación de clave pública).

Al crear usuarios administrados por el servicio, se establece su directorio de inicio, ya sea lógico o físico. Del mismo modo, necesitamos que los resultados de la función de Lambda transmitan la estructura de directorios física o lógica deseada por el usuario. Los parámetros que defina dependen del valor del campo de [HomeDirectoryType](#).

- `HomeDirectoryType` establecido como `PATH`: el campo `HomeDirectory` debe ser un prefijo absoluto de bucket de Amazon S3 o una ruta absoluta de Amazon EFS visible para los usuarios.
- `HomeDirectoryType` establecido como `LOGICAL`: no defina un campo `HomeDirectory`. En su lugar, configuramos un `HomeDirectoryDetails` campo que proporciona las `Entry/Target` asignaciones deseadas, similares a los valores descritos en el [HomeDirectoryDetails](#) parámetro para los usuarios gestionados por el servicio.

Las funciones de ejemplo se muestran en [Ejemplo de función de Lambda](#).

Función Lambda para usar con AWS Secrets Manager

Para AWS Secrets Manager utilizarla como proveedor de identidad, puede trabajar con la función Lambda de la plantilla de ejemplo CloudFormation . La función de Lambda consulta el servicio Secrets Manager con sus credenciales y, si se ejecuta correctamente, devuelve un secreto designado. Para obtener más información acerca de Secrets Manager, consulte la [Guía del usuario de AWS Secrets Manager](#).

Para descargar una CloudFormation plantilla de ejemplo que utilice esta función Lambda, vaya al [bucket de Amazon S3 proporcionado por](#). AWS Transfer Family

Mejoras en las plantillas CloudFormation

Se han realizado mejoras en la interfaz de API Gateway en las CloudFormation plantillas publicadas. Las plantillas ahora usan BASE64-encoded contraseñas con la API Gateway. Sus implementaciones actuales siguen funcionando sin esta mejora, pero no permiten contraseñas con caracteres que no estén incluidos en el conjunto de US-ASCII caracteres básico.

Los cambios en la plantilla que habilitan esta capacidad son los siguientes:

- El `GetUserConfigRequest` `AWS::ApiGateway::Method` recurso debe tener este `RequestTemplates` código (la línea en cursiva es la línea actualizada)

```
RequestTemplates:
  application/json: |
    {
      "username": "$util.urlDecode($input.params('username'))",
      "password":
        "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll('\\"', '\"')",
      "protocol": "$input.params('protocol')",
      "serverId": "$input.params('serverId')",
      "sourceIp": "$input.params('sourceIp')"
    }
```

- El `RequestParameters` campo correspondiente al `GetUserConfig` recurso debe cambiar para poder utilizar el `PasswordBase64` encabezado (la línea en cursiva es la línea actualizada):

```
RequestParameters:
  method.request.header.PasswordBase64: false
  method.request.querystring.protocol: false
  method.request.querystring.sourceIp: false
```

Para comprobar si la plantilla de tu pila es la más reciente

1. Abre la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
2. De la lista de pilas, elige la tuya.
3. En el panel de detalles, selecciona la pestaña Plantilla.

- Busca RequestTemplates y asegúrate de tener esta línea:

- Busca RequestParameters y asegúrate de tener esta línea:

247

- SOLO con contraseña: los usuarios deben proporcionar su contraseña para conectarse.
- SOLO clave: los usuarios deben proporcionar su clave privada para conectarse.
- Contraseña y clave: los usuarios deben proporcionar su clave privada y su contraseña para conectarse. El servidor comprueba primero la clave y, después, si la clave es válida, el sistema solicita una contraseña. Si la clave privada proporcionada no coincide con la clave pública que se encuentra almacenada, se produce un error en la autenticación.

Compatibilidad con IPv6 para proveedores de identidad personalizados

AWS Transfer Family los proveedores de identidad personalizados son totalmente compatibles con las conexiones IPv6. Al implementar un proveedor de identidades personalizado, la función Lambda puede recibir y procesar solicitudes de autenticación de clientes IPv4 e IPv6 sin ninguna configuración adicional. La función Lambda recibe la dirección IP del cliente en el `sourceIp` campo de la solicitud, que puede ser una dirección IPv4 (por ejemplo `203.0.113.42`) o una dirección IPv6 (por ejemplo, `2001:db8:85a3:8d3:1319:8a2e:370:7348`). La implementación de su proveedor de identidad personalizado debe gestionar ambos formatos de dirección de forma adecuada.

Important

Si su proveedor de identidad personalizado realiza la IP-based validación o el registro, asegúrese de que su implementación gestione correctamente los formatos de direcciones IPv6. Las direcciones IPv6 son más largas que las direcciones IPv4 y utilizan un formato de notación diferente.

Note

Al gestionar las direcciones IPv6 en su proveedor de identidad personalizado, asegúrese de utilizar las funciones de análisis de direcciones IPv6 adecuadas en lugar de simples comparaciones de cadenas. Las direcciones IPv6 se pueden representar en varios formatos canónicos (por ejemplo, `o). fd00:b600::ec2 fd00:b600:0:0:0:0:ec2`). Utilice las bibliotecas o funciones de direcciones IPv6 adecuadas en su lenguaje de implementación para validar y comparar correctamente las direcciones IPv6.

Example Gestión de las direcciones IPv4 e IPv6 en un proveedor de identidad personalizado

```
def lambda_handler(event, context):
    # Extract the source IP address from the request
    source_ip = event.get('sourceIp', '')

    # Log the client IP address (works for both IPv4 and IPv6)
    print(f"Authentication request from: {source_ip}")

    # Example of IP-based validation that works with both IPv4 and IPv6
    if is_ip_allowed(source_ip):
        # Continue with authentication
        # ...
    else:
        # Reject the authentication request
        return {
            "Role": "",
            "HomeDirectory": "",
            "Status": "DENIED"
        }
```

Para obtener más información sobre la implementación de proveedores de identidad personalizados, consulte. [Se utiliza AWS Lambda para integrar su proveedor de identidad](#)

Uso AWS de Directory Service para Microsoft Active Directory

Puede utilizarlos AWS Transfer Family para autenticar su transferencia de archivos a los usuarios finales. AWS Directory Service for Microsoft Active Directory Permite una migración fluida de los flujos de trabajo de transferencia de archivos que se basan en la autenticación de Active Directory sin cambiar las credenciales de los usuarios finales ni necesitar un autorizador personalizado.

Con AWS Managed Microsoft AD, puede proporcionar a Directory Service los usuarios y grupos acceso de forma segura a través de SFTP, FTPS y FTP a los datos almacenados en Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS). Si utiliza Active Directory para almacenar las credenciales de sus usuarios, ahora dispone de una forma más sencilla de habilitar la transferencia de archivos para estos usuarios.

Puede proporcionar acceso a los grupos de Active Directory AWS Managed Microsoft AD en su entorno local o en la AWS nube mediante conectores de Active Directory. Puede dar a los usuarios que ya están configurados en su entorno de Microsoft Windows, ya sea en la AWS nube o en su

red local, acceso a un AWS Transfer Family servidor que utilice AWS Managed Microsoft AD como identidad. El blog AWS de almacenamiento contiene una publicación que detalla una solución para usar Active Directory con Transfer Family: [Simplifique la autenticación de Active Directory con un proveedor de identidad personalizado para AWS Transfer Family](#).

 Note

- AWS Transfer Family no es compatible con Simple AD.
- Transfer Family no admite configuraciones de Active Directory entre regiones: solo admitimos integraciones de Active Directory que estén en la misma región que la del servidor de Transfer Family.
- Transfer Family no admite el uso de AD Connector AWS Managed Microsoft AD ni el uso de AD Connector para habilitar la autenticación multifactor (MFA) en su infraestructura de RADIUS-based MFA existente.
- AWS Transfer Family no admite regiones replicadas de Active Directory administrado.

Para usarlo AWS Managed Microsoft AD, debe realizar los siguientes pasos:

1. Cree uno o más AWS Managed Microsoft AD directorios mediante la Directory Service consola.
2. Utilice la consola Transfer Family para crear un servidor que AWS Managed Microsoft AD lo utilice como proveedor de identidad.
3. Configure el AWS directorio mediante un conector de Active Directory.
4. Agregue el acceso desde uno o más de sus Directory Service grupos.
5. Aunque no es obligatorio, le recomendamos que pruebe y verifique el acceso de los usuarios.

Temas

- [Antes de empezar a usar AWS Directory Service for Microsoft Active Directory](#)
- [Trabajando con dominios de Active Directory](#)
- [Elegir AWS Managed Microsoft AD como proveedor de identidad](#)
- [Conexión a Microsoft Active Directory local](#)
- [Conceder acceso a los grupos](#)
- [Probando usuarios](#)
- [Eliminar el acceso al servidor de un grupo](#)

- [Conexión al servidor mediante SSH \(Secure Shell\)](#)
- [Conexión AWS Transfer Family a un Active Directory autoadministrado mediante bosques y fideicomisos](#)

Antes de empezar a usar AWS Directory Service for Microsoft Active Directory

Note

AWS Transfer Family tiene un límite predeterminado de 100 grupos de Active Directory por servidor. Si su caso de uso requiere más de 100 grupos, considere la posibilidad de utilizar una solución de proveedor de identidad personalizada, tal como se describe en [Simplifique la autenticación de Active Directory con un proveedor de identidad personalizado para AWS Transfer Family](#).

Proporcione un identificador único para sus grupos de AD

Antes de poder usarlo AWS Managed Microsoft AD, debe proporcionar un identificador único para cada grupo del directorio de Microsoft AD. Para ello, puede utilizar el identificador de seguridad (SID) de cada grupo. Los usuarios del grupo que asocie tienen acceso a sus recursos de Amazon S3 o Amazon EFS a través de los protocolos habilitados mediante AWS Transfer Family.

Utilice el siguiente PowerShell comando de Windows para recuperar el SID de un grupo y *YourGroupName* sustitúyalo por el nombre del grupo.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select  
SamAccountName,ObjectSid
```

Note

Si lo utiliza AWS Directory Service como proveedor de identidad `userPrincipalName` y `SamAccountName` tiene valores diferentes, AWS Transfer Family acepta el valor `inSamAccountName`. Transfer Family no acepta el valor especificado en `userPrincipalName`.

Añada Directory Service permisos a su función

También necesitas permisos Directory Service de API para usarlos AWS Directory Service como proveedor de identidades. Los siguientes permisos son necesarios o recomendados:

- Se requiere `ds:DescribeDirectories` para que Transfer Family busque en el directorio
- `ds:AuthorizeApplication` es necesario añadir una autorización para Transfer Family
- Se sugiere `ds:UnauthorizeApplication` para eliminar todos los recursos que se hayan creado provisionalmente, en caso de que algo vaya mal durante el proceso de creación del servidor

Añada estos permisos al rol que está utilizando para crear sus servidores de Transfer Family. Para obtener información detallada sobre estos permisos, consulte Permisos API [Directory Service : acciones, recursos y referencia de condiciones](#).

Trabajando con dominios de Active Directory

Cuando esté pensando en cómo hacer que los usuarios de Active Directory accedan a los servidores de AWS Transfer Family , tenga en cuenta el dominio del usuario y el dominio de su grupo. Lo ideal es que el dominio del usuario y el dominio de su grupo coincidan. Es decir, tanto el usuario como el grupo están en el dominio predeterminado o ambos están en el dominio de confianza. Si este no es el caso, Transfer Family no podrá autenticar al usuario.

Puede probar al usuario para asegurarse de que la configuración es correcta. Para obtener más información, consulte [Probando usuarios](#). Si hay algún problema con el user/group dominio, aparece el mensaje de error: No se ha encontrado ningún acceso asociado a los grupos de usuarios.

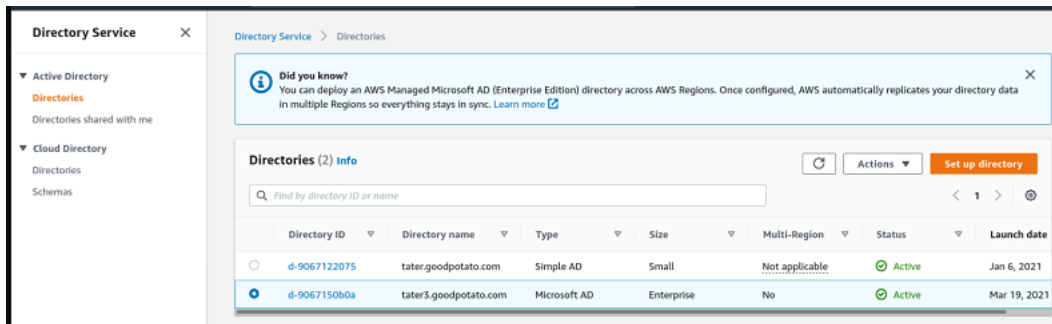
Elegir AWS Managed Microsoft AD como proveedor de identidad

En esta sección se describe cómo usarlo AWS Directory Service for Microsoft Active Directory con un servidor.

Para usar AWS Managed Microsoft AD con Transfer Family

1. Inicia sesión en Consola de administración de AWS y abre la Directory Service consola en <https://console.aws.amazon.com/directoryservicev2/>.

Utilice la Directory Service consola para configurar uno o más directorios gestionados. Para obtener más información, consulte [AWS Managed Microsoft AD](#) en la Guía para administradores de Directory Service .

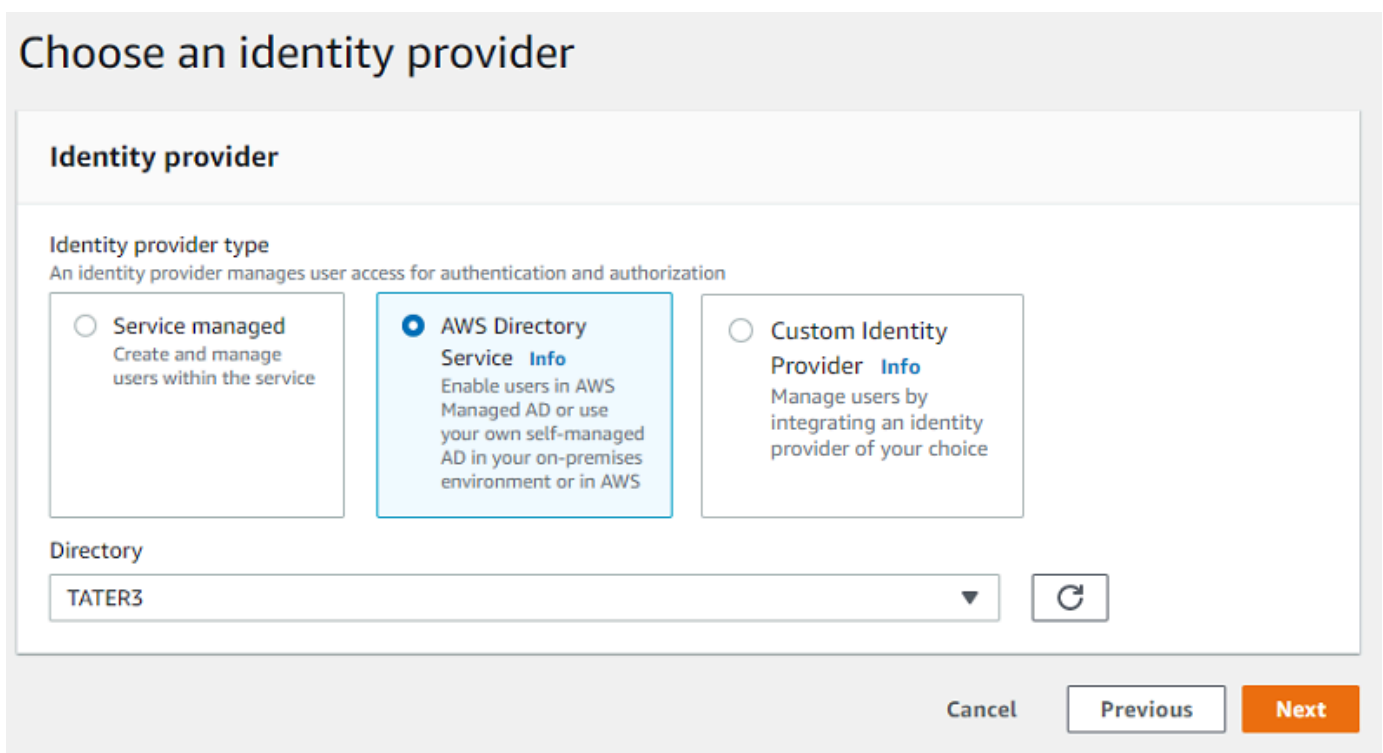


- Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/> y seleccione Crear servidor.
- En la página Elegir protocolos, elija uno o más protocolos de la lista.

Note

Si selecciona FTPS, debe proporcionar el certificado de AWS Certificate Manager .

- En Elegir un proveedor de identidad, elija Directory Service de AWS .



- La lista Directorio contiene todos los directorios administrados que ha configurado. Elija un directorio de la lista y elija Siguiente.

 Note

- Cross-Account y no se admiten los directorios compartidos AWS Managed Microsoft AD.
- Para configurar un servidor con Directory Service como proveedor de identidad, debe añadir algunos Directory Service permisos. Para obtener más información, consulte [Antes de empezar a usar AWS Directory Service for Microsoft Active Directory](#).

6. Para terminar de crear el servidor, utilice uno de los procedimientos siguientes:

- [Crea un SFTP-enabled servidor](#)
- [Cree un FTPS-enabled servidor](#)
- [Cree un servidor FTP-enabled](#)

En esos procedimientos, continúe con el paso siguiente: elegir un proveedor de identidad.

 Important

No puedes eliminar un directorio de Microsoft AD Directory Service si lo usaste en un servidor Transfer Family. Primero debe eliminar el servidor y, a continuación, puede eliminar el directorio.

Conexión a Microsoft Active Directory local

En esta sección se describe cómo configurar un AWS directorio mediante un conector AD.

Para configurar el AWS directorio mediante AD Connector

1. Abra la consola [Servicio de directorio](#) y seleccione Directorios.
2. Seleccione Configurar directorio.
3. Para el tipo de directorio, elija Conector de AD.
4. Seleccione un tamaño de directorio, seleccione Siguiente y, a continuación, seleccione su VPC y sus subredes.
5. Seleccione Siguiente y, a continuación, rellene los campos de la siguiente manera:

- Nombre DNS del directorio: introduzca el nombre de dominio que está utilizando para su Microsoft Active Directory.
- Direcciones IP DNS: introduzca las direcciones IP de Microsoft Active Directory.
- Nombre de usuario y contraseña de la cuenta del servidor: introduzca los detalles de la cuenta de servicio que va a utilizar.

6. Complete las pantallas para crear el servicio de directorio.

El siguiente paso es crear un servidor Transfer Family con el protocolo SFTP y el tipo de proveedor de identidad de AWS Directory Service. En la lista desplegable del directorio, seleccione el directorio que agregó en el procedimiento anterior.

Conceder acceso a los grupos

Tras crear el servidor, debe elegir qué grupos del directorio deben tener acceso para cargar y descargar archivos mediante los protocolos habilitados AWS Transfer Family. Para ello, debe crear un acceso.

Note

AWS Transfer Family tiene un límite predeterminado de 100 grupos de Active Directory por servidor. Si su caso de uso requiere más de 100 grupos, considere la posibilidad de utilizar una solución de proveedor de identidad personalizada, tal como se describe en [Simplifique la autenticación de Active Directory con un proveedor de identidad personalizado para AWS Transfer Family](#).

Note

Los usuarios deben pertenecer directamente al grupo al que se concede el acceso. Por ejemplo, supongamos que Bob es un usuario y pertenece al grupo A y que el propio grupo A está incluido en el grupo B.

- Si concede acceso al Grupo A, a Bob se le concede el acceso.
- Si concede acceso al grupo B (y no al grupo A), Bob no tendrá acceso.

Cómo conceder acceso a un grupo

1. Abra la consola en AWS Transfer Family . <https://console.aws.amazon.com/transfer/>
2. Navegue a la página de detalles del servidor.
3. En la sección Accesos, seleccione Añadir acceso.
4. Introduzca el SID del AWS Managed Microsoft AD directorio al que desea acceder a este servidor.

Note

Para obtener información acerca de cómo buscar el SID de su grupo, consulte [the section called “Antes de empezar a usar AWS Directory Service for Microsoft Active Directory”](#).

5. En Access, elija un rol AWS Identity and Access Management (IAM) para el grupo.
6. En la sección Política, elija una política. El valor predeterminado es Ninguno.
7. En el directorio principal, elija un bucket de Amazon S3 que corresponda al directorio principal del grupo.

Note

Puede limitar las partes del bucket que ven los usuarios mediante la creación de una política de sesión. Por ejemplo, para limitar a los usuarios a su propia carpeta en el directorio de /filetest, introduzca el siguiente texto en el cuadro.

```
/filetest/${transfer:UserName}
```

Para obtener más información sobre la creación de una política de sesión, consulte [Creación de una política de sesión para un bucket de Amazon S3](#).

8. Seleccione Añadir para crear la asociación.
9. Seleccione su servidor.
10. Seleccione Añadir acceso.
 - Introduzca el SID del grupo.

Note

Para obtener información acerca de cómo encontrar el SID, consulte [the section called “Antes de empezar a usar AWS Directory Service for Microsoft Active Directory”](#).

11. Seleccione Añadir acceso.

En la sección Accesos, se muestran los accesos al servidor.

The screenshot displays the AWS Directory Service console interface. At the top, the 'Endpoint configuration' section shows the 'Availability Zone' as 'us-east-1a', the 'Subnet ID' as 'subnet-...', and the 'Private IPv4 Address' as '172.31.80.36'. Below this, the 'Accesses (1)' section features a search bar, an 'Actions' dropdown menu, and an 'Associate access' button. A table lists the access details with columns for 'External Id', 'Home directory', and 'Role'. The table contains one entry: 'S-' for 'External Id', '/padbucket3' for 'Home directory', and 'ADGuy_S3_And_EFS' for 'Role'. The 'Additional details' section at the bottom includes 'Logging role' (info icon), 'Server activity not logged to Amazon CloudWatch' (info icon), 'Server host key' (info icon), 'Security Policy' (info icon), 'TransferSecurityPolicy-2018-11', 'Domain' (Amazon S3), and an 'Edit' button.

External Id	Home directory	Role
S-	/padbucket3	ADGuy_S3_And_EFS

Probando usuarios

Puede comprobar si un usuario tiene acceso al AWS Managed Microsoft AD directorio de su servidor.

Note

Un usuario debe pertenecer exactamente a un grupo (un identificador externo) que aparece en la sección Acceso de la página Configuración del punto de conexión. Si el usuario no está en ningún grupo o está en más de un grupo, no se le concede el acceso.

Comprobación de si un usuario específico tiene acceso

1. En la página de detalles del servidor, elija Acciones y, a continuación, elija Probar.
2. Para Realizar pruebas con un proveedor de identidad, introduzca las credenciales de inicio de sesión de un usuario que pertenezca a uno de los grupos a los que tenga acceso.
3. Seleccione Probar

Aparece una prueba de proveedor de identidad correcta, que indica que se ha concedido acceso al servidor al usuario seleccionado.

Identity provider testing

User configuration [Info](#)

Username

transferuser1

Password

Response

```
{
  "Response": "
  {\"homeDirectory\":\"/padbucket3\", \"homeDirectoryDetails\":null, \"homeDirectoryType\":\"PATH\", \"posixProfile\",
  \"null\", \"publicKeys\":null, \"role\":\"arn:aws:iam::195886157073:role/MDGuy_53_Amazon_EFS\", \"policy\":null, \"userName\": \"transferuser1\", \"identityProviderType\":null, \"userConfigMessage\":null},
  \"StatusCode\": 200,
  \"Message\": \"\"
}
```

Cancel

Test

Si el usuario pertenece a más de un grupo al que tiene acceso, recibirá la siguiente respuesta.

```
"Response": "",  
"StatusCode": 200,  
"Message": "More than one associated access found for user's groups."
```

Eliminar el acceso al servidor de un grupo

Eliminación del acceso al servidor de un grupo

1. En la página de detalles del servidor, elija Acciones y, a continuación, elija Eliminar acceso.
2. En el cuadro de diálogo, confirme que desea eliminar el acceso para este grupo.

Al volver a la página de detalles del servidor, verá que el acceso a este grupo ya no aparece en la lista.

Conexión al servidor mediante SSH (Secure Shell)

Después de configurar el servidor y los usuarios, puede conectarse al servidor mediante SSH y utilizar el nombre de usuario completo para un usuario que tenga acceso.

```
sftp user@active-directory-domain@vpc-endpoint
```

Por ejemplo: `transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-svc-987654zyxabc.us-east-1.vpce.amazonaws.com`.

Este formato apunta a la búsqueda de la federación, lo que limita la búsqueda de un Active Directory potencialmente grande.

Note

Puede especificar un nombre de usuario sencillo. Sin embargo, en este caso, el código de Active Directory debe buscar en todos los directorios de la federación. Esto podría limitar la búsqueda y la autenticación podría fallar aunque el usuario tuviera acceso.

Tras la autenticación, el usuario se encuentra en el directorio de inicio que especificó al configurar el usuario.

Conexión AWS Transfer Family a un Active Directory autoadministrado mediante bosques y fideicomisos

Directory Service dispone de las siguientes opciones para conectarse a un Active Directory autoadministrado:

- One-way La confianza en el bosque (entrante AWS Managed Microsoft AD y saliente en el caso de Active Directory local) solo funciona para el dominio raíz.
- Para dominios secundarios, puede utilizar uno de los procedimientos a continuación:
 - Utilice la confianza bidireccional entre Active Directory AWS Managed Microsoft AD y el local
 - Utilice una confianza externa unidireccional para cada dominio secundario.

Al conectarse al servidor mediante un dominio de confianza, el usuario debe especificar el dominio de confianza, por ejemplo, `transferuserexample@mycompany.com`.

Uso AWS de Directory Service para los servicios de dominio Entra ID

Para los clientes que solo necesitan la transferencia por SFTP y no desean administrar un dominio, existe Simple Active Directory. Como alternativa, los clientes que desean disfrutar de las ventajas de Active Directory y la alta disponibilidad en un servicio totalmente administrado pueden usar AWS Managed Microsoft AD. Por último, para los clientes que desean aprovechar su bosque de Active Directory existente para realizar la transferencia por SFTP, existe Conector Active Directory.

Tenga en cuenta lo siguiente:

- Para aprovechar el bosque de Active Directory existente para sus necesidades de transferencia por SFTP, puede usar [Conector Active Directory](#).
- Si desea disfrutar de las ventajas de Active Directory y de la alta disponibilidad en un servicio totalmente administrado, puede utilizar AWS Directory Service for Microsoft Active Directory. Para obtener más información, consulte [Uso AWS de Directory Service para Microsoft Active Directory](#).

En este tema se describe cómo usar un conector de Active Directory y los [servicios de dominio Entra ID \(anteriormente Azure AD\) para autenticar a los](#) usuarios de SFTP Transfer con Entra ID.

Temas

- [Antes de empezar a utilizar AWS Directory Service para los servicios de dominio Entra ID](#)
- [Paso 1: Añadir los servicios de dominio Entra ID](#)

- [Paso 2: creación de una cuenta de servicio](#)
- [Paso 3: Configuración del AWS directorio mediante AD Connector](#)
- [Paso 4: Configurar el AWS Transfer Family servidor](#)
- [Paso 5: concesión de acceso a los grupos](#)
- [Paso 6: prueba de usuarios](#)

Antes de empezar a utilizar AWS Directory Service para los servicios de dominio Entra ID

 Note

AWS Transfer Family tiene un límite predeterminado de 100 grupos de Active Directory por servidor. Si su caso de uso requiere más de 100 grupos, considere la posibilidad de utilizar una solución de proveedor de identidad personalizada, tal como se describe en [Simplifique la autenticación de Active Directory con un proveedor de identidad personalizado para AWS Transfer Family](#).

Para AWS ello, necesita lo siguiente:

- Una nube privada virtual (VPC) en una AWS región en la que utilice sus servidores Transfer Family
- Al menos dos subredes privadas en la VPC
- Los VPC deben tener conexión a Internet
- Una puerta de enlace para clientes y una puerta de enlace privada virtual para la conexión VPN de sitio a sitio con Microsoft Entra

Para Microsoft Entra, necesitas lo siguiente:

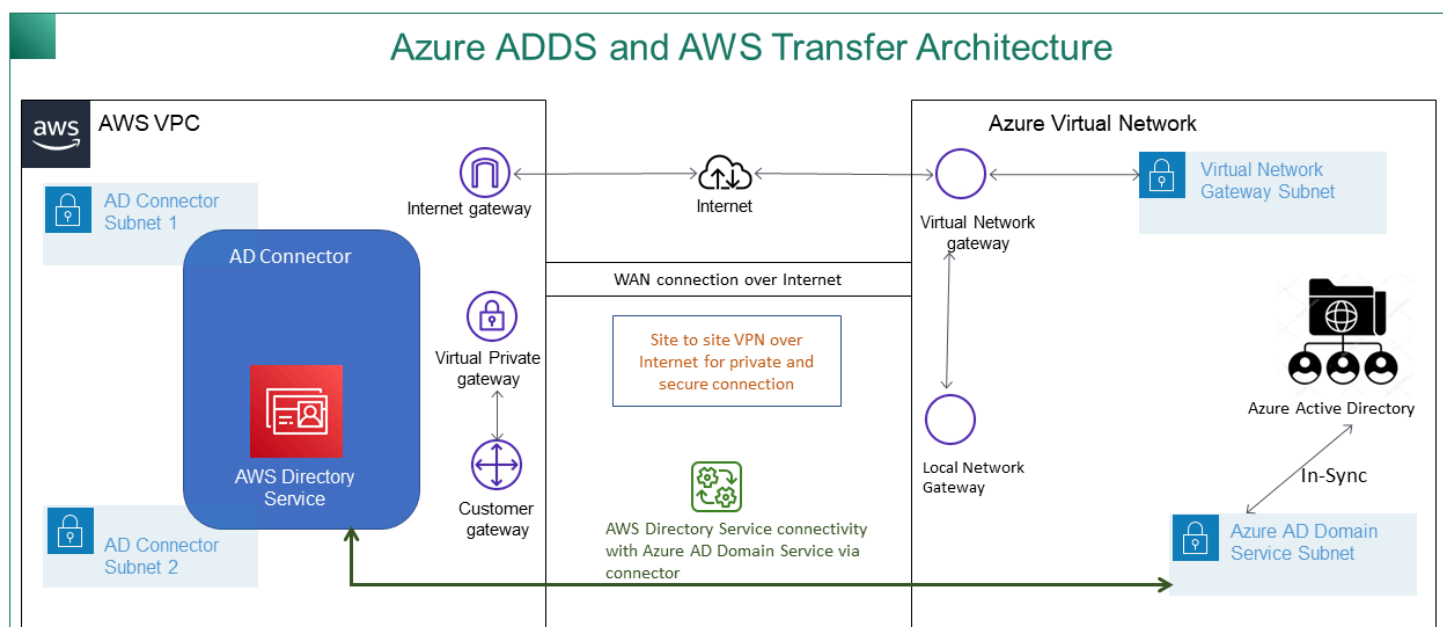
- Un servicio de dominio de Active Directory e ID de Entra
- Un grupo de recursos de Entra
- Una red virtual Entra
- Conectividad VPN entre su Amazon VPC y su grupo de recursos Entra

Note

Esto puede realizarse a través de túneles IPSEC nativos o mediante dispositivos VPN. En este tema, utilizamos túneles IPSEC entre una puerta de enlace de red Entra Virtual y una puerta de enlace de red local. Los túneles deben estar configurados para permitir el tráfico entre los puntos finales del Entra Domain Service y las subredes que alojan la AWS VPC.

- Una puerta de enlace para clientes y una puerta de enlace privada virtual para la conexión VPN de sitio a sitio con Microsoft Entra

En el siguiente diagrama se muestra la configuración necesaria antes de comenzar.



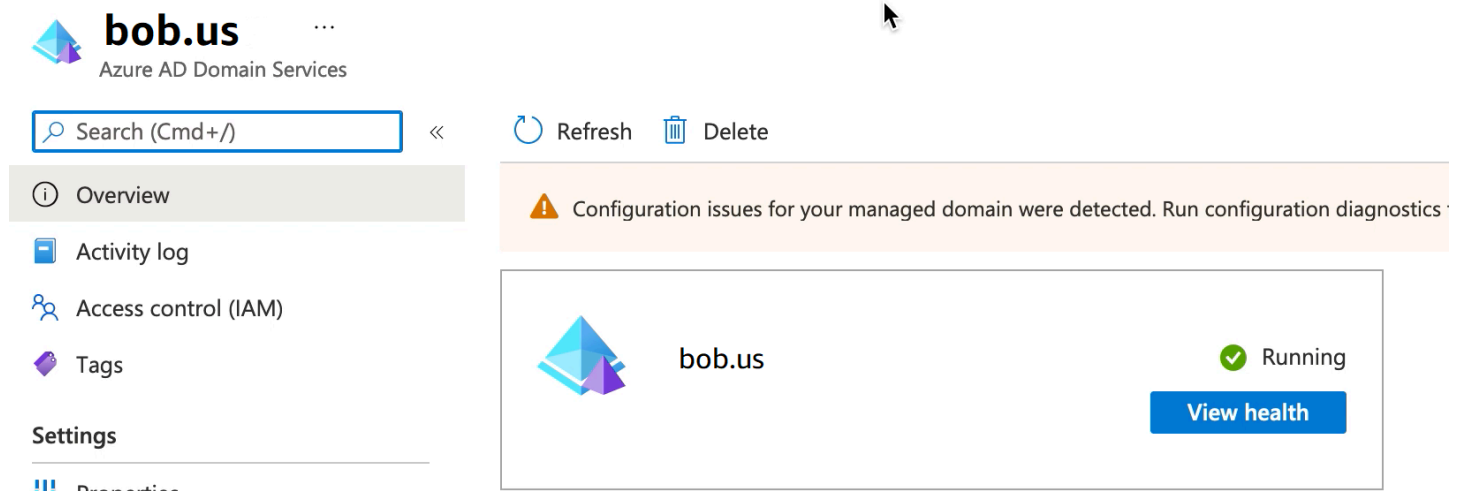
Paso 1: Añadir los servicios de dominio Entra ID

Entra ID no admite instancias de unión de dominios de forma predeterminada. Para realizar acciones como unirse a un dominio y utilizar herramientas como la política de grupo, los administradores deben habilitar los servicios de dominio Entra ID. Si aún no has añadido Entra DS o tu implementación actual no está asociada al dominio que quieres que utilice tu servidor de transferencia SFTP, debes añadir una nueva instancia.

Para obtener información sobre cómo habilitar los Servicios de dominio Entra ID, consulte el [Tutorial: Creación y configuración de un dominio administrado de Microsoft Entra ID Domain Services](#).

Note

Cuando habilite Entra DS, asegúrese de que esté configurado para el grupo de recursos y el dominio Entra al que está conectando su servidor de transferencia SFTP.



The screenshot shows the Azure AD Domain Services interface for the domain **bob.us**. The left sidebar contains navigation links: Overview (selected), Activity log, Access control (IAM), Tags, Settings, and Properties. The main content area displays the domain name **bob.us** with a status indicator showing a green checkmark and the word **Running**. A blue button labeled **View health** is visible. Above the domain card, there is a search bar and buttons for **Refresh** and **Delete**. A warning banner at the top of the main content area states: "Configuration issues for your managed domain were detected. Run configuration diagnostics".

Paso 2: creación de una cuenta de servicio

Entra debe tener una cuenta de servicio que forme parte de un grupo de administradores de Entra DS. Esta cuenta se usa con el conector de AWS Active Directory. Asegúrese de que esta cuenta esté sincronizada con Entra DS.

[Home](#) > [Default Directory](#) > [Users](#) > [bobatusa](#)


bobatusa | Profile

User



Edit



Reset password



Revoke sessions



Delete



Refresh



Got feedback?

Diagnose and solve problems

Manage



Profile



Assigned roles



Administrative units



Groups



Applications



Licenses



Devices



Azure role assignments



Authentication methods

Activity



Sign-in logs



Audit logs

bobatusa

bobsmith@xyz.com



User Sign-ins

30

20

10

0

Oct 10 Oct 17 Oct 24 Oct 31

Group memberships

2

Creation time

10/6/2021, 1:32:27 AM

Identity

Name

bobatusa

First name

Bob

Last name

Smith

User Principal Name

bobsmith@xyz.com

User type

Member

Tip

Multi-factor la autenticación para Entra ID no es compatible con los servidores Transfer Family que utilizan el protocolo SFTP. El servidor de Transfer Family no puede proporcionar el token de MFA después de que un usuario se autentique en SFTP. Asegúrese de deshabilitar el MFA antes de intentar conectarse.

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)
Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users



Multi-Factor Auth status: Any

bulk update



DISPLAY NAME ^

USER NAME

MULTI-FACTOR AUTH STATUS



Christopher

admin@christopher[REDACTED].com

Disabled



Robert

test@christopher[REDACTED].com

Disabled

Select a user

Paso 3: Configuración del AWS directorio mediante AD Connector

Una vez que haya configurado Entra DS y creado una cuenta de servicio con túneles VPN IPSEC entre su AWS VPC y la red virtual Entra, puede probar la conectividad haciendo ping a la dirección IP DNS de Entra DS desde AWS cualquier instancia de EC2.

Después de comprobar que la conexión está activa, puede continuar a continuación.

Para configurar el AWS directorio mediante AD Connector

1. Abra la consola [Servicio de directorio](#) y seleccione Directorios.
2. Seleccione Configurar directorio.
3. Para el tipo de directorio, elija Conector de AD.
4. Seleccione un tamaño de directorio, seleccione Siguiente y, a continuación, seleccione su VPC y sus subredes.
5. Seleccione Siguiente y, a continuación, rellene los campos de la siguiente manera:
 - Nombre DNS del directorio: introduce el nombre de dominio que utilizas para tu Entra DS.
 - Direcciones IP de DNS: introduzca sus direcciones IP de Entra DS.
 - Nombre de usuario de la cuenta del servidor y contraseña: introduzca los detalles de la cuenta de servicio que creó en el Paso 2: Crear una cuenta de servicio.
6. Complete las pantallas para crear el servicio de directorio.

Ahora el estado del directorio debería ser Activo y está listo para usarse con un servidor de transferencia SFTP.

[Directory Service](#) > [Directories](#)

 **Did you know?**
You can deploy an AWS Managed Microsoft AD (Enterprise Edition) directory across AWS Regions. Once configured, AWS automatically replicates your directory data in multiple Regions so everything stays in sync. [Learn more](#)

Directories (1) [Info](#)

 **Actions**  **Set up directory**

 **1**  

	Directory ID	Directory name	Type	Size	Multi-Region	Status	Launch date
	d-906752c0d7		AD Connector	Small	Not applicable	 Active	Nov 3, 2021

Paso 4: Configurar el AWS Transfer Family servidor

Cree un servidor Transfer Family con el protocolo SFTP y el tipo de proveedor de identidad de AWS Directory Service. En la lista desplegable de Directorios, seleccione el directorio que agregó en el Paso 3: configuración del directorio de AWS mediante AD Connector.

Note

No puede eliminar un directorio de Microsoft AD en AWS Directory Service si lo utilizó en un servidor Transfer Family. Primero debe eliminar el servidor y, a continuación, puede eliminar el directorio.

Paso 5: concesión de acceso a los grupos

Tras crear el servidor, debe elegir qué grupos del directorio deben tener acceso para cargar y descargar archivos mediante los protocolos habilitados AWS Transfer Family. Para ello, debe crear un acceso.

Note

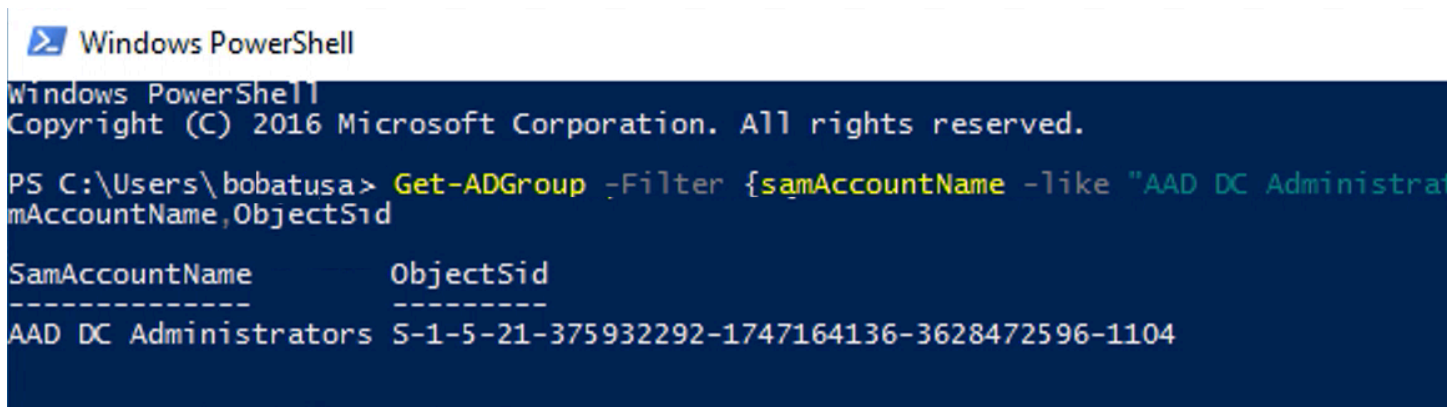
Los usuarios deben pertenecer directamente al grupo al que se concede el acceso. Por ejemplo, supongamos que Bob es un usuario y pertenece al grupo A y que el propio grupo A está incluido en el grupo B.

- Si concede acceso al Grupo A, a Bob se le concede el acceso.
- Si concede acceso al grupo B (y no al grupo A), Bob no tendrá acceso.

Para conceder el acceso, debe recuperar el SID del grupo.

Use el siguiente PowerShell comando de Windows para recuperar el SID de un grupo y *YourGroupName* sustitúyalo por el nombre del grupo.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select SamAccountName, ObjectSid
```



```

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\bobatusa> Get-ADGroup -Filter {samAccountName -like "AAD DC Administrat
mAccountName,ObjectSid

SamAccountName      ObjectSid
-----
AAD DC Administrators S-1-5-21-375932292-1747164136-3628472596-1104
  
```

Conceda acceso a los grupos

1. Abra <https://console.aws.amazon.com/transfer/>.
2. Ve a la página de detalles del servidor y, en la sección Accesos, seleccione Añadir acceso.
3. Introduzca el SID que recibió de la salida del procedimiento anterior.
4. En Access, elija un AWS Identity and Access Management rol para el grupo.
5. En la sección Política, elija una política. El valor predeterminado es None (Ninguno).
6. En el directorio principal, elija un bucket de Amazon S3 que se corresponda con el directorio principal del grupo.
7. Seleccione Añadir para crear la asociación.

Los detalles de su servidor de transferencia deben ser similares a los siguientes:

Protocols
Edit

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider
Edit

Identity provider type
AWS Directory Service

Directory ID
d-123456789a

Accesses (1)
Actions ▾
Add access

☐
External Id

☐
S-1-5-21-375932292-1747164136-3628472596-1104

☐
Home directory

☐
/s3/transfer

☐
Role

☐
sftp-user-role

Paso 6: prueba de usuarios

Puede probar ([Probando usuarios](#)) si un usuario tiene acceso al directorio AWS Managed Microsoft AD de su servidor. Un usuario debe pertenecer exactamente a un grupo (un identificador externo) que aparece en la sección Acceso de la página Configuración del punto de conexión. Si el usuario no está en ningún grupo o está en más de un grupo, no se le concede el acceso.

Uso de directorios lógicos para simplificar las estructuras de directorios de Transfer Family

Los directorios lógicos simplifican la estructura AWS Transfer Family de directorios del servidor. Con los directorios lógicos, puede crear una estructura de directorios virtuales con nombres fáciles de usar por los que navegan los usuarios cuando se conectan a su bucket de Amazon S3 o al sistema de archivos Amazon EFS. Esto impide que los usuarios vean las rutas de directorio reales, los nombres de los buckets y los nombres del sistema de archivos.

Note

Debe usar políticas de sesión para que los usuarios finales solo puedan realizar las operaciones que usted les permita realizar.

Debe usar directorios lógicos para crear un directorio virtual fácil de usar para sus usuarios finales y eliminar los nombres de los segmentos. Las asignaciones de directorios lógicos solo permiten a los usuarios acceder a sus rutas lógicas y subdirectorios designados, y prohíben las rutas relativas que atraviesan las raíces lógicas.

Transfer Family valida todas las rutas que puedan incluir elementos relativos y bloquea activamente estas rutas para que no se resuelvan antes de pasarlas a Amazon S3; esto evita que los usuarios vayan más allá de sus asignaciones lógicas.

Si bien Transfer Family impide que los usuarios finales accedan a directorios fuera de su directorio lógico, le recomendamos que también utilice funciones o políticas de sesión únicas para aplicar los privilegios mínimos a nivel de almacenamiento.

Comprender el chroot y la estructura de directorios

Una operación chroot le permite establecer el directorio raíz de un usuario en cualquier ubicación de la jerarquía de almacenamiento. Esto restringe a los usuarios a su directorio principal o raíz configurado, lo que impide el acceso a los directorios de nivel superior.

Pensemos en un caso en el que un usuario de Amazon S3 esté limitado a `amzn-s3-demo-bucket/home/${transfer:UserName}`. Sin `chroot`, algunos clientes podrían permitir a los usuarios pasar a `/amzn-s3-demo-bucket/home`, lo que requeriría cerrar sesión e iniciar sesión para volver al directorio correspondiente. Al realizar una operación de `chroot`, se evita este problema.

Puede crear estructuras de directorios personalizadas en varios buckets y prefijos. Esto resulta útil si tu flujo de trabajo requiere un diseño de directorio específico que los prefijos de bucket por sí solos no pueden proporcionar. También puede vincular a varias ubicaciones no contiguas dentro de Amazon S3, de forma similar a la creación de un enlace simbólico en un sistema de archivos de Linux en el que la ruta del directorio hace referencia a una ubicación diferente del sistema de archivos.

Reglas para el uso de directorios lógicos

En esta sección, se describen algunas reglas y otras consideraciones para usar directorios lógicos.

Límites de mapeo

- Solo se permite un mapeo cuando `Entry` está `"/` (no se permiten rutas superpuestas).
- Los directorios lógicos admiten mapeos de hasta 2,1 MB para los usuarios personalizados de IDP y AD, y de 2000 entradas para los usuarios gestionados por el servicio. Puede calcular el tamaño de las asignaciones de la siguiente manera:
 1. Escribe un mapeo típico en el formato `{"Entry": "/"entry-path", "Target": "/"target-path"}`, donde *entry-path* y *target-path* están los valores reales que utilizarás.
 2. Cuente los caracteres de esa cadena y, a continuación, añada uno (1).
 3. Multiplique ese número por el número aproximado de mapeos que tiene para su servidor.

Si el número estimado en el paso 3 es inferior a 2,1 MB, las asignaciones se encuentran dentro del límite aceptable.

Requisitos de la ruta de destino

- Utilice la `${transfer:UserName}` variable si la ruta del depósito o del sistema de archivos se ha parametrizado en función del nombre de usuario.
- Los destinos se pueden configurar para que apunten a diferentes depósitos o sistemas de archivos de Amazon S3, siempre que la función de IAM asociada tenga los permisos necesarios para acceder a esas ubicaciones de almacenamiento.

- Todos los objetivos deben empezar con una barra inclinada (/), pero no pueden terminar con una. Por ejemplo, /amzn-s3-demo-bucket/images es correcto, mientras que amzn-s3-demo-bucket/images y /amzn-s3-demo-bucket/images/ no lo es.

Consideraciones de almacenamiento

- Amazon S3 es un almacén de objetos en el que las carpetas solo existen como un concepto virtual. Cuando se utiliza el almacenamiento de Amazon S3, Transfer Family muestra los prefijos como directorios en las operaciones STAT, incluso si no hay ningún objeto de cero bytes con una barra al final. Un objeto de cero bytes propiamente dicho con una barra al final también se presenta como directorio en las operaciones de STAT. Este comportamiento se describe en [Organizar objetos en la consola de Amazon S3 mediante carpetas](#) de la Guía del usuario de Amazon Simple Storage Service.
- Para las aplicaciones que necesitan distinguir entre archivos y carpetas, utilice Amazon Elastic File System (Amazon EFS) como opción de almacenamiento de Transfer Family.
- Si especifica valores de directorio lógicos para su usuario, el parámetro que utilice depende del tipo de usuario:
 - Para los usuarios administrados por el servicio, introduzca los valores del directorio lógico en `HomeDirectoryMappings`.
 - Para los usuarios de proveedores de identidad personalizados, proporcione los valores del directorio lógico en `HomeDirectoryDetails`.

Valores del directorio de usuarios

- El parámetro para especificar los valores del directorio lógico depende del tipo de usuario:
 - Para los usuarios administrados por el servicio, introduzca los valores del directorio lógico en `HomeDirectoryMappings`.
 - Para los usuarios de proveedores de identidades personalizados, proporcione los valores del directorio lógico en `HomeDirectoryDetails`.
- Al usar `LOGICAL HomeDirectoryType`, puede especificar un `HomeDirectory` valor para los usuarios gestionados por el servicio, el acceso a Active Directory y las implementaciones de proveedores de identidad personalizados, siempre que `HomeDirectoryDetails` se indique en la respuesta. Si no se especifica, el `HomeDirectory` valor predeterminado es. /

Para obtener más información sobre cómo implementar directorios lógicos, consulte [Implementación de directorios lógicos](#).

Implementación de directorios lógicos

Important

Requisitos del directorio raíz

- Si no utiliza la configuración de optimización del rendimiento de Amazon S3, su directorio raíz debe existir al inicio.
- Para Amazon S3, esto significa crear un objeto de cero bytes que termine con una barra diagonal (/).
- Para evitar este requisito, considere habilitar la optimización del rendimiento de Amazon S3 al crear o actualizar el servidor.
- Al especificar a HomeDirectory con LOGICAL HomeDirectoryType, el valor debe asignarse a una de sus asignaciones de directorios lógicos. El servicio lo valida tanto durante la creación del usuario como durante las actualizaciones para evitar configuraciones que no funcionen.

Configuración del directorio principal lógico

Cuando utilice LOGICAL como su archivo HomeDirectoryType, tenga en cuenta lo siguiente:

- El HomeDirectory valor debe corresponder a una de las asignaciones de directorios lógicos existentes.
- El sistema lo valida automáticamente durante la creación y las actualizaciones del usuario.
- Esta validación evita las configuraciones que podrían provocar problemas de acceso.

Habilite los directorios lógicos

Para usar directorios lógicos para un usuario, defina LOGICAL el HomeDirectoryType parámetro en. Haga esto cuando cree un nuevo usuario o actualice un usuario existente.

```
"HomeDirectoryType": "LOGICAL"
```

Habilitar **chroot** para los usuarios

Para chroot, cree una estructura de directorios que consista en un único Entry y un par Target para cada usuario. La entrada/representa la carpeta raíz, mientras que Target especifica la ubicación real en el depósito o sistema de archivos.

Example for Amazon S3

```
[{"Entry": "/", "Target": "/amzn-s3-demo-bucket/jane"}]
```

Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

Puede utilizar una ruta absoluta, como en el ejemplo anterior, o puede usar una sustitución dinámica del nombre de usuario por `${transfer:UserName}`, como en el ejemplo siguiente.

```
[{"Entry": "/", "Target":  
"/amzn-s3-demo-bucket${transfer:UserName}"}]
```

En el ejemplo anterior, el usuario está bloqueado en su directorio raíz y no puede ascender en la jerarquía.

Estructura de directorio virtual

Para una estructura de directorios virtuales, puede crear varios pares Entry Target, con destinos en cualquier lugar de los buckets S3 o sistemas de archivos EFS, incluso en varios buckets o sistemas de archivos, siempre que la asignación de roles de IAM del usuario tenga permisos para acceder a ellos.

En el siguiente ejemplo de estructura virtual, cuando el usuario inicia sesión en AWS SFTP, se encuentra en el directorio raíz con los subdirectorios de/pics, /doc/reporting, y. /anotherpath/subpath/financials

Note

A menos que elija optimizar el rendimiento de sus directorios de Amazon S3 (al crear o actualizar un servidor), el usuario o el administrador deberán crear los directorios si aún no

existen. Evitar este problema es un motivo para considerar la optimización del rendimiento de Amazon S3.

En el caso de Amazon EFS, aún necesita que el administrador cree las asignaciones lógicas del / directorio.

```
[
{"Entry": "/pics", "Target": "/amzn-s3-demo-bucket1/pics"},
{"Entry": "/doc", "Target": "/amzn-s3-demo-bucket1/anotherpath/docs"},
{"Entry": "/reporting", "Target": "/amzn-s3-demo-bucket2/Q1"},
{"Entry": "/anotherpath/subpath/financials", "Target": "/amzn-s3-demo-bucket2/financials"}]
```

Note

Solo puede cargar archivos en las carpetas específicas que se asignen. Esto significa que, en el ejemplo anterior, no puede subirlos a los directorios /anotherpath o anotherpath/subpath, únicamente a anotherpath/subpath/financials. Tampoco puede asignar esas rutas directamente, ya que no se permite la superposición de rutas.

Por ejemplo, supongamos que realiza las siguientes asignaciones:

```
{
  "Entry": "/pics",
  "Target": "/amzn-s3-demo-bucket/pics"
},
{
  "Entry": "/doc",
  "Target": "/amzn-s3-demo-bucket/mydocs"
},
{
  "Entry": "/temp",
  "Target": "/amzn-s3-demo-bucket2/temporary"
}
```

Solo puede cargar archivos en esos buckets. Cuando se conecta por primera vez a través de sftp, iniciará en el directorio raíz, /. Si intenta cargar un archivo en ese directorio, la carga no se realizará correctamente. Los siguientes comandos muestran una secuencia de ejemplo:

```
sftp> pwd
Remote working directory: /
sftp> put file
Uploading file to /file
remote open("/file"): No such file or directory
```

Para subirlo a cualquier `directory/sub-directory`, debe asignar de forma explícita la ruta a `sub-directory`.

Para obtener más información sobre la configuración de los directorios lógicos y chroot para sus usuarios, incluida una AWS CloudFormation plantilla que pueda descargar y usar, consulte [Simplifique la estructura de AWS SFTP con directorios chroot y lógicos](#) en el blog de almacenamiento. AWS

Ejemplos de configuración de directorios lógicos

En este ejemplo, creamos un usuario y asignamos dos directorios lógicos. El siguiente comando crea un nuevo usuario (para un servidor de Transfer Family existente) con directorios lógicos `pics` y `doc`.

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs\"}]" \
  --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Si **marymajor** es un usuario existente y su tipo de directorio de inicio es `PATH`, puede cambiarlo a `LOGICAL` con un comando similar al anterior.

```
aws transfer update-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
```

```
--home-directory-mappings "[{"Entry\\":\\"/pics\\", \"Target\\":\\"/amzn-s3-demo-bucket1/pics\\"}, {"Entry\\":\\"/doc\\", \"Target\\":\\"/amzn-s3-demo-bucket2/test/mydocs\\"}]"
```

Tenga en cuenta lo siguiente:

- Si los directorios `/amzn-s3-demo-bucket1/pics` y `/amzn-s3-demo-bucket2/test/mydocs` aún no existen, el usuario (o un administrador) debe crearlos.

Note

El servidor Transfer Family crea estos directorios automáticamente si ha configurado directorios optimizados.

- Cuando **marymajor** se conecta al servidor y ejecuta el `ls -l` comando, Mary ve lo siguiente:

```
drwxr--r--  1      -      -      0 Mar 17 15:42 doc
drwxr--r--  1      -      -      0 Mar 17 16:04 pics
```

- **marymajor** no puede crear ningún archivo o directorio en este nivel. Sin embargo, dentro de `pics` y `doc`, puede añadir subdirectorios.
- Archivos que Mary añade `pics` y `doc` se añaden a las rutas de Amazon S3 `/amzn-s3-demo-bucket2/test/mydocs`, `/amzn-s3-demo-bucket1/pics` respectivamente.
- En este ejemplo, especificamos dos buckets diferentes para ilustrar esa posibilidad. Sin embargo, puede usar el mismo bucket para varios o todos los directorios lógicos que especifique para el usuario.

Este ejemplo proporciona una configuración alternativa para una ruta de inicio lógica.

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory /home/marymajor \
  --home-directory-mappings "[{"Entry\\":\\"/home/marymajor/pics\\", \"Target\\":\\"/amzn-s3-demo-bucket1/pics\\"}, {"Entry\\":\\"/home/marymajor/doc\\", \"Target\\":\\"/amzn-s3-demo-bucket2/test/mydocs\\"}]" \
  --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Tenga en cuenta lo siguiente:

- Las asignaciones proporcionan una ruta común/home/marymajor, que es la primera parte de las dos rutas lógicas. A continuación, se pueden añadir archivos a las carpetas pics y doc.
- Como en el ejemplo anterior, el directorio principal,/home/marymajor, es de solo lectura.

Configuración de directorios lógicos para Amazon EFS

Si su servidor de Transfer Family utiliza Amazon EFS, el directorio de inicio del usuario debe crearse con acceso de lectura y escritura para que el usuario pueda trabajar en su directorio de inicio lógico. El usuario no puede crear este directorio por sí mismo, ya que carecería de permisos para `mkdir` en su directorio de inicio lógico.

Si el directorio de inicio del usuario no existe y este ejecuta un comando `ls`, el sistema responde de la siguiente manera:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Un usuario con acceso administrativo al directorio de inicio debe crear el directorio de inicio lógico del usuario.

Respuesta personalizada AWS Lambda

Puede utilizar directorios lógicos con una función de Lambda que se conecte al proveedor de identidad personalizado. Para ello, en la función de Lambda, especifique `HomeDirectoryType` como **LOGICAL**, y añada los valores `Entry` y `Target` para el parámetro `HomeDirectoryDetails`. Por ejemplo:

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{\"Entry\": \"/\", \"Target\": \"/amzn-s3-demo-bucket/
theRealFolder\"}]"
```

El siguiente código es un ejemplo de una respuesta correcta de una llamada de autenticación de Lambda personalizada.

```
aws transfer test-identity-provider \
  --server-id s-1234567890abcdef0 \
  --user-name myuser
```



```
{
  "Url": "https://a1b2c3d4e5.execute-api.us-east-2.amazonaws.com/prod/servers/s-1234567890abcdef0/users/myuser/config",
  "Message": "",
  "Response": "{\\"Role\\": \\"arn:aws:iam::123456789012:role/bob-usa-role\\",
    \\"HomeDirectoryType\\": \\"LOGICAL\\",
    \\"HomeDirectoryDetails\\": \\"[{\\\\"Entry\\\\":\\\\""/myhome\\\\"},\\\\"
\\\"Target\\\\":\\\\""/amzn-s3-demo-bucket/theRealFolder\\\\"}]\\",
    \\"PublicKeys\\": \\"[ssh-rsa myrsapubkey]\\\"",
  "StatusCode": 200
}
```

Note

La línea "Url": se devuelve solo si utiliza un método de puerta de enlace API como proveedor de identidad personalizado.

Acceda a sus sistemas de archivos FSx para NetApp ONTAP con Transfer Family

Contenido

- [Descripción general de](#)
- [Requisitos previos](#)
 - [Requisitos de FSx para ONTAP NetApp](#)
 - [Permisos de IAM necesarios](#)
- [Cómo funciona el almacenamiento FSx con Transfer Family](#)
 - [Identidad de usuario del sistema de archivos](#)
- [Creación de un punto de acceso S3 para FSx](#)
 - [Denominación de puntos de acceso](#)
 - [Creación de un punto de acceso para FSx para ONTAP NetApp](#)
 - [Configuración de los permisos del sistema de archivos](#)
- [Uso de alias de puntos de acceso S3 con FSx](#)
 - [Acerca de los alias de los puntos de acceso](#)
 - [Cómo encontrar el alias del punto de acceso](#)

- [Configuración de Transfer Family para el almacenamiento FSx](#)
 - [Creación de un rol de IAM](#)
- [Administración de usuarios para el almacenamiento de FSx](#)
 - [Creación de un usuario](#)
 - [Configuración de múltiples mapeos de directorios](#)
- [Configuración de clientes de transferencia de archivos](#)
 - [Configuración WinSCP](#)
 - [Otros clientes SFTP](#)
- [Solución de problemas de almacenamiento FSx](#)
 - [Problemas con el funcionamiento de los archivos](#)

Descripción general de

Transfer Family es compatible con Amazon FSx para NetApp ONTAP a través de puntos de acceso S3. Amazon FSx para NetApp ONTAP es un servicio totalmente gestionado que proporciona un almacenamiento de archivos altamente fiable, escalable, de alto rendimiento y rico en funciones basado en NetApp el popular sistema de archivos ONTAP. Al configurar Transfer Family con un sistema de archivos FSx, los usuarios se conectan a los puntos finales de Transfer Family mediante clientes de transferencia de archivos estándar. Transfer Family dirige las operaciones de archivos a través de un punto de acceso S3 conectado al volumen FSx, mientras que los datos permanecen en el sistema de archivos FSx. Para obtener más información sobre FSx para NetApp ONTAP, consulte [¿Qué es Amazon FSx para ONTAP? NetApp](#)

Esta integración le permite:

- Transfiera archivos mediante los protocolos SFTP, FTPS o FTP a un almacenamiento de archivos de nivel empresarial
- Acceda a los mismos datos a través de varios protocolos (SFTP, NFS, SMB)
- Utilice las funciones de FSx, como las instantáneas, las copias de seguridad y la organización de datos en niveles

Important

Algunas operaciones de archivos no se admiten cuando se utilizan sistemas de archivos FSx con Transfer Family, incluidas las operaciones de cambio de nombre y adición. Para las

operaciones de carga, el tamaño de los archivos está limitado a 5 GB. Para obtener una lista completa de las limitaciones, consulte [Compatibilidad con los puntos de acceso](#).

Requisitos previos

Antes de configurar Transfer Family con Amazon FSx, debe cumplir los siguientes requisitos.

Requisitos de FSx para ONTAP NetApp

Para utilizar FSx para NetApp ONTAP con Transfer Family, necesita:

- Un sistema de archivos FSx para NetApp ONTAP que ejecute ONTAP 9.17.1 o posterior
- El sistema de archivos y el punto de acceso S3 en la misma región AWS
- La misma AWS cuenta que posee el sistema de archivos y el punto de acceso

Para obtener más información, consulte [Introducción a Amazon FSx para NetApp](#) ONTAP.

Permisos de IAM necesarios

Puede configurar cada punto de acceso S3 con distintos permisos y controles de red que S3 aplicará a cualquier solicitud que se realice mediante ese punto de acceso. Los puntos de acceso S3 admiten las políticas de recursos de IAM que puede utilizar para controlar el uso del punto de acceso por recurso, usuario u otras condiciones. Para que una aplicación o un usuario accedan a los archivos a través de un punto de acceso, tanto el punto de acceso como el volumen subyacente deben permitir la solicitud. Para obtener más información, consulte las [políticas de puntos de acceso de IAM](#).

Los puntos de acceso Amazon S3 para FSx utilizan un modelo de autorización de doble capa que combina los permisos de IAM con los permisos a nivel del sistema de archivos. Este enfoque garantiza que las solicitudes de acceso a los datos estén debidamente autorizadas tanto a nivel de AWS servicio como a nivel del sistema de archivos subyacente.

Para que una aplicación o un usuario puedan acceder correctamente a los datos a través de un punto de acceso, tanto la política del punto de acceso S3 como el volumen FSx subyacente deben permitir la solicitud.

Para crear y configurar esta integración, necesita los siguientes permisos:

- `fsx:CreateAndAttachS3AccessPoint`

- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`
- `s3:PutAccessPointPolicy`(si crea una política de puntos de acceso opcional)

Cómo funciona el almacenamiento FSx con Transfer Family

Al configurar Transfer Family con un sistema de archivos FSx, los siguientes componentes funcionan juntos para permitir la transferencia de archivos:

1. Un usuario se conecta al servidor Transfer Family mediante un cliente SFTP, FTPS o FTP.
2. Transfer Family autentica al usuario mediante identidades administradas por el servicio, un proveedor de identidades personalizado o. AWS Directory Service for Microsoft Active Directory. Una vez autenticado, Transfer Family asume la función de IAM asociada al usuario.
3. Para cada operación de archivo, Transfer Family actúa como un cliente API de S3 estándar, realiza solicitudes al punto de acceso S3 utilizando la función de IAM asumida por el usuario y verifica los permisos según la política del punto de acceso de S3.
4. El sistema de archivos FSx comprueba que el usuario del sistema de archivos asociado al punto de acceso tiene permiso para realizar la operación solicitada. A continuación, la operación de archivo se realiza en el volumen FSx.

Para que una operación de archivo se realice correctamente, ambas capas de autorización deben permitir la solicitud.

Note

La conexión de un punto de acceso S3 a un volumen FSx no cambia el comportamiento del volumen cuando se accede directamente a través de NFS o SMB. El acceso al protocolo de archivos existente sigue funcionando sin cambios.

Identidad de usuario del sistema de archivos

Cada punto de acceso utiliza una identidad de usuario del sistema de archivos que se especifica al crear el punto de acceso. Esta identidad autoriza todas las solicitudes de acceso a los archivos realizadas a través de ese punto de acceso. El usuario del sistema de archivos es una cuenta de usuario en el sistema de archivos Amazon FSx subyacente. Si el usuario del sistema de archivos

tiene acceso de solo lectura, solo se autorizan las solicitudes de lectura realizadas desde el punto de acceso y se bloquean las solicitudes de escritura. Si el usuario del sistema de archivos tiene acceso de lectura y escritura, se autorizan tanto las solicitudes de lectura como las de escritura al volumen adjunto realizadas mediante el punto de acceso.

Creación de un punto de acceso S3 para FSx

Antes de configurar Transfer Family, debe crear un punto de acceso S3 adjunto al volumen FSx. Los puntos de acceso S3 se denominan puntos de conexión de red que se conectan a una fuente de datos, como un bucket o Amazon FSx para el volumen de ONTAP. Puede crear y conectar un punto de acceso a un FSx para NetApp ONTAP mediante la consola, la AWS CLI o la API de Amazon FSx. Una vez adjuntado, puede usar las API de objetos de S3 para acceder a los datos de los archivos. Los datos seguirán residiendo en el sistema de archivos de Amazon FSx y seguirán siendo directamente accesibles para las cargas de trabajo existentes. Seguirá gestionando su almacenamiento con todas las funciones de gestión del almacenamiento de FSx for NetApp ONTAP, incluidas las copias de seguridad, las instantáneas, las cuotas de usuarios y grupos y la compresión.

Para obtener más información, consulte [Creación de puntos de acceso](#).

Denominación de puntos de acceso

Cuando asigne un nombre a su punto de acceso, siga estas pautas:

- Los nombres de los puntos de acceso deben ser únicos en su AWS cuenta y región.
- Los nombres no pueden terminar por `-ext-s3alias` (reservado para los alias).
- Evite incluir información confidencial en los nombres porque están publicados en el DNS.

Para obtener una lista completa de las reglas de nomenclatura, consulte [Reglas, restricciones y limitaciones de nomenclatura de los puntos de acceso](#).

Creación de un punto de acceso para FSx para ONTAP NetApp

Utilice el siguiente procedimiento para crear un punto de acceso S3 para un volumen FSx for NetApp ONTAP.

Para crear un punto de acceso (consola)

1. Abra la consola Amazon FSx en. <https://console.aws.amazon.com/fsx/>

2. En el panel de navegación, elija Sistema de archivos.
3. Elija su sistema de archivos FSx para NetApp ONTAP.
4. Seleccione la pestaña Volúmenes.
5. Seleccione el volumen que desee adjuntar.
6. En Acciones, elija Crear punto de acceso S3.
7. En Nombre del punto de acceso, introduzca un nombre descriptivo (por ejemplo, transfer-family-ap).
8. En el tipo de identidad de usuario del sistema de archivos, elija una de las siguientes opciones:
 - Identidad UNIX: para volúmenes con el estilo de seguridad UNIX
 - Identidad de Windows: para volúmenes con estilo de seguridad NTFS
9. (Opcional) En el caso de la política de puntos de acceso, introduzca una política de IAM que defina qué responsables de IAM pueden realizar determinadas operaciones en los objetos a los que se accede a través de este punto de acceso. Para obtener más información, consulte [Administrar el acceso a los puntos de acceso](#).
10. Seleccione Crear.
11. Tras la creación, anote el alias del punto de acceso para usarlo en la configuración de Transfer Family.

Note

Cuando AWS Transfer Family accede a los recursos de S3 en nombre de SFTP/FTPS los usuarios conectados, las solicitudes se originan en la AWS Transfer Family infraestructura, no en la VPC. Por ello, los puntos de acceso S3 configurados con un origen de red de VPC denegarán estas solicitudes. Sin embargo, incluso si utiliza un punto de acceso configurado con un origen de red de Internet, todo el tráfico entre Transfer Family y el punto de acceso permanece privado y viaja a través de la red AWS troncal, no atraviesa la Internet pública.

Configuración de los permisos del sistema de archivos

El usuario del sistema de archivos que especifique determinará qué operaciones pueden realizar los usuarios de Transfer Family. Debe configurar los permisos adecuados en el volumen FSx.

Ejemplo de UNIX:

```
# Create a directory for Transfer Family users
mkdir -p /vol1/transfer-users

# Set ownership to match the access point user
chown 1001:1001 /vol1/transfer-users

# Set permissions
chmod 755 /vol1/transfer-users
```

Ejemplo de Windows:

```
# Create a directory for Transfer Family users
New-Item -Path "D:\vol1\transfer-users" -ItemType Directory

# Set permissions for the file system user associated with the access point
# Replace DOMAIN\TransferUser with your Windows user identity
icacls "D:\vol1\transfer-users" /grant "DOMAIN\TransferUser:(OI)(CI)M" /T

# Verify permissions
icacls "D:\vol1\transfer-users"
```

Uso de alias de puntos de acceso S3 con FSx

Cuando utilice sistemas de archivos FSx con Transfer Family, debe utilizar los alias de punto de acceso S3. Transfer Family no admite el uso de ARN de puntos de acceso u otros métodos de referencia para el almacenamiento de FSx.

Important

AWS Transfer Family solo admite alias de puntos de acceso S3 cuando se utilizan sistemas de archivos FSx. No puede utilizar ARN de puntos de acceso ni URI de tipo hospedado virtual.

Important

El punto de acceso debe estar en la misma región que el volumen.

Acerca de los alias de los puntos de acceso

Al crear un punto de acceso S3 adjunto a un volumen FSx, Amazon S3 genera automáticamente un alias de punto de acceso. Este alias es un identificador único que puede utilizar en cualquier lugar donde utilice un nombre de bucket de S3.

Para los puntos de acceso adjuntos a los volúmenes de FSx, el alias utiliza el siguiente formato:

```
access-point-name-metadata-ext-s3alias
```

Ejemplo de alias:

```
my-fsx-ap-aqfqprnstn7aefdfbarligizwgfyfouse1a-ext-s3alias
```

Note

El `-ext-s3alias` sufijo está reservado para los alias de los puntos de acceso FSx. No puede utilizar este sufijo en los nombres de los puntos de acceso.

Cómo encontrar el alias del punto de acceso

Puede encontrar el alias del punto de acceso después de crear el punto de acceso.

Para buscar el alias del punto de acceso (consola)

1. Abra la consola Amazon FSx en <https://console.aws.amazon.com/fsx/>
2. En el panel de navegación, elija Sistema de archivos.
3. Elija su sistema de archivos
4. Elija la pestaña Volúmenes y seleccione el volumen para el que creó el punto de acceso.
5. Vaya a la columna de detalles del punto de acceso S3.
6. El alias se muestra en la columna Alias.

Para buscar el alias del punto de acceso (CLI)

Utilice el comando `describe-s3-access-point-attachments`.

```
aws fsx describe-s3-access-point-attachments \
```



```
--filters Name=file-system-id,Values=fs-0123456789abcdef0
```

La respuesta incluye el alias:

```
{
  "S3AccessPointAttachments": [
    {
      "S3AccessPoint": {
        "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-fsx-
ap",
        "Alias": "my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias"
      }
    }
  ]
}
```

Al configurar los usuarios de Transfer Family, utilice el alias del punto de acceso en las asignaciones del directorio principal.

Formato de directorio principal:

```
/access-point-alias/path/to/directory
```

Ejemplo:

```
/my-fsx-ap-aqfqprnstn7aefdfbarligizwgryfouse1a-ext-s3alias/users/jsmith
```

Configuración de Transfer Family para el almacenamiento FSx

Después de crear el punto de acceso S3, configure un servidor Transfer Family para usarlo.

Creación de un rol de IAM

Debe crear un rol de IAM que conceda a Transfer Family acceso al punto de acceso S3.

Important

Las políticas de IAM requieren el formato ARN del punto de acceso, no el alias. Utilice el formato `arn:aws:s3:region:account-id:accesspoint/access-point-name` en las

declaraciones de recursos de su política de IAM. El alias del punto de acceso (que termina en-`ext-s3alias`) solo se usa para mapear el directorio principal.

Creación del rol de IAM

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, elija Funciones y, a continuación, seleccione Crear función.
3. En Tipo de entidad de confianza, elija Servicio de AWS .
4. En Caso de uso, selecciona Transferir.
5. Elija Siguiente.
6. Selecciona Crear política e introduce tu política (consulta un ejemplo de política a continuación).
7. Adjunta la política al rol y selecciona Crear rol.

Ejemplo de política de IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFileOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap/
object/*"
    },
    {
      "Sid": "AllowDirectoryOperations",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
```

```
    "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap"  
  }  
]  
}
```

Administración de usuarios para el almacenamiento de FSx

Cree usuarios de Transfer Family con asignaciones de directorios principales que usen el alias del punto de acceso S3.

Creación de un usuario

Al crear un usuario para el almacenamiento de FSx, utilice el alias del punto de acceso en las asignaciones del directorio principal.

Para crear un usuario de Service Managed (consola)

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación, seleccione Servers (Servidores).
3. Seleccione su servidor.
4. En la sección Usuarios, seleccione Añadir usuario.
5. En Nombre de usuario, introduzca un nombre de usuario.
6. En Función, elija la función de IAM que creó.
7. En el directorio principal, elija Restringido.
8. Para las asignaciones del directorio principal, añada una asignación con el alias del punto de acceso:

```
[{"Entry": "/", "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/jsmith"}]
```

Para crear un usuario (CLI)

Utilice el comando `create-user`. Sustituya el alias del punto de acceso por el suyo.

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --path /my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/jsmith
```

```
--home-directory-type LOGICAL \
--home-directory-mappings '[
  {
    "Entry": "/",
    "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/
jsmith"
  }
]'
```

Configuración de múltiples mapeos de directorios

Puede asignar varios directorios virtuales a diferentes rutas del volumen FSx.

Ejemplo: directorios de carga y descarga separados

```
aws transfer create-user \
  --server-id s-0123456789abcdef0 \
  --user-name jsmith \
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \
  --home-directory-type LOGICAL \
  --home-directory-mappings '[
    {
      "Entry": "/inbox",
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/
jsmith/inbox"
    },
    {
      "Entry": "/outbox",
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/
jsmith/outbox"
    }
  ]'
```

Configuración de clientes de transferencia de archivos

Cuando utilice sistemas de archivos FSx con Transfer Family, debe configurar sus clientes de transferencia de archivos para deshabilitar las funciones que no son compatibles.

Configuración WinSCP

WinSCP utiliza una función de cambio de nombre temporal de forma predeterminada que no es compatible con los puntos de acceso S3 para FSx.

 Warning

Si no deshabilita la función de cambio de nombre temporal en WinSCP, se producirá un error al cargar los archivos.

Para deshabilitar el cambio de nombre temporal en WinSCP

1. Abre WinSCP.
2. En el cuadro de diálogo de inicio de sesión, seleccione Editar para modificar la configuración de la sesión.
3. Seleccione Avanzado.
4. En el menú de navegación de la izquierda, en Transferir, selecciona Endurance.
5. En Habilitar la transferencia resume/transfer a un nombre de archivo temporal, seleccione Desactivar.
6. Seleccione Aceptar para guardar la configuración.

Como alternativa, puedes deshabilitar esta configuración para una sesión existente:

1. Conéctese a su servidor Transfer Family.
2. Selecciona Opciones y, a continuación, Preferencias.
3. Selecciona Transfer y, a continuación, Endurance.
4. En Habilitar la transferencia resume/transfer a un nombre de archivo temporal, seleccione Desactivar.
5. Seleccione Aceptar.

Otros clientes SFTP

Para otros clientes SFTP, deshabilite las siguientes funciones, si están disponibles:

- Cargas de archivos temporales (cárguelos en un archivo temporal y, a continuación, cámbieles el nombre)
- Reanude las transferencias mediante archivos temporales
- Atomic carga mediante operaciones de cambio de nombre
- Modo de adición para las cargas

Consulte la documentación del cliente para conocer los pasos de configuración específicos.

Solución de problemas de almacenamiento FSx

En esta sección se describe cómo identificar y resolver problemas comunes al utilizar Transfer Family con sistemas de archivos FSx.

Problemas con el funcionamiento de los archivos

Permiso denegado

Si recibes errores de permiso denegado:

1. Compruebe que la función de IAM tenga los permisos correctos para el alias del punto de acceso. Para ello, puede realizar pruebas directamente con las API de S3.
2. Compruebe que la política de puntos de acceso permita el rol de IAM.
3. Compruebe que el usuario del sistema de archivos tenga permisos en la ruta de destino.
4. Confirme que la asignación del directorio principal utilice el alias de punto de acceso correcto.

La carga falla con WinSCP

Si la carga de archivos falla con WinSCP, deshabilite el cambio de nombre temporal:

1. En WinSCP, seleccione Opciones y, a continuación, Preferencias.
2. Selecciona Transfer y, a continuación, Endurance.
3. En Habilitar la transferencia resume/transfer a un nombre de archivo temporal, seleccione Desactivar.

Para obtener más información, consulte [the section called “Configuración de clientes de transferencia de archivos”](#).

La carga del archivo falla

Si se produce un error al cargar los archivos:

1. Compruebe que el tamaño del archivo sea inferior a 5 GB.
2. Compruebe que el volumen FSx tiene suficiente espacio de almacenamiento disponible.
3. Supervise CloudWatch las métricas de regulación.

Aplicaciones web Transfer Family

Puede crear aplicaciones web para habilitar una interfaz sencilla para transferir datos desde y hacia Amazon Simple Storage Service (S3) a través de un navegador web. Esto no requiere que cree ni aprovisiones AWS Transfer Family servidores.

Antes de la introducción de las aplicaciones web Transfer Family, los usuarios finales necesitaban usar una solución cliente, personalizada o de terceros para acceder a sus datos en Amazon S3. Esto se debía a los estrictos requisitos de seguridad para los clientes y socios, y a que las aplicaciones de los clientes eran difíciles de operar para los usuarios sin conocimientos técnicos.

Con el lanzamiento de las aplicaciones web, ahora puede ampliar un portal de marca, seguro y de alta disponibilidad para que sus usuarios finales naveguen, carguen y descarguen datos en Amazon S3. Las aplicaciones web se integran de forma nativa con AWS IAM Identity Center Amazon S3 Access Grants. Esto significa que solo los usuarios autenticados pueden ver los datos a los que están autorizados a acceder. Las aplicaciones web se crean con [Storage Browser para Amazon S3](#) y ofrecen las mismas funcionalidades para el usuario final en una oferta totalmente gestionada sin tener que escribir código ni alojar su propia aplicación.

Para obtener más información sobre las demás aplicaciones web Servicios de AWS que utilizas con las aplicaciones web de Transfer Family, consulta la siguiente documentación:

- [Administración del acceso con S3 Access Grants en la guía del usuario de Amazon Simple Storage Service](#)
- [AWS IAM Identity Center Guía del usuario](#)
- [Taller sobre las subvenciones de acceso a Amazon S3](#)
- [Anunciamos aplicaciones AWS Transfer Family web para transferencias de archivos de Amazon S3 totalmente gestionadas](#)

Los siguientes recursos están disponibles para ayudarle a empezar a utilizar las aplicaciones web Transfer Family.

- La guía del usuario ofrece un recorrido detallado paso a paso sobre cómo configurar una aplicación web Transfer Family aquí: [Tutorial: Cómo configurar una aplicación web básica de Transfer Family](#).
- El Centro de recursos de AWS introducción ofrece un tutorial aquí: [Cómo empezar con la aplicación AWS Transfer Family web](#).

- Consulte [Cómo empezar a utilizar la aplicación AWS Transfer Family web](#).

Regiones de AWS para aplicaciones web Transfer Family

AWS Transfer Family las aplicaciones web están disponibles en todas las regiones compatibles con Transfer Family, tal y como se indica en la [tabla de AWS regiones](#), excepto en Asia-Pacífico (Nueva Zelanda) AWS European Sovereign Cloud y.

Los puntos finales de VPC para aplicaciones web son compatibles en todos los Regiones de AWS lugares donde estén disponibles las aplicaciones web.

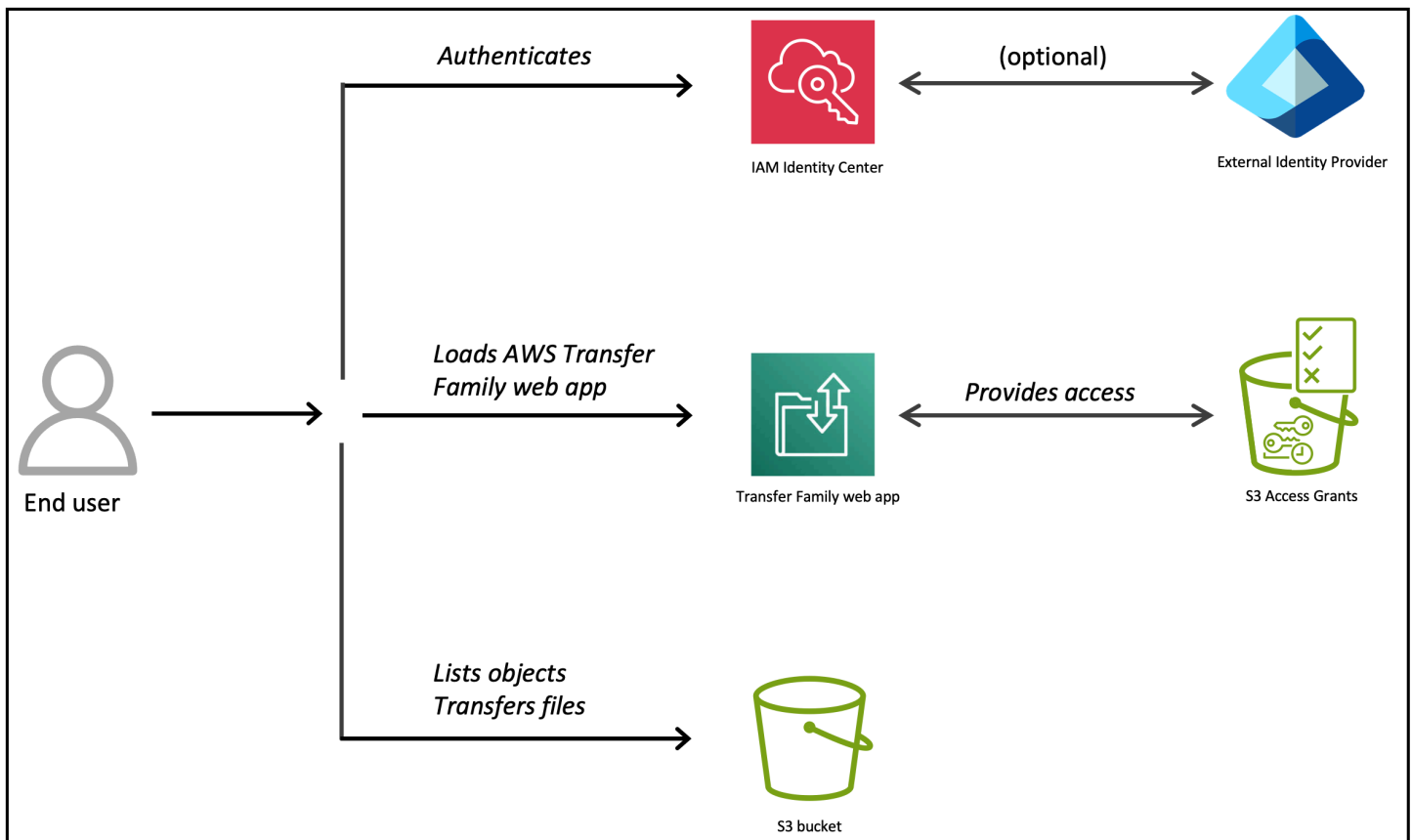
Compatibilidad de navegadores para aplicaciones AWS Transfer Family web

Las aplicaciones web Transfer Family son compatibles con los siguientes navegadores.

Navegador	Versión	Compatibilidad
Microsoft Edge	Últimas 3 versiones	Compatible
Mozilla Firefox	Últimas 3 versiones	Compatible
Google Chrome	Últimas 3 versiones	Compatible
Apple Safari	Últimas 3 versiones	Compatible

Cómo crear una aplicación web Transfer Family

El siguiente diagrama ilustra la arquitectura de la aplicación web Transfer Family.



Según el diagrama, puede ver que las aplicaciones web de Transfer Family interactúan con lo siguiente Servicios de AWS:

- Amazon S3 para almacenamiento y Amazon S3 Access Grants para adquirir credenciales de sesión.
- AWS IAM Identity Center como proveedor de identidad federado.
- Amazon CloudFront si configuras una URL personalizada para tu aplicación web.

Tenga en cuenta las siguientes limitaciones cuando utilice aplicaciones web.

- Número máximo de resultados de búsqueda por consulta: 10 000
- Los buckets de Amazon S3 que utiliza la aplicación web Transfer Family deben estar en la misma cuenta que la propia aplicación web. Cross-account Los buckets no se admiten actualmente.
- Amplitud máxima de búsqueda por consulta: 10 000 archivos buscados
- Tamaño máximo de carga por archivo: 160 GB (149 GiB)
- Tamaño máximo de archivo para copiar: 5,36 GB (5 GiB)

- No se admiten nombres de carpetas que comiencen o terminen con puntos (.)

Requisitos previos

En AWS Identity and Access Management, configure las funciones necesarias. Pegue los bloques de código que le proporcionamos en las instrucciones. Para obtener información sobre la configuración de las funciones necesarias, consulte [Configurar las funciones de IAM para las aplicaciones web Transfer Family](#).

- Cree un rol de portador de identidad.
- Cree un rol de IAM para que lo utilice S3 Access Grants. S3 Access Grants asume esta función de IAM para vender credenciales temporales al concesionario para la ubicación registrada de Amazon S3.

Proceso para crear una aplicación web Transfer Family

Para crear su aplicación web y poner en funcionamiento a sus usuarios finales, debe realizar las siguientes tareas:

1. Configure el Centro de identidades de IAM para que actúe como su proveedor de identidades federado. Realice las siguientes tareas en el Centro de identidades de IAM. Para obtener más información sobre la configuración del Centro de identidades de IAM, consulte. [Configura tu proveedor de identidad para las aplicaciones web Transfer Family](#)
 - a. Cree una instancia del IAM Identity Center, si aún no tiene una.
 - b. Determine su fuente de identidad. Puede ser el directorio predeterminado del centro de identidad de IAM o un proveedor externo (por ejemplo, Okta).
 - c. Cree o identifique los usuarios o grupos que utilizarán su aplicación web.
 - d. Si utiliza el directorio del Centro de identidades de IAM como fuente de identidad, anote los ID de usuario o grupo que cree. Los necesitará más adelante cuando cree una concesión de acceso mediante S3 Access Grants.
2. En Amazon S3, configure Amazon S3 Access Grants. Para obtener más información sobre Concesiones de acceso a S3, consulte [Configuración de las concesiones de acceso a Amazon S3 para las aplicaciones web Transfer Family](#).
 - Cree una instancia de S3 Access Grants si aún no tiene una Región de AWS.
 - Registre su ubicación mediante el rol de IAM.

- Cree la concesión de acceso.
3. En Transfer Family, lleve a cabo las siguientes tareas.
 - a. Cree la aplicación web Transfer Family. Para obtener más información sobre cómo crear la aplicación web Transfer Family, consulte [Configurar una aplicación web Transfer Family](#).

 Important

Configure el uso compartido de Cross-origin recursos (CORS) para todos los buckets de Amazon S3 que utilice su aplicación web. Para obtener información sobre la configuración de CORS, consulte. [Configure el uso compartido de Cross-origin recursos \(CORS\) para su depósito](#)

- b. Asigne usuarios o grupos a la aplicación web. Para obtener más información sobre cómo asignar usuarios y grupos, consulte [Asigne o añada usuarios o grupos a una aplicación web Transfer Family](#).
- c. (Opcional) Actualice el punto de acceso de su aplicación web con una URL personalizada. Para obtener información sobre cómo crear una URL personalizada, consulte [Actualice su terminal de acceso con una URL personalizada](#).
- d. Proporcione a sus usuarios finales la URL del punto de acceso para que puedan iniciar sesión e interactuar con su aplicación web.

Configura tu proveedor de identidad para las aplicaciones web Transfer Family

En la siguiente sección, se describe cómo configurar su proveedor de identidad.

Para empezar, debe tener una fuente de identidad. Puede utilizar un directorio del centro de identidad de IAM o un proveedor de identidad externo. AWS Directory Service for Microsoft Active Directory Transfer Family utiliza IAM Identity Center como proveedor de identidad federado, que es un sistema que almacena las credenciales de los usuarios y autentica a los usuarios de varias organizaciones.

Si no utiliza un directorio del centro de identidad de IAM como fuente de identidad, consulte los siguientes temas:

- [Administre un proveedor de identidad externo](#)

- [Conectarse a un directorio de Microsoft AD](#)
- [Instancias de organización y cuenta del IAM Identity Center](#)
- [Tutoriales sobre las fuentes de identidad del IAM Identity Center](#)

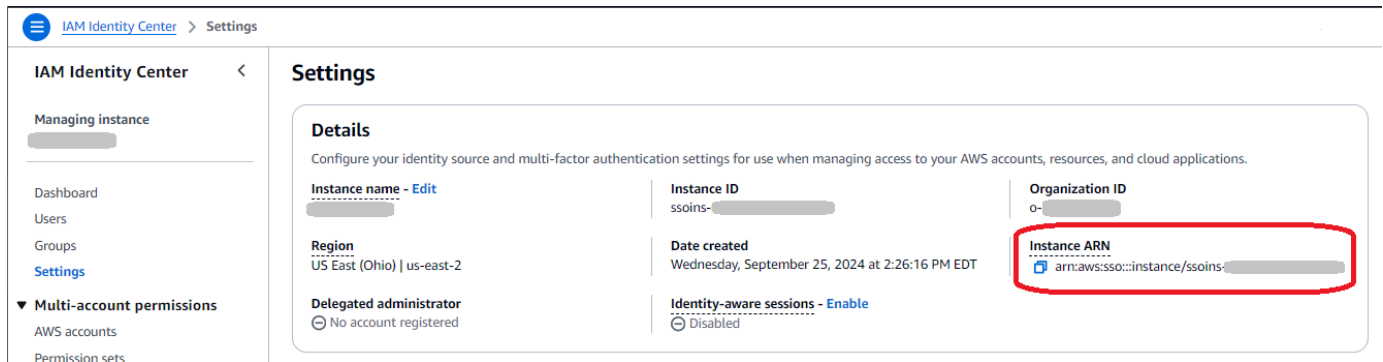
 Note

Solo puede tener una fuente de identidad en el Centro de identidades de IAM, por instancia, por instancia. Región de AWS Para obtener más información, consulte los [requisitos previos y las consideraciones del IAM Identity Center](#).

Si piensa utilizar el directorio del Centro de Identidad de IAM como fuente de identidad y desea realizar una configuración rápida, puede omitir este tema e ir [Crea una aplicación web de Transfer Family](#) a Crear una instancia del Centro de Identidad de IAM desde el asistente.

Para configurarlo AWS IAM Identity Center para su uso con las aplicaciones web Transfer Family

1. Inicia sesión en Consola de administración de AWS y abre la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. Puede crear y utilizar una instancia de cuenta o una instancia de organización de AWS IAM Identity Center.
 - Para obtener más información sobre las instancias de cuentas, consulte [Crear una instancia de cuenta de AWS IAM Identity Center](#). Con una instancia de cuenta de IAM Identity Center, puede implementar aplicaciones AWS gestionadas compatibles y aplicaciones gestionadas por clientes basadas en OpenID Connect (OIDC). Las instancias de cuentas admiten despliegues aislados de aplicaciones en una sola Cuenta de AWS, aprovechando las funciones del portal de acceso e identidad de los empleados de IAM Identity Center.
 - Para obtener más información sobre las instancias de organización, consulte [Instancias de organización del IAM Identity Center](#). Puede gestionar de forma centralizada el acceso de los usuarios y grupos con una única instancia de organización.
3. En la página de configuración del centro de identidad de IAM, anote el ARN de la instancia. Necesitará este valor cuando cree una instancia de Amazon S3 Access Grant.



4. Cree uno o más usuarios y, opcionalmente, grupos para usarlos con su aplicación web Transfer Family. Si utilizas un directorio del Centro de Identidad de IAM como proveedor de identidad, también puedes añadir usuarios directamente desde la propia aplicación web. Para obtener más información, consulte [Asigne o añada usuarios o grupos a una aplicación web Transfer Family](#).

Configurar las funciones de IAM para las aplicaciones web Transfer Family

Necesitará dos funciones: una para usarla como función portadora de identidad para su aplicación web y otra para configurar una concesión de acceso. Un rol de portador de identidad es un rol que incluye la identidad de un usuario autenticado en sus sesiones. Se utiliza para solicitar el acceso a los datos a S3 Access Grants en nombre del usuario.

Note

Puede omitir el procedimiento de creación de un rol de portador de identidad. Para obtener información sobre cómo hacer que el servicio Transfer Family cree el rol de portador de identidad, consulte [Crea una aplicación web de Transfer Family](#).

Puede omitir el procedimiento de creación de un rol de concesión de acceso. En el procedimiento para crear una concesión de acceso, en el paso en el que se registra una ubicación de S3, seleccione Crear un nuevo rol.

Cree un rol de portador de identidad

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en. <https://console.aws.amazon.com/iam/>
2. Elija Funciones y, a continuación, Crear función.

3. Elija Política de confianza personalizada y, a continuación, pegue el siguiente código.

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

4. Selecciona Siguiente y, a continuación, omite Añadir permisos y vuelve a seleccionar Siguiente.
5. Introduce un nombre, por ejemplo web-app-identity-bearer.
6. Elija Crear rol para crear el rol de portador de identidad.
7. Elija el rol que acaba de crear de la lista y, a continuación, en el panel de políticas de permisos, elija Añadir permisos > Crear política integrada.
8. En el editor de políticas, selecciona JSON y pega el siguiente bloque de código.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "s3:ListAccessGrantsInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

9. Para el nombre de la política, introduzca `yAllowS3AccessGrants`, a continuación, seleccione Crear política.

A continuación, debe crear la función que S3 Access Grants asume para vender las credenciales temporales al concesionario.

 Note

Si permite que el servicio cree el rol de portador de identidad para usted, ese rol establece una protección de adjunto confusa. Por lo tanto, su código es diferente al que se muestra aquí.

Cree un rol de concesión de acceso

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/iam/>.
2. Elija Funciones y, a continuación, Crear función. Este rol debe tener permiso para acceder a sus datos de S3 en Región de AWS.
3. Elija Política de confianza personalizada y, a continuación, pegue el siguiente código.

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

4. Selecciona Siguiente y agrega una política mínima como se describe en [Registrar una ubicación](#). Si bien no se recomienda, puede añadir la política AmazonS3FullAccessgestionada, que puede resultar demasiado permisiva para sus necesidades.
5. Seleccione Siguiente e introduzca un nombre (por ejemplo `access-grants-location`).
6. Elija Crear rol para crear el rol.

 Note

Si permites que el servicio cree la función de concesión de acceso por ti, esa función establece una confusa protección de diputado. Por lo tanto, su código es diferente al que se muestra aquí.

Configurar una aplicación web Transfer Family

En esta sección se describen los procedimientos para crear una aplicación web Transfer Family. Para asignar usuarios y grupos que puedan utilizarla, consulte [Asigne o añada usuarios o grupos a una aplicación web Transfer Family](#).

 Note

Repita estos procedimientos para añadir aplicaciones web adicionales. Puede reutilizar las funciones de IAM que creó anteriormente. Asegúrese de añadir los puntos finales de acceso a las nuevas aplicaciones web a la política de uso compartido de Cross-origin recursos (CORS) de cada grupo.

Crea una aplicación web de Transfer Family

 Note

Si no utiliza el directorio del Centro de Identidad de IAM como proveedor de identidad, no intente crear una aplicación web hasta que no haya configurado el Centro de Identidad de IAM y haya configurado un proveedor de identidades externo, tal y como se describe en [Configura tu proveedor de identidad para las aplicaciones web Transfer Family](#)

Complete los siguientes pasos para crear una aplicación web Transfer Family.

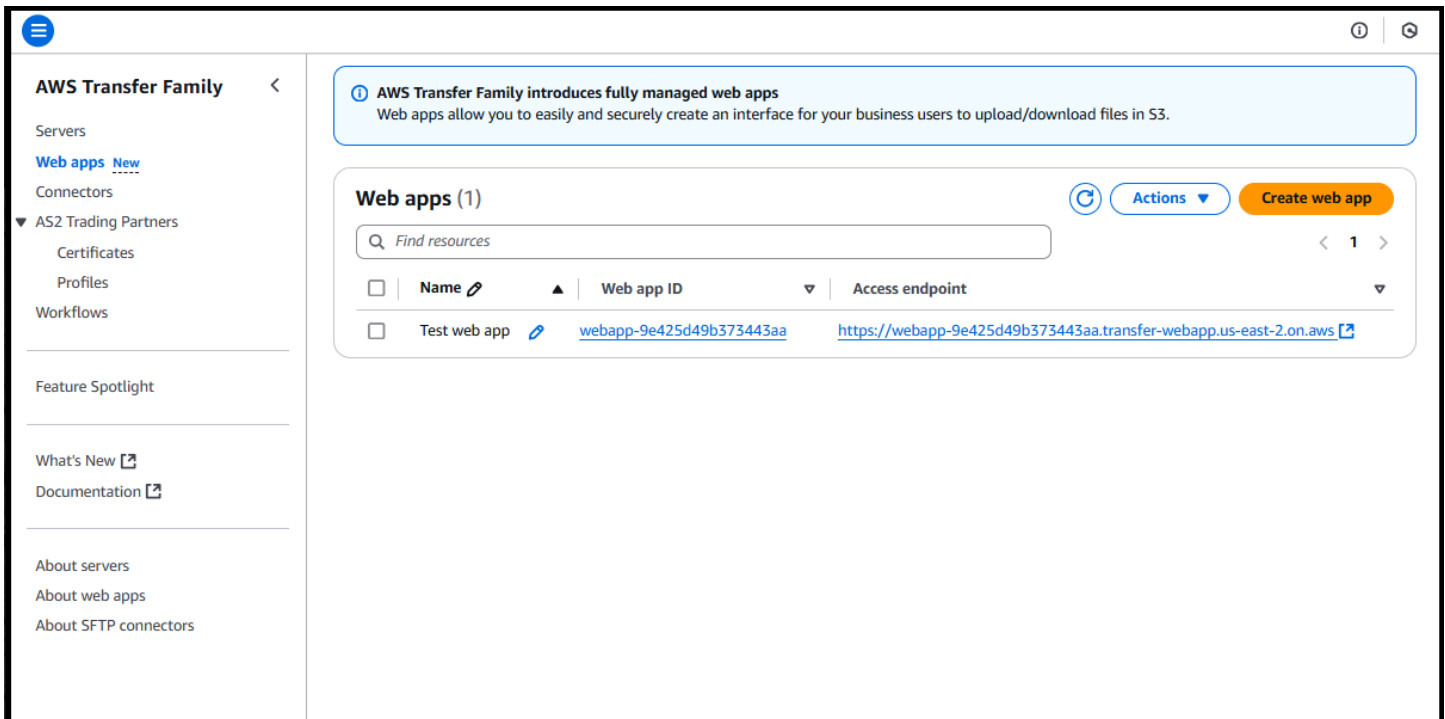
Para crear una aplicación web Transfer Family

1. Inicia sesión en Consola de administración de AWS y abre la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, selecciona Aplicaciones web.
3. Seleccione Crear aplicación web.

Para el acceso de autenticación, el panel se rellena de la siguiente manera.

- Si ya ha creado una organización o una instancia de cuenta en AWS IAM Identity Center, verá este mensaje: Su AWS Transfer Family aplicación está conectada a una instancia de cuenta de IAM Identity Center.
 - Si ya tiene una instancia de cuenta y es miembro de una instancia de organización, tiene la opción de elegir la instancia a la que desea conectarse.
 - Si aún no tienes una instancia de cuenta o eres miembro de una instancia de organización, se te presentan las opciones para crear una instancia de cuenta.
4. En el tipo de punto de conexión, seleccione el tipo de punto de conexión de acceso público. Para ver un punto de conexión alojado en una VPC, consulte [Creación de una aplicación web de Transfer Family en una VPC](#).
 5. En el panel de tipos de permisos, puedes usar un rol creado anteriormente o hacer que el servicio cree uno por ti.
 - Si ya ha creado un rol portador de identidad, elija Usar un rol existente y elija el suyo en el menú Seleccione un rol existente.
 - Para que el servicio cree un rol para usted, elija Crear y usar un nuevo rol de servicio.
 6. En el panel de unidades de aplicaciones web, elija un valor. Una unidad de aplicación web permite la actividad de la aplicación web desde hasta 250 sesiones únicas. Al crear una aplicación web, aprovisiona el número de unidades que necesita en función de los volúmenes máximos de carga de trabajo esperados. Cambiar las unidades de la aplicación web repercute en la facturación. Para obtener más información acerca de los precios, consulte [AWS Transfer Family Precios](#).
 7. Si utiliza Transfer Family en un dispositivo AWS GovCloud (US) Region, puede seleccionar la casilla de verificación del punto final con FIPS activado en el panel FIPS activado. Para todas las demás Regiones de AWS, esta opción no está disponible.

8. (Opcional) Agregue una etiqueta que le ayude a organizar sus aplicaciones web. Le sugerimos que añada una etiqueta con Nombre como clave y un nombre descriptivo como valor.
9. Elija Siguiente. En esta pantalla, si lo desea, puede proporcionar un título para su aplicación web. Si no proporciona un título, se proporciona el título predeterminado de Transfer Web App. También puedes cargar archivos de imagen para tu logotipo y favicon.
10. Selecciona Siguiente y, a continuación, selecciona Crear aplicación web.



Note

Asegúrese de configurar una política de uso compartido de Cross-origin recursos (CORS) para todos los depósitos a los que se accede desde el punto final de la aplicación web.

Direccionamiento IP

Las aplicaciones web Transfer Family utilizan puntos finales de doble pila y admiten conectividad IPv4 e IPv6. Para la autenticación, las aplicaciones web utilizan puntos de conexión de AWS IAM Identity Center doble pila, que también admiten IPv6.

Si su cuenta tenía aplicaciones web en una región cuando se lanzó la compatibilidad con terminales de IAM Identity Center de doble pila, todas las aplicaciones web de esa cuenta y región seguirán utilizando el punto de conexión del IPv4-only IAM Identity Center para garantizar la compatibilidad con versiones anteriores. Esto se aplica tanto a las aplicaciones web existentes como a las recién creadas. Las cuentas que no tenían aplicaciones web en el momento del lanzamiento utilizan el terminal de doble pila de IAM Identity Center. Si necesita cambiar el punto final del IAM Identity Center que utiliza su aplicación web, póngase en contacto con AWS Support.

Note

Para determinar qué terminal utiliza su aplicación web, inspeccione la URL cuando se le redirija a la página de inicio de sesión del IAM Identity Center:

- IPv4-only: [Region].signin.aws.amazon.com
- Dual-stack: [Region].sso.signin.aws

Si su organización utiliza firewalls o puertas de enlace de red, incluya en una lista los terminales IPv4 existentes y los nuevos terminales de doble pila del IAM Identity Center para garantizar un acceso ininterrumpido independientemente del terminal que utilicen sus aplicaciones web. Para ver la lista completa de dominios y puntos de enlace URL que se pueden incluir en la lista, consulte [Actualizar los firewalls y las puertas de enlace para permitir el acceso al portal de acceso](#) en la Guía del usuario del IAM Identity Center. AWS

Creación de una aplicación web de Transfer Family en una VPC

En esta sección se describen los procedimientos para crear una aplicación web Transfer Family en una VPC. Puede alojar el punto final de su aplicación web en una nube privada virtual (VPC) para utilizarla para transferir datos hacia y desde un bucket de Amazon S3 sin tener que recurrir a la Internet pública. Para asignar usuarios y grupos que puedan usar su aplicación web, consulte [Asigne o añada usuarios o grupos a una aplicación web Transfer Family](#).

Note

Para garantizar un flujo de datos privado de principio a fin al utilizar un punto final de VPC de una aplicación web Transfer Family, debe implementar tres componentes adicionales. En primer lugar, configure un PrivateLink punto de conexión para las operaciones de la

API de control de Amazon S3, que es necesario para las llamadas a la API Amazon S3 Access Grants. En segundo lugar, configure un punto de enlace para el acceso a los datos de PrivateLink Amazon S3 mediante un punto de enlace de Amazon S3 Gateway (para el tráfico desde su VPC) o un punto de enlace de la interfaz de Amazon S3 (para el tráfico de redes locales a través de VPN o Direct Connect). En tercer lugar, bloquee el acceso al bucket de Amazon S3 actualizando las políticas del bucket para permitir únicamente el tráfico desde estos puntos de enlace de VPC. Esta combinación garantiza que todas las transferencias de datos permanezcan dentro de su infraestructura de red privada y nunca pasen por la Internet pública.

Crea una aplicación web de Transfer Family

Requisitos previos

- AWS IAM Identity Center configurarla con el proveedor de identidad configurado. Consulte [Configura tu proveedor de identidad para las aplicaciones web Transfer Family](#).
- Configuración de componentes de red y VPC. Consulte [Crear una VPC](#).
- Punto final de API configurado para las operaciones de control de Amazon S3. Consulte [Acceder a los puntos de enlace de la interfaz de Amazon S3](#).
- Configuración de puntos de enlace de VPC para Amazon S3 (puerta de enlace o interfaz). Consulte [Tipos de puntos de enlace de VPC para Amazon S3](#). Si utiliza un punto final de interfaz, debe habilitar el DNS privado. Para ver un ejemplo, consulte [Introducción al soporte de DNS privado para Amazon S3 con AWS PrivateLink](#).

Note

AWS IAM Identity Center no admite puntos finales de VPC; todas las solicitudes de autenticación transitan por la Internet pública. Además, las aplicaciones web de Transfer Family requieren acceso a Internet para cargar contenido estático (como JavaScript archivos CSS y HTML). Los requisitos para el acceso público a Internet son independientes del acceso a los datos. Su punto de enlace de VPC garantiza que las conexiones se enruten a través de su infraestructura de VPC.

Para crear una aplicación web Transfer Family

1. Inicia sesión en Consola de administración de AWS y abre la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, selecciona Aplicaciones web.
3. Seleccione Crear aplicación web. Para el acceso de autenticación, el panel se rellena de la siguiente manera.
 - Si ya ha creado una organización o una instancia de cuenta en AWS IAM Identity Center, verá este mensaje: Su AWS Transfer Family aplicación está conectada a una instancia de cuenta de IAM Identity Center.
 - Si ya tiene una instancia de cuenta y es miembro de una instancia de organización, tiene la opción de elegir la instancia a la que desea conectarse.
 - Si aún no tienes una instancia de cuenta o eres miembro de una instancia de organización, se te presentan las opciones para crear una instancia de cuenta.
4. En la sección de configuración de Endpoint, elige cómo accederán los usuarios a tu aplicación web:
 - Accesible públicamente: se puede acceder al punto final de su aplicación web de forma pública a través de HTTPS. Esta opción no requiere ninguna configuración de VPC, por lo que es fácil de configurar y adecuada para aplicaciones destinadas a un uso público amplio.
 - Alojado en VPC: el punto final de su aplicación web está alojado en su Nube Privada Virtual (VPC), lo que proporciona acceso a la red privada a través de su red de VPC o conexiones de VPN. AWS Direct Connect Esta opción ofrece una seguridad mejorada mediante el aislamiento de la red y se recomienda para aplicaciones internas.

Al configurar un punto de conexión alojado en una VPC, tendrás que especificar:

- VPC: seleccione una VPC existente o cree una nueva. Hay disponible el botón Crear una VPC.
- Zonas de disponibilidad: elija las zonas de disponibilidad en las que se implementará su punto final.
- Subredes: seleccione subredes dentro de cada zona de disponibilidad elegida.
- Grupos de seguridad: seleccione o cree grupos de seguridad para controlar el acceso en función de las direcciones IP de origen. Si no se especifica, se utiliza el grupo de seguridad predeterminado de la VPC. Administre los grupos de seguridad a través de la consola de VPC. Configure sus grupos de seguridad de VPC para permitir el tráfico entrante de su red

a través de HTTPS en el puerto TCP 443. Esto es necesario para la autenticación del IAM Identity Center y para cargar el contenido estático de las aplicaciones web.

 Note

El punto de acceso no se puede personalizar para los puntos de enlace de VPC. Para añadir una URL personalizada, usa el punto de conexión público.

Post-creation pasos

- Asegúrese de configurar una política de uso compartido de Cross-origin recursos (CORS) para todos los depósitos a los que se accede desde el punto final de la aplicación web. Consulte [Cross-origin política de uso compartido de recursos \(CORS\)](#).
- Actualice su política de bucket para permitir que el tráfico que se origine únicamente en su VPC pase por su punto de enlace de VPC. Consulte [Restricción del acceso a un punto de conexión de la VPC específico](#).
- Asigne o añada usuarios o grupos a la aplicación web Transfer Family. Consulte [Asigne o añada usuarios o grupos a una aplicación web Transfer Family](#).

Cross-origin política de uso compartido de recursos (CORS)

Debe configurar el intercambio de recursos entre orígenes (CORS) para todos los depósitos que utilice su aplicación web. Para obtener más información acerca de CORS, consulte [Configure el uso compartido de Cross-origin recursos \(CORS\) para su depósito](#).

 Important

Antes de usar la siguiente política de ejemplo, reemplaza el origen permitido por tu punto de acceso. De lo contrario, los usuarios finales recibirán un error cuando intenten acceder a una ubicación de su aplicación web.

Ejemplo de política:

```
[  
  {
```

```
"AllowedHeaders": [
  "*"
],
"AllowedMethods": [
  "GET",
  "PUT",
  "POST",
  "DELETE",
  "HEAD"
],
"AllowedOrigins": [
  "https://vpce-1234567-example.vpce-mq.transfer-webapp.us-east-1.on.aws"
],
"ExposeHeaders": [
  "last-modified",
  "content-length",
  "etag",
  "x-amz-version-id",
  "content-type",
  "x-amz-request-id",
  "x-amz-id-2",
  "date",
  "x-amz-cf-id",
  "x-amz-storage-class",
  "access-control-expose-headers"
],
"MaxAgeSeconds": 3000
}
]
```

Restricción del acceso a un punto de conexión de la VPC específico

El siguiente es un ejemplo de una política de bucket de Amazon S3 que restringe el acceso a un bucket específico, `amzn-s3-demo-bucket`, solo desde el punto de conexión de la VPC con el ID `vpce-1a2b3c4d`. Si el punto de conexión específico no se usa, la política deniega todo el acceso al bucket. La condición `aws:SourceVpce` especifica el punto de conexión. La condición `aws:SourceVpce` no requiere un ARN para el recurso de punto de enlace de la VPC, solo el ID de la VPC. Para obtener más información sobre cómo actualizar su política de bucket para permitir únicamente el tráfico que se origina en su VPC, consulte [Controlar el acceso desde los puntos de enlace de la VPC](#) con políticas de bucket. Para obtener más información sobre el uso de condiciones

en una política, consulta los [ejemplos de políticas de buckets que utilizan claves](#) de condición. Como requisito previo para aplicar esta política, debe crear un punto de enlace de [VPC de Amazon S3](#).

Important

Antes de utilizar la política de ejemplo siguiente, reemplace el ID del punto de conexión de la VPC por un valor adecuado para su caso de uso. De lo contrario, no podrá acceder a su bucket.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Asigne o añada usuarios o grupos a una aplicación web Transfer Family

Después de crear una aplicación web Transfer Family, puede asignar usuarios y grupos que, a su vez, podrán acceder a la aplicación web. Puede recuperar los usuarios que ya estén creados y almacenados en el Centro de identidad de IAM o puede [añadir nuevos usuarios directamente](#) (si utiliza un directorio del Centro de identidades de IAM como proveedor de identidad). Si añade nuevos usuarios, también se añadirán a su instancia del Centro de identidades de IAM.

Tenga en cuenta lo siguiente:

- Solo puede añadir nuevos usuarios si utiliza el directorio del Centro de Identidad de IAM como fuente de identidad y si tiene los permisos adecuados. Si es miembro de una instancia de la organización, es posible que no tenga los permisos necesarios para añadir usuarios.

 Note

Si no asignas usuarios o grupos a tu aplicación, los usuarios recibirán un mensaje de error cuando intenten iniciar sesión en la aplicación web.

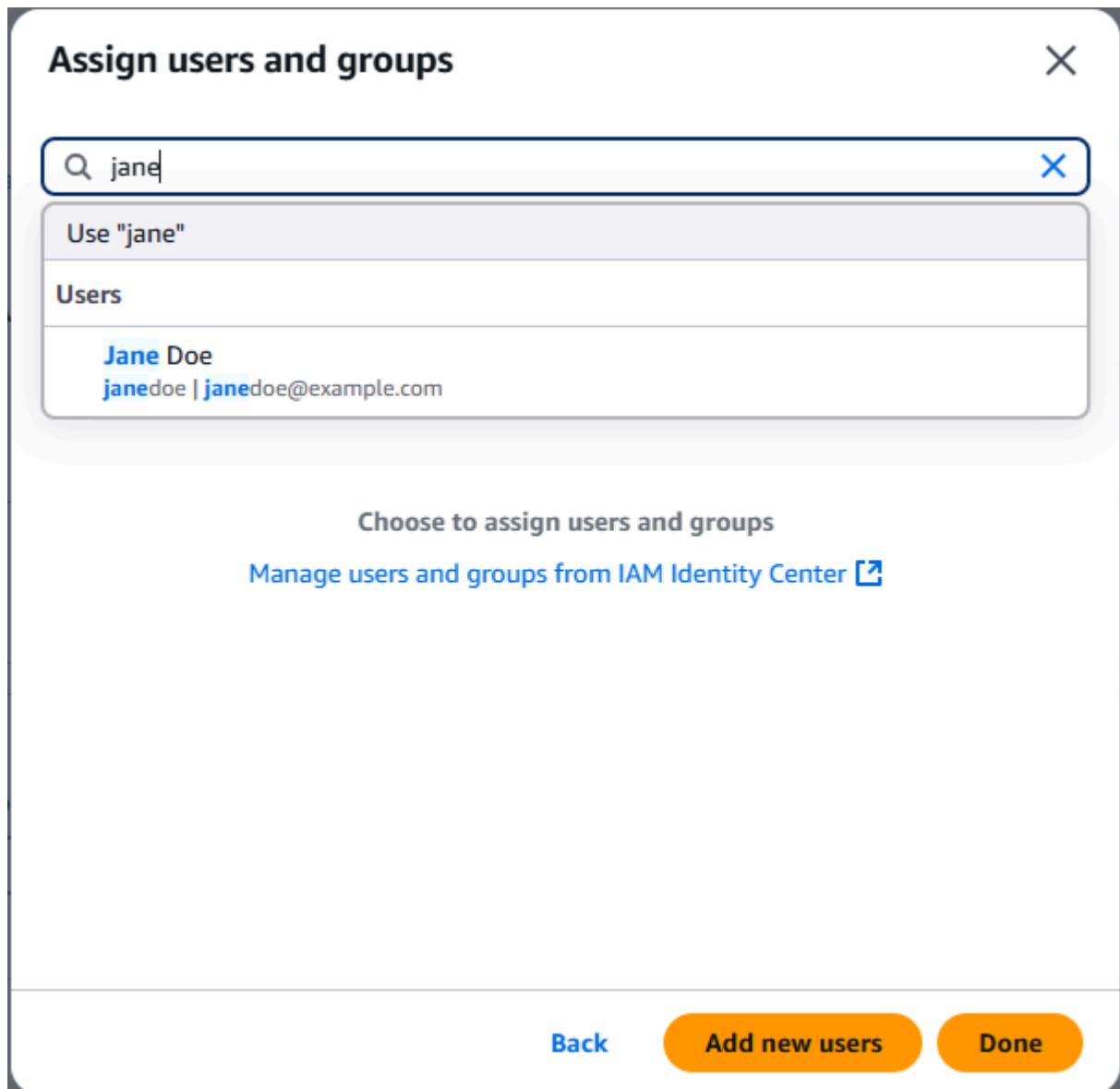
- Si crea un usuario nuevo, también debe crear una concesión de acceso a S3 para que este usuario pueda acceder a los datos de su aplicación web.
- Tras crear un nuevo usuario, ese usuario recibe un correo electrónico de incorporación del Centro de Identidad de IAM con instrucciones sobre cómo proceder.

Para asignar usuarios a una aplicación web Transfer Family

1. Ve a tu lista de aplicaciones web y elige la que quieras editar.
2. Elija Asignar usuarios y grupos.

The screenshot shows the AWS IAM console interface for a web application named 'webapp-'. At the top, there are buttons for 'Assign users and groups' (orange), 'Clear customization', and 'Delete'. Below this is the 'Web app details' section, which includes an 'Access endpoint' (a URL ending in '.transfer-webapp.us-east-2.on.aws'), a 'Web app endpoint' (a URL ending in '-webapp.us-east-2.on.aws'), and 'Web app units' (1). To the right, the 'Identity provider' is 'AWS IAM Identity Center', the 'IAM role' is a role with a policy, and the 'Instance ARN' is 'arn:aws:sso::instance/ssoins-'. Below the details is a tabbed interface with 'Users' selected. The 'Users (2)' section shows a search bar and a table with two columns: 'Display name' and 'User ID'. The table lists two users, each with a checkbox, a display name, a user ID, and a username.

3. Para asignar los usuarios que haya creado anteriormente en el Centro de identidades de IAM, seleccione Asignar usuarios y grupos existentes. Para crear nuevos usuarios, vaya al paso 4.
 - a. Aparece una pantalla de información. Seleccione Comenzar para continuar.
 - b. Busca al usuario. Tenga en cuenta que no aparece ningún usuario hasta que comience a introducir sus criterios de búsqueda. Debe buscar por el nombre que se muestra, no por el nombre de usuario, si es diferente. Solo se muestran las coincidencias exactas. Si no encuentra a su usuario, vaya a la consola de administración del IAM Identity Center, busque al usuario y, a continuación, copie y pegue aquí su nombre para mostrar.



- c. Elija los usuarios y grupos que desee añadir y, a continuación, seleccione Asignar.
4. Para crear un usuario nuevo, selecciona Agregar y asignar nuevos usuarios.
 - a. Aparece una pantalla de información. Selecciona Comenzar para continuar.
 - b. Elija Agregar usuarios nuevos.
 - c. Introduzca los siguientes detalles de usuario en el cuadro de diálogo: nombre de usuario, nombre y apellidos y una dirección de correo electrónico.

Add new users [X]

Information: Newly-created users are enabled by default. To grant them access to Add User Widget, you must set their password in the IAM Identity Center console. [Manage user passwords in the IAM Identity Center console](#) [X]

Username
A username is required for this person to sign in to the AWS access portal. You can't change the username later.

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: +,=,.,@,-,_

First name **Last name**

Email address **Confirm email address**

Display name
This is typically the full name of the user (first and last name) and appears in the users list.

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

- d. Seleccione Siguiente y, a continuación, seleccione Añadir para añadir el usuario y cerrar el cuadro de diálogo o Añadir nuevo usuario para crear otro usuario.

Configure el uso compartido de Cross-origin recursos (CORS) para su depósito

Debe configurar el intercambio de recursos entre orígenes (CORS) para todos los depósitos que utilice su aplicación web. Una configuración de CORS es un documento que define las reglas que identifican los orígenes a los que permitirá acceder a su depósito. Para obtener más información sobre CORS, consulte [Configuración del uso compartido de recursos entre orígenes \(CORS\)](#).

 Important

Si no configura CORS, los usuarios finales recibirán un error cuando intenten acceder a una ubicación de su aplicación web.

Para configurar el uso compartido Cross-origin de recursos (CORS) para su bucket de Amazon S3

1. Inicie sesión en la consola de Amazon S3 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/s3/>.
2. Selecciona Buckets en el panel de navegación izquierdo y busca tu bucket en el cuadro de diálogo de búsqueda y, a continuación, selecciona la pestaña Permisos.
3. En el uso compartido de Cross-origin recursos (CORS), selecciona Editar y pega el siguiente código. *WebAppEndpoint* Sustitúyalo por el punto de acceso real de tu aplicación web. Puede ser el punto final de acceso público o alojado en la VPC que se crea al crear la aplicación web, o un punto final de acceso personalizado, si usted crea uno. Asegúrese de no introducir barras diagonales finales, ya que al hacerlo se producen errores cuando los usuarios intentan iniciar sesión en su aplicación web.
 - Ejemplo incorrecto: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Ejemplos correctos:
 - `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`
 - `https://vpce-05668789767a-fh45z079.vpce-mq.transfer-webapp.us-east-1.on.aws`

Si va a reutilizar un depósito para varias aplicaciones web, añada sus puntos finales a la lista. AllowedOrigins

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
```

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

4. Seleccione Guardar cambios para actualizar el CORS.

Para probar la configuración del CORS, consulte [Probar](#) el CORS.

Configuración de las concesiones de acceso a Amazon S3 para las aplicaciones web Transfer Family

En este tema se describe cómo añadir una concesión de acceso mediante Amazon S3 Access Grants. Esta concesión de acceso define el acceso a sus datos directamente a los usuarios y grupos de su directorio corporativo y proporciona credenciales temporales puntuales y con menos privilegios en función de las concesiones. Una concesión individual en una instancia de S3 Access Grants permite a un usuario o grupo específico de un directorio corporativo acceder desde una ubicación que esté registrada en su instancia de S3 Access Grants. Para obtener más información, consulte los [conceptos de S3 Access Grants](#) en la Guía del usuario de Amazon S3.

 Note

No puede usar el directorio del Centro de Identidad de IAM con S3 Access Grants excepto con las aplicaciones web Transfer Family.

Debe especificar una concesión de acceso a Amazon S3 para la propagación de la identidad. Una concesión de acceso a Amazon S3 almacena los datos a los que deben acceder los usuarios finales. Cuando los usuarios finales inician sesión en la aplicación web Transfer Family, S3 Access Grants transfiere la identidad del usuario a la aplicación de confianza. En esta sección se describe cómo añadir y configurar una instancia de concesión de acceso a Amazon S3 y, a continuación, una concesión de acceso para un bucket de Amazon S3.

 Note

Tenga preparados el [ARN de su instancia del IAM Identity Center](#) y su ID de usuario o grupo, ya que los necesitará para completar la configuración de su concesión de acceso.

Para crear una subvención con Amazon S3 Access Grants

1. Inicie sesión en la consola de Amazon S3 Consola de administración de AWS y ábrala en <https://console.aws.amazon.com/s3/>.
2. Cree un depósito o anote uno existente para usarlo con su aplicación web. Para obtener información sobre la creación de buckets, consulte la [Guía del usuario de Amazon S3](#).
3. En el panel de navegación izquierdo, elija Access Grants.
4. Elija Crear instancia de S3 Access Grants y proporcione la siguiente información.
 - Seleccione Añadir instancia de IAM Identity Center en el *your-Region* lugar donde *your-Region* se encuentra la suya Región de AWS. Mantenga esta casilla desactivada si no utiliza el Centro de identidad de IAM como proveedor de identidad.
 - Pegue el ARN de la instancia de IAM Identity Center.

[Amazon S3](#) > [Access Grants](#) > Set up Access Grants Instance

- Step 1
☒ **Create S3 Access Grants instance**
- Step 2
☐ Register S3 Buckets or prefixes as locations
- Step 3
☐ Create grant
- Step 4
☐ Review and finish

Create S3 Access Grants instance [Info](#)

When you create your S3 Access Grants instance, you can use identities from your corporate directory or you can use IAM users and roles. This Access Grants instance serves as the container for your individual grants.

S3 Access Grants instance [Info](#)

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

☒ Add IAM Identity Center instance in US East (Ohio) us-east-2 - *optional*

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

IAM Identity Center instance ARN

You can find the IAM Identity Center instance ARN in the [IAM Identity Center console](#).

arn:aws:sso::instance/ssoin-

Format: arn:aws:sso::instance/<instanceidentifier>

Elija Siguiente para continuar.

- Registre los buckets o prefijos de S3 como ubicaciones. Le recomendamos que registre la ubicación predeterminada y la asigne a un rol de IAM. `s3://` La ubicación en esta ruta predeterminada cubre el acceso a todos los buckets de Amazon S3 Región de AWS de su cuenta. Al crear una concesión de acceso, puede limitar el ámbito a un depósito, un prefijo o un objeto dentro de la ubicación predeterminada.

Proporcione la siguiente información.

- Para el ámbito, busca un depósito o introduce el nombre del mismo y, si lo prefieres, un prefijo.
- Para el rol de IAM, elija Crear nuevo rol para que el servicio cree un rol.

Como alternativa, puede crear el rol usted mismo, tal y como se describe en [Configurar las funciones de IAM para las aplicaciones web Transfer Family](#), y luego introducir su ARN aquí.

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

Register location [Info](#)

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

Location [Info](#)

Location scope [Info](#)

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

Scope

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

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

Permissions

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

Permissions

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

IAM role [Info](#)

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

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

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

Elija Siguiente para continuar.

- En la pantalla Crear subvención, proporcione los siguientes detalles.
 - Para los permisos, selecciona Leer y escribir. Los permisos de concesión de acceso pueden ser de solo lectura o de lectura y escritura, pero no se admite el permiso de solo escritura.
 - Para el tipo de concesionario, elija la identidad del directorio en el Centro de identidades de IAM.
 - En el tipo de identidad del directorio, seleccione Usuario o Grupo, según el tipo que desee registrar ahora.
 - En el user/group ID del centro de identidad de IAM, pegue el ID de su usuario o grupo. Este ID está disponible en la consola del IAM Identity Center y en la aplicación web Transfer Family, en la tabla de usuarios y grupos.

Create Grant [Info](#)**Grant** [Info](#)

Grant a user or role a specific level of access to your S3 data.

Grant scope

The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location

s3://test

Location ID [Info](#)**IAM role** [Info](#)

[web-app-access-grants](#)

[Browse locations](#)

[Register location](#)

Subprefix - optional [Info](#)

Further scope the grant to a bucket, prefix, or an individual object.

*

Don't include any part of the grant already specified in the location.

Format for bucket: <bucket>/*

Format for prefix: <bucket>/<prefix-with-path>*

Format for object: <bucket>/<prefix-with-path>/<object>

Grant scope [Info](#)

s3://test/*

☐ The grant scope is an object

Permissions and access

Grant a user or role a specific level of access to your S3 data.

 The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions

☒ Read

☒ Write

Grantee type [Info](#)

☒ Directory identity from IAM Identity Center

☐ IAM principal

Directory identity type [Info](#)

☒ User

☐ Group

IAM Identity Center user ID [Info](#)

The user that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#)

Format: a1b2c3d4-5678-90ab-cdef-EXAMPLE1111

► **Application - optional**

Elija Siguiente.

7. Revise la configuración de la pantalla. Si todo es correcto, selecciona Finalizar para crear la concesión de acceso. Como alternativa, puede elegir Cancelar o Anterior para realizar cambios.

- Step 1
- Create S3 Access Grants instance
- Step 2
- Register S3 Buckets or prefixes as locations
- Step 3
- Create grant
- Step 4
- Review and finish

Review and finish

Step 1 - Create S3 Access Grants instance

S3 Access Grants instance

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

arn:aws:sso:::application/ssoinstance:/apl

Successfully created S3 Access Grants instance

Instance ARN: arn:aws:s3:us-east-2:::access-grants/default

You can grant other accounts access to this S3 Access Grants instance in the Resource Access Management console

Step 2 - Register S3 buckets or prefixes as locations

Location

Location scope

s3://

IAM role

web-app-beta-access-grants

Successfully registered location

Location ID:

Step 3 - Create grants

Grant

Grant a user or role a specific level of access to your S3 data.

Grant scope

s3:///*

IAM role

web-app-beta-access-grants

Location ID

Permissions and access

Access Type

READWRITE

Grantee type

Directory identity user

Grantee ID

Application - optional

-

Successfully created grant

Grant ARN: arn:aws:s3:us-east-2:::access-grants/default/grant/

Create another grant

Cancel

Previous

Finish

Amazon S3 > Access Grants > US East (Ohio) us-east-2: default

US East (Ohio) us-east-2: default

Share InstanceDelete Instance

S3 Access Grants provides scalable access control to data sets in your S3 buckets. To share an S3 Access Grants instance with external accounts by using the AWS Resource Access Manager console, choose Share instance. With S3 Access Grants, you can use identities from your corporate directory or from AWS Identity and Access Management (IAM) to control access. You can create one S3 Access Grants instance per AWS Region per account.

S3 Access Grants instance overview

Amazon Resource Name (ARN)
arn:aws:s3:us-east-2:access-grants/default

Creation date
October 25, 2024, 11:50:11 (UTC-04:00)

Account ID

IAM Identity Center

DeregisterAdd

IAM Identity Center instance ARN
arn:aws:sso:application/ssoins/apl

GrantsLocations

Grants (1)

Find by grant scope or grantee

DeleteCreate Grant

< 1 > ⚙

Grant scope	Grant ID	Permission	Grantee type	Grantee ID	Creation date	Location ID	Application ARN
s3:///*		Read, Write	Directory identity user		October 25, 2024, 11:57:30 (UTC-04:00)		ALL

Esto completa la configuración de la aplicación web. Los usuarios y grupos que haya configurado pueden visitar la aplicación web en el punto de acceso, iniciar sesión y cargar y descargar archivos.

Actualice su terminal de acceso con una URL personalizada

El punto de acceso predeterminado que se crea con tu aplicación web contiene identificadores generados por el servicio. Para ofrecer una experiencia de marca, es posible que desees proporcionar una URL personalizada para que tus usuarios accedan a tu aplicación web Transfer Family. En este tema se describe cómo actualizar tu terminal de acceso con una URL personalizada.

Note

El punto de acceso no se puede personalizar para los puntos de enlace de VPC. Para añadir una URL personalizada, usa el punto de conexión público.

Note

El siguiente procedimiento se basa en el uso de la [plantilla de CloudFormation pila](#) recomendada. No necesita usar la plantilla: puede crear la distribución directamente desde la [CloudFront consola](#).

Usa una URL personalizada

320

Sin embargo, la plantilla proporcionada simplifica el proceso y evita errores de configuración. Si no utilizas la CloudFormation plantilla, asegúrate de seguir estas pautas:

- La [política de solicitudes de Origin](#) debe reenviar las cadenas de consulta y las cookies al origen y no debe reenviar el Host encabezado al origen.
- La [política de caché](#) no debe incluir el Host encabezado en la clave de caché.

Para personalizar la URL de su aplicación web

1. Cree una CloudFront distribución mediante la AWS CloudFormation plantilla proporcionada por Transfer Family, la [plantilla de CloudFormation pila](#).
 - a. Abra la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
 - b. Elija Crear pila y especifique lo siguiente.
 - En la sección Requisitos previos: preparar una plantilla, elija Elegir una plantilla existente.
 - En la sección Especificar plantilla, elija Cargar un archivo de plantilla.
 - Guarde el archivo [de plantilla de CloudFormation pila](#) y cárguelo aquí.
 - c. Selecciona Siguiente y proporciona la siguiente información.
 - WebAppEndpoint: copie el valor de su aplicación web
 - AccessEndpoint: proporcione el nombre de dominio personalizado que quieres usar
 - AcmCertificateArn: proporcione el ARN de un SSL/TLS certificado público o privado que esté almacenado en AWS Certificate Manager
 - d. Complete el CloudFormation asistente hasta que se cree la nueva pila.
2. En su aplicación web, edite el punto final de acceso y actualice la URL personalizada por la URL que desee usar.

Transfer Family > Web apps > webapp- > Edit web app details

Edit web app details

Authentication access [Info](#)

Connect or create an Identity Center instance

Instance ARN

Select your instance ARN

Permission type [Info](#)

Create and use a new service role

Create and use an IAM role to allow the service to access the AWS resource it needs to create your application

Use an existing role

Use an existing IAM role to allow the service to access the AWS resources it needs to create your application

By selecting use existing role, you need to manually create an IAM Role in order for the Transfer Family web application to access your AWS services data. Please select an existing IAM role below or [create a new role in IAM console](#)

Select an existing role

If your newly created role is not showing up in the dropdown list, please try the refresh button on the right

Find your IAM role

Make sure you have attached the trust policy and permission policy to the role you selected.

[learn more about required policies](#)

Access endpoint [Info](#)

Map your own fully qualified domain name to this web app so your end users can use your custom URL, not the service-provided URL to access your web app. Note- you can only complete this step in CloudFront after you have created the web app.

Custom URL

`https://my-custom-url`

[Create a new distribution](#)

3. Crea registros de DNS para dirigir el tráfico de tu nombre de dominio personalizado a la CloudFront distribución. Si usa Route 53 para la zona, puede crear un registro de alias o CNAME para el nombre de la CloudFront distribución (por ejemplo, xxxx.cloudfront.net). Para obtener información sobre el uso de Amazon Route 53 con CloudFront, consulte [Configuración de Amazon Route 53 para enrutar el tráfico a una CloudFront distribución](#).
4. Actualice su política de intercambio de recursos entre orígenes sustituyendo el punto de acceso predeterminado por la siguiente línea en el bloque de AllowedOrigins códigos:

```
"https://custom-url"
```

Debes realizar este cambio para cada segmento que utilice tu aplicación web.

Tras realizar la actualización, la AllowedOrigins sección de la política CORS debería tener el siguiente aspecto:

```
"AllowedOrigins": [
  "https://custom-url",
```

Solo necesitas una AllowedOrigins entrada para cada aplicación web de Transfer Family.

Consulte el procedimiento [Configurar el uso compartido de Cross-origin recursos \(CORS\) para su bucket de Amazon S3](#) para obtener más información.

Ahora puede visitar su punto de acceso personalizado y compartir este enlace con sus usuarios finales.

CloudTrail registro para aplicaciones web Transfer Family

CloudTrail es un Servicio de AWS que crea un registro de las acciones tomadas dentro de su Cuenta de AWS. Supervisa y registra continuamente las operaciones de la API para actividades como los inicios de sesión en la consola, AWS Command Line Interface los comandos y SDK/API las operaciones. Esto te permite llevar un registro de quién realizó qué acción, cuándo y desde dónde. CloudTrail contribuye a la auditoría, la gestión del acceso y el cumplimiento de las normas, ya que proporciona un historial de todas las actividades de su AWS entorno.

En el caso de las aplicaciones web Transfer Family, puede realizar un seguimiento tanto de los eventos de autenticación como de las operaciones de acceso a los datos realizadas por sus usuarios. Para habilitar un registro completo, debes:

1. Configure CloudTrail para registrar los eventos de administración a fin de realizar un seguimiento de las actividades de autenticación.
2. Habilite los eventos de datos de Amazon S3 para realizar un seguimiento de las operaciones de archivos realizadas a través de su aplicación web.

Véase también

- [CloudTrail casos de uso del IAM Identity Center](#)
- [Descripción de los eventos de inicio de sesión en el Centro de Identidad de IAM](#)
- [CloudTrail Elemento UserIdentity](#)
- [Habilitar CloudTrail el registro de eventos para cubos y objetos de S3](#)
- [CloudTrailEventos de Amazon S3](#)

Habilitación de eventos de datos de Amazon S3

Para realizar un seguimiento de las operaciones de archivos realizadas a través de las aplicaciones web Transfer Family en sus buckets de Amazon S3, debe habilitar los eventos de datos para esos buckets. Los eventos de datos proporcionan actividad de API a nivel de objeto y son particularmente útiles para rastrear las cargas y descargas de archivos y otras operaciones realizadas por los usuarios de aplicaciones web.

Para habilitar los eventos de datos de Amazon S3 en su aplicación web Transfer Family:

1. Abre la CloudTrail consola en <https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación, elija Rutas y, a continuación, seleccione una ruta existente o cree una nueva.
3. En los selectores de eventos avanzados, selecciona Editar.
4. Selecciona Añadir un selector de eventos avanzado.
5. Para el primer selector de campos:
 - Defina el campo como `eventCategory`
 - Defina el operador como igual
 - Establezca el valor en `Data`
6. Selecciona Añadir campo y, para el segundo selector de campos:
 - Defina el campo como `resources.type`
 - Defina el operador como igual
 - Establezca el valor en `AWS::S3::Object`
7. (Opcional) Para registrar eventos solo para grupos específicos, selecciona Agregar campo y agrega:
 - Defina el campo como `resources.ARN`
 - Defina el operador para que comience con
 - Establezca el valor en `arn:aws:s3:::your-bucket-name/`
8. Selecciona Save changes (Guardar cambios).

Como alternativa, puede usar la configuración de eventos de datos heredada:

1. En Eventos de datos, selecciona Editar.
2. En el tipo de evento de datos, seleccione Eventos de bucket y objeto de S3.

3. Elija los buckets de Amazon S3 para registrar los eventos de datos. Puede seleccionar Todos los depósitos S3 actuales y futuros o especificar depósitos individuales.
4. Elija si desea registrar los eventos de lectura, de escritura o ambos.
5. Seleccione Save changes (Guardar cambios).

Tras habilitar los eventos de datos, puede acceder a estos registros en el bucket de Amazon S3 configurado para CloudTrail. Los registros incluyen detalles como el usuario que realizó la acción, la marca temporal de la acción, el objeto específico afectado y el `onBehalfOf` campo que ayuda a rastrear las acciones realizadas a través `userId` de las aplicaciones web Transfer Family.

Buscar y ver tus registros

Hay varias formas de buscar y ver CloudTrail los registros de la aplicación web Transfer Family:

Uso de la CloudTrail consola

La forma más rápida de ver los eventos recientes:

1. Abre la CloudTrail consola en <https://console.aws.amazon.com/cloudtrail/>.
2. Elija Historial de eventos.
3. Filtrar eventos por:
 - Origen del evento: `signin.amazonaws.com` para eventos de aplicaciones web
 - Origen del evento: `s3.amazonaws.com` para operaciones con archivos
4. Haga clic en cualquier evento para ver información detallada.

Acceso a los registros en Amazon S3

Para acceder a los archivos de registro completos almacenados en Amazon S3:

1. Identifica el bucket de Amazon S3 de tu CloudTrail ruta:

```
aws cloudtrail describe-trails --query 'trailList[*].[Name,S3BucketName]' --output table
```

2. Navegue hasta los archivos de registro en Amazon S3:

```
aws s3 ls s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/
```

3. Descargue y busque archivos de registro para su ID de aplicación web:

```
aws s3 cp s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/ . --recursive
gunzip *.json.gz
grep -l "webapp-1a2b3c4d5e6f7g8h9" *.json
```

Se utiliza AWS CLI para buscar eventos

Busque eventos específicos de aplicaciones web mediante AWS CLI:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "webapp-1a2b3c4d5e6f7g8h9" \
  --start-time $(date -d "1 day ago" +%s)000
```

O busque eventos de autenticación:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "UserAuthentication" \
  --start-time $(date -d "1 day ago" +%s)000
```

Ejemplos de registros de autenticación

CloudTrail registra los eventos de autenticación de las aplicaciones web de Transfer Family, lo que puede ayudarte a realizar un seguimiento de los intentos de inicio de sesión correctos y fallidos. Estos registros son especialmente útiles para la supervisión de la seguridad y el cumplimiento.

Temas

- [Ejemplo de entrada de registro para la verificación de credenciales](#)
- [Ejemplo de entrada de registro para la autenticación de inicio de sesión](#)
- [Ejemplo de entrada de registro para ListCallerAccessGrants](#)
- [Ejemplo de entrada de registro para GetDataAccess un evento](#)

Ejemplo de entrada de registro para la verificación de credenciales

El siguiente ejemplo muestra una entrada de CloudTrail registro para un evento de verificación de credenciales que se produce durante el proceso de autenticación.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "58138a11-87e5-401d-8f0b-7161c9389112"
  },
  "eventTime": "2025-08-08T15:29:30Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.224",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "f304a48b-7b6d-41c8-b136-4f49c91c1f31",
    "CredentialType": "PASSWORD"
  },
  "requestID": "ff936828-4a81-453c-802d-81368b6bca1a",
  "eventID": "70cb7008-493d-42c2-a9eb-38bf168af6a8",
  "readOnly": false,
  "eventType": "AWS ServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
    "CredentialVerification": "Success"
  },
}
```

```
"eventCategory": "Management"
}
```

Este evento proporciona detalles adicionales sobre el paso de verificación de credenciales del proceso de autenticación y muestra el identificador de credencial específico y el identificador del flujo de trabajo de autenticación utilizados.

Ejemplo de entrada de registro para la autenticación de inicio de sesión

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro de un evento de autenticación de usuario correcto durante el inicio de sesión en una aplicación web mediante el IAM Identity Center.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "b41f0a02-1635-4d07-a414-aecf9e14b906"
  },
  "eventTime": "2025-08-07T14:09:07Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.14",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "7a4ef12c-7c4b-4bc3-b5bd-c2469afcc795",
    "LoginTo": "https://example.awsapps.com/start/",
    "CredentialType": "PASSWORD"
  },
}
```

```

    "requestID": "fc91bcf0-ac53-4454-a1a0-fb911eacc095",
    "eventID": "18522007-1e60-4a71-b2b5-150baf504ab3",
    "readOnly": false,
    "eventType": "AWS ServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
      "UserAuthentication": "Success"
    },
    "eventCategory": "Management"
  }

```

En este ejemplo, anote los siguientes campos importantes:

- `eventSource`: Muestra «signin.amazonaws.com», lo que indica que se trata de un evento de autenticación del IAM Identity Center.
- `userIdentity.onBehalfOf`: Contiene el ID de usuario y el ARN del almacén de identidades del usuario de la aplicación web.
- `additionalEventData.LoginTo`: Muestra la URL de la aplicación del Centro de Identidad de IAM a la que se accede.
- `additionalEventData.CredentialType`: Indica el método de autenticación utilizado (CONTRASEÑA).
- `serviceEventDetails`: Muestra el resultado de la autenticación (correcto).

Ejemplo de entrada de registro para ListCallerAccessGrants

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro de un ListCallerAccessGrants evento, que se produce cuando la aplicación web Transfer Family consulta las concesiones de acceso disponibles para un usuario.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:aws-transfer",
    "arn": "arn:aws:sts::123456789012:assumed-role/AWS
TransferWebAppIdentityBearer-us-east-2/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {

```

```

    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROEXAMPLEID",
      "arn": "arn:aws:iam::123456789012:role/service-role/AWS
TransferWebAppIdentityBearer-us-east-2",
      "accountId": "123456789012",
      "userName": "AWS TransferWebAppIdentityBearer-us-east-2"
    },
    "attributes": {
      "creationDate": "2025-08-08T15:29:34Z",
      "mfaAuthenticated": "false"
    }
  },
  "invokedBy": "transfer.amazonaws.com",
  "onBehalfOf": {
    "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
    "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9a670c546e"
  }
},
"eventTime": "2025-08-08T15:29:35Z",
"eventSource": "s3.amazonaws.com",
"eventName": "ListCallerAccessGrants",
"awsRegion": "us-east-2",
"sourceIPAddress": "transfer.amazonaws.com",
"userAgent": "transfer.amazonaws.com",
"requestParameters": {
  "Host": "123456789012.s3-control.dualstack.us-east-2.amazonaws.com",
  "allowedByApplication": "true",
  "maxResults": "100"
},
"responseElements": null,
"additionalEventData": {
  "SignatureVersion": "SigV4",
  "CipherSuite": "TLS_AES_128_GCM_SHA256",
  "bytesTransferredIn": 0,
  "AuthenticationMethod": "AuthHeader",
  "x-amz-id-2": "1g34AaAELn/
fntxwriFVsr41VDl8dp5ygWFasHJFNVq5FDCWYfX0ye7s4tWHEJC8ppI5lLePYLIcw3iTXAgn5Q==",
  "bytesTransferredOut": 462
},
"requestID": "48485MTZEDWT0ANT",
"eventID": "3de5dd60-b7cf-474c-a1ab-631467c1a5c3",
"readOnly": true,

```

```
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS:S3::AccessGrantsInstance",
    "ARN": "arn:aws:s3:us-east-2:123456789012:access-grants/default"
  }
],
"eventType": "AWS ApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}
```

En este ejemplo, anote los siguientes campos importantes:

- `eventName`: Muestra que se trata de un `ListCallerAccessGrants` evento que consulta las concesiones de acceso a S3 disponibles.
- `requestParameters.allowedByApplication`: Indica que la consulta se filtra para incluir las concesiones permitidas por la aplicación.
- `requestParameters.maxResults`: Muestra el número máximo de concesiones que se pueden devolver en la respuesta.
- `userIdentity.onBehalfOf`: vincula la solicitud al usuario específico de la aplicación web.

Este evento ayuda a rastrear cuándo la aplicación web Transfer Family consulta a qué recursos de S3 tiene acceso un usuario, lo que proporciona visibilidad de las operaciones de descubrimiento de las concesiones de acceso.

Ejemplo de entrada de registro para GetDataAccess un evento

El siguiente ejemplo muestra una entrada de CloudTrail registro de un `GetDataAccess` evento, que se produce cuando la aplicación web Transfer Family solicita permisos de acceso a los recursos de S3 en nombre de un usuario.

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AR0ASEQRAEABP7ADWEZA5:aws-transfer",
    "arn": "arn:aws:sts::123456789012:assumed-role/AWSTransferWebAppIdentityBearer-
ap-southeast-1/aws-transfer",

```

```

    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROASEQRAEABP7ADWEZA5",
        "arn": "arn:aws:iam::123456789012:role/service-role/
AWSTransferWebAppIdentityBearer-ap-southeast-1",
        "accountId": "123456789012",
        "userName": "AWSTransferWebAppIdentityBearer-ap-southeast-1"
      },
      "attributes": {
        "creationDate": "2025-05-08T16:09:05Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "transfer.amazonaws.com",
    "onBehalfOf": {
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9667b0da7a",
      "userId": "191a35ec-10a1-70c1-e4ab-e2802411e13e"
    }
  },
  "eventTime": "2025-05-08T16:10:25Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetDataAccess",
  "awsRegion": "ap-southeast-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "Host": "123456789012.s3-control.dualstack.ap-southeast-1.amazonaws.com",
    "durationSeconds": 900,
    "permission": "READWRITE",
    "target": "s3://amzn-s3-demo-bucket/users/john.doe/documents/*"
  },
  "responseElements": null,
  "additionalEventData": {
    "AuthenticationMethod": "AuthHeader",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "SignatureVersion": "SigV4",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2244,
    "x-amz-id-2": "8ce8sZ0gNwsaj9w1mzagyA
+cs0NjYl8FgEw4FGpE8DARi90aNC0RFWlTYNEN7ChqE9RCJrTzMvS+ru7Vz2xXHrkQt/1uQ9exZTZdlhX+/fm="

```



```
    },
    "requestID": "BXGSKKQXCWS5RAHB",
    "eventID": "c11db1d1-dfb8-431e-8625-48eba2ebadfe",
    "readOnly": true,
    "resources": [
      {
        "type": "AWS:S3::AccessGrantsInstance",
        "ARN": "arn:aws:s3:ap-southeast-1:123456789012:access-grants/default",
        "accountId": "123456789012"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
  }
}
```

En este ejemplo, anote los siguientes campos importantes:

- `eventName`: Muestra que se trata de un `GetDataAccess` evento que se produce cuando Transfer Family solicita permisos de acceso para los recursos de S3.
- `userIdentity.onBehalfOf`: contiene el ARN y el ID de usuario del almacén de identidades, lo que vincula la solicitud de acceso al usuario específico de la aplicación web.
- `requestParameters.target`: Muestra el patrón de ruta S3 para el que se solicitó el acceso.
- `requestParameters.permission`: Indica el tipo de acceso solicitado (READWRITE, READ o WRITE).
- `requestParameters.durationSeconds`: Muestra durante cuánto tiempo es válida la concesión de acceso (normalmente 900 seconds/15 minutos).
- `sourceIPAddress` y `userAgent`: ambos muestran «transfer.amazonaws.com», lo que indica que se trata de una solicitud de servicio interna.

GetDataAccess los eventos son particularmente útiles para rastrear cuándo los usuarios de la aplicación web Transfer Family tienen acceso a recursos específicos de S3, lo que ayuda a monitorear los patrones de acceso y garantizar la autorización adecuada.

Visualización de las entradas de CloudTrail registro

Hay varias formas de ver y analizar las entradas de CloudTrail registro de su aplicación web Transfer Family:

Uso de la CloudTrail consola

La CloudTrail consola proporciona una interfaz fácil de usar para ver y filtrar las entradas de registro:

1. Abra la CloudTrail consola en <https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación, elija Historial de eventos.
3. Utilice las opciones de filtro para restringir los eventos:
 - Defina la fuente del evento en `transfer.amazonaws.com` para ver solo los eventos de Transfer Family.
 - Filtra por nombre de evento para ver operaciones específicas, como `UserAuthentication`.
 - Use el rango de tiempo para centrarse en los eventos dentro de un período específico.
4. Haga clic en cualquier evento para ver su información detallada.

Acceso a los registros en Amazon S3

Si ha configurado un registro para CloudTrail entregar los registros a un bucket de Amazon S3, puede acceder directamente a los archivos de registro sin procesar:

1. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3/>.
2. Navegue hasta el depósito y el prefijo donde están almacenados sus CloudTrail registros.
3. Los registros están organizados por año, mes, día y región. Navegue hasta el directorio correspondiente.
4. Descargue y abra los archivos de registro, que están en formato JSON.

Solución de problemas de sus aplicaciones web

Note

Estos consejos de solución de problemas están dirigidos al administrador de la aplicación web y no al usuario final. Para los usuarios finales, si tienen algún problema, pónganse en contacto con el administrador de la aplicación web. Todos los casos en los que aparece en los párrafos siguientes se refieren al administrador de la aplicación web.

Solucionar errores de red

Descripción

El usuario final ve un aviso de red llamado Error de red al cargar el punto final de la aplicación web.

Causa

Los problemas más comunes son los siguientes:

- El administrador no asignó el usuario que intenta iniciar sesión en la nueva aplicación.
- El administrador no agregó las acciones necesarias a sus funciones de IAM.
- Aparece una lista de concesiones de acceso de S3 asignadas a su usuario, pero CORS no está configurado correctamente para su depósito o depósitos de Amazon S3.

Solución

- En el Centro de identidades de IAM, asegúrese de asignar el usuario a la aplicación correcta. O bien, si tiene un grupo asignado, asegúrese de que el usuario que intenta iniciar sesión pertenece al grupo correcto. Esto se describe en [Asigne o añada usuarios o grupos a una aplicación web Transfer Family](#).
- Compruebe si sus funciones contienen las acciones necesarias en la política de confianza personalizada tanto para las acciones como para `sts:AssumeRole` las `sts:SetContext` acciones. Esto se describe en [Configurar las funciones de IAM para las aplicaciones web Transfer Family](#).
- Comprueba la política CORS para todos los buckets que utiliza tu aplicación web. Esto se describe en [Configurar el uso compartido Cross-origin de recursos \(CORS\) para su bucket de Amazon S3](#).

Solucione el problema de que el bucket configurado no aparece

Descripción

Todo parece estar configurado correctamente, pero el bucket de Amazon S3 no aparece en la aplicación web.

Causa

Una posible causa es que el bucket de Amazon S3 no esté en la misma cuenta que la aplicación web.

Solución

Asegúrese de que el bucket de Amazon S3 esté en la misma cuenta que la aplicación web. Cross-accountLos buckets no son compatibles actualmente.

Solucionar errores de URL personalizadas

Descripción

Cuando el usuario final inicia sesión en la aplicación web, recibe el mensaje de error Error en la autorización: falta el código de autorización.

Causa

Si usó CloudFront directamente la CloudFormation plantilla proporcionada, en lugar de la proporcionada, es probable que haya configurado mal la política de solicitudes de origen para no reenviar las cadenas de consulta.

Solución

Actualiza tu política de solicitudes de origen para reenviar las cadenas de consulta y las cookies al origen.

Descripción

Cuando el usuario final intenta acceder a una aplicación web de Transfer Family, recibe una respuesta 404.

Causa

Si la usaste CloudFront directamente, en lugar de la CloudFormation plantilla proporcionada, es probable que hayas configurado mal la política de caché para incluir el Host encabezado en la clave de caché o hayas configurado mal la política de solicitud de origen para reenviar el Host encabezado.

Solución

- Asegúrese de que su política de caché no incluya el Host encabezado en la clave de caché
- Asegúrate de que tu política de solicitudes de origen no reenvíe el Host encabezado.

Soluciona errores varios

Descripción

El usuario final no puede iniciar sesión, no puede ver ningún depósito o archivo, o recibe otro error.

Causa

Una posible causa es que el ARN de la instancia del Centro de Identidad de IAM no coincide con el valor del ARN de sus subvenciones o el ARN de la instancia del Centro de Identidad de IAM de su aplicación web.

Solución

Compruebe los siguientes elementos para ver si coinciden.

- En el Centro de identidades de IAM, vaya a Configuración y consulte el ARN de la instancia.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

- En Amazon S3, vaya a Access Grants y consulte el ARN de su instancia de IAM Identity Center.

```
arn:aws:sso:::account-id:application/ssoins-instance-identifier/apl-1234567890abcdef0
```

- En Transfer Family, vaya a la página de detalles de la aplicación web y consulte el ARN de su instancia.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

El *instance-identifier* valor debe ser el mismo en estos tres lugares.

Aparecen cubos S3 duplicados en la aplicación web

Descripción

Los usuarios ven el mismo bucket de S3 enumerado varias veces en la interfaz de la aplicación web Transfer Family.

Causa

Esto ocurre cuando un usuario forma parte de varios grupos de Active Directory que tienen concesiones duplicadas en el mismo depósito de S3. La aplicación web muestra todas las concesiones de nivel superior asociadas al usuario (UID o GID), independientemente de si el usuario tiene varias concesiones asignadas a la misma ubicación del depósito.

Solución

Para resolver este problema, los administradores deben deduplicar las concesiones para que cada usuario solo tenga una concesión para cada ubicación de S3. Revise la configuración de las concesiones de acceso de S3 y consolide las concesiones duplicadas para el mismo segmento en diferentes grupos de Active Directory.

Instrucciones para el usuario final de las aplicaciones web Transfer Family

Note

En este tema, la información está destinada a los usuarios finales que interactúan con la aplicación web. Todas las instancias en las que aparece en este tema se refieren a los usuarios finales.

En este tema se describe cómo acceder a una aplicación AWS Transfer Family web que está autorizado a usar y cómo puede interactuar con ella.

Cuotas de aplicaciones web

Tenga en cuenta las siguientes limitaciones cuando utilice aplicaciones web.

- Número máximo de resultados de búsqueda por consulta: 10 000
- Los buckets de Amazon S3 que utiliza la aplicación web Transfer Family deben estar en la misma cuenta que la propia aplicación web. Cross-account Los buckets no se admiten actualmente.
- Amplitud máxima de búsqueda por consulta: 10 000 archivos buscados
- Tamaño máximo de carga por archivo: 160 GB (149 GiB)
- Tamaño máximo de archivo para copiar: 5,36 GB (5 GiB)
- No se admiten nombres de carpetas que comiencen o terminen con puntos (.)

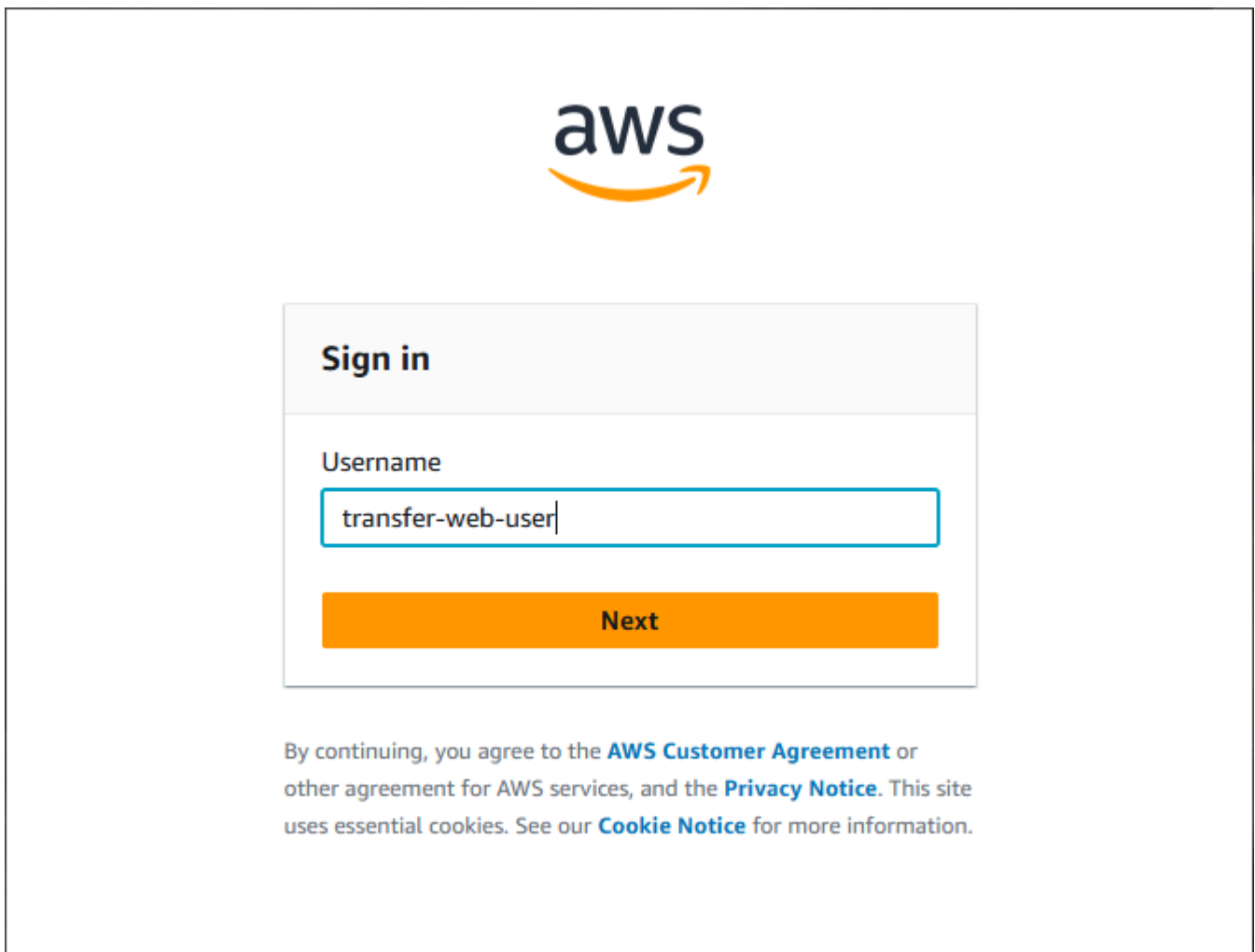
Experiencia de usuario para los usuarios del IAM Identity Center

En esta sección se describe la experiencia del usuario si su organización utilizaba el Centro de identidades de IAM para configurar sus usuarios.

Para acceder a una aplicación web de Transfer Family

1. Deberías recibir un correo electrónico de `no-reply@login.awsapps.com` titulado «Invitación a unirse» AWS IAM Identity Center. Acepte la invitación para activar su cuenta de usuario.
2. En el mensaje, elija la URL situada debajo de la URL de su portal de AWS acceso.

Esto lo llevará a la pantalla de inicio de AWS sesión.



The screenshot shows the AWS sign-in interface. At the top center is the AWS logo. Below it is a light gray box titled "Sign in". Inside this box, there is a "Username" label followed by a text input field containing the text "transfer-web-user". Below the input field is a large orange button labeled "Next". At the bottom of the page, outside the sign-in box, is a line of text: "By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information."

3. Introduce tus credenciales y selecciona Iniciar sesión.

Esto le llevará a la Portal de acceso a AWS, que muestra una lista de las aplicaciones disponibles.

4. Elija la aplicación para su aplicación web Transfer Family.

Experiencia de usuario para usuarios de proveedores de identidad externos

Si su organización no utilizó AWS IAM Identity Center para configurar a sus usuarios, su experiencia de incorporación dependerá de la aplicación de proveedor de identidad que haya utilizado para configurar sus usuarios finales. Tras autenticarse e iniciar sesión, la interfaz de la aplicación web será la misma que la que se describe en la siguiente sección.

Note

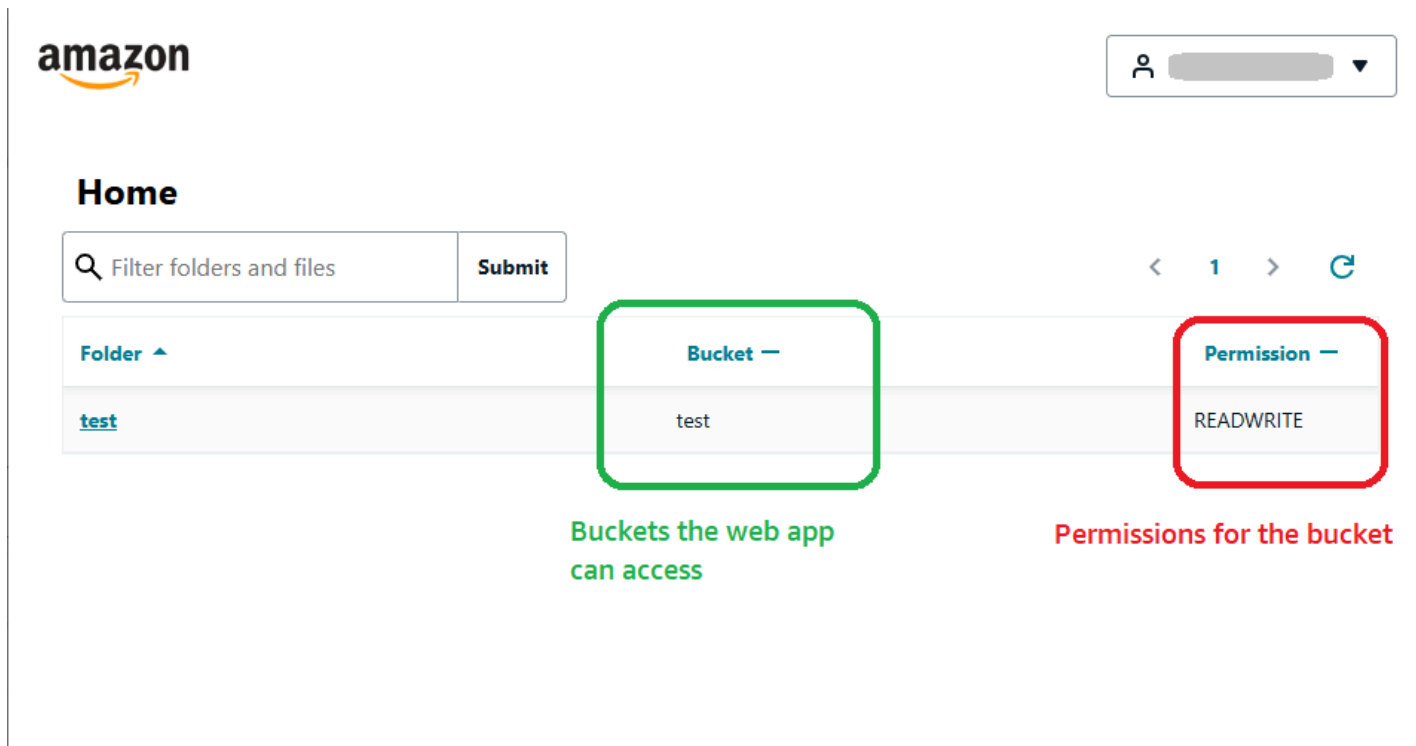
Si un usuario pertenece a varios grupos de Active Directory que tienen concesiones para el mismo bucket de Amazon S3, el bucket aparece varias veces en la interfaz de la aplicación web. Esto se debe a que la aplicación web enumera todas las concesiones de nivel superior asociadas al UID o GID del usuario, incluidas las concesiones duplicadas al mismo depósito. Para evitar la duplicación de listados, los administradores pueden consolidar varias concesiones para que cada usuario tenga solo una concesión por ubicación de Amazon S3.

Interfaz de usuario final de Transfer Family

Una vez que te hayas autenticado e iniciado sesión, podrás interactuar con la aplicación web.

Hay cuatro vistas principales.

- **Página de inicio:** su página de inicio muestra las ubicaciones de S3 a las que puede acceder, así como los permisos de cada una de ellas. Una ubicación de S3 es un depósito o prefijo de S3, que puede definir al utilizar S3 Access Grants. Esta es la vista inicial para los usuarios que muestra los recursos de S3 de nivel raíz a los que tienen acceso los usuarios finales y los permisos de cada ubicación de S3.



- Detalles de ubicación: esta vista permite a los usuarios examinar archivos y carpetas en S3, así como cargar o descargar archivos.
- Acción de ubicación: después de elegir una acción (como Cargar), se abre otra vista de la ubicación del archivo.
- Puntos suspensivos verticales: el icono de puntos suspensivos verticales abre el menú Acciones.

Acciones disponibles

La mayoría de las acciones están disponibles en el menú Acciones. Para la otra acción principal, la descarga de archivos, se utiliza el icono de descarga después de seleccionar un archivo (actualmente, solo se puede descargar un archivo a la vez).

Transfer Web App

Scott

Home / test2 / Testing-01

Testing-01/

☐ Include subfolders

< 1 > ↺ ⋮

☐	Name ▲	Type —	Last Modified —	Size —	
☐	scott-small.png	png	10/30/2024, 2:28:31 PM	375.4 kB	
☐	Scott-02.jpg	jpg	10/30/2024, 2:28:30 PM	196.6 kB	
☐	Scott-badge.jpg	jpg	10/30/2024, 2:28:31 PM	1.3 MB	

Download icon

Desde una carpeta, utilice el menú Acciones para realizar cualquiera de las siguientes tareas:

- Copie uno o más archivos a otra ubicación.
- Crear una carpeta.
- Elimine uno o más archivos.
- Cargue uno o más archivos.
- Sube una carpeta completa (incluidas las subcarpetas, si las hubiera).
- Selecciona una carpeta y navega hasta ella. A continuación, puede realizar cualquiera de las acciones enumeradas anteriormente.
- Ordenar por página.
- Filtra por nombre de archivo o carpeta por carpeta y subcarpetas.

amazon

Home / test

test

🔍 Search current folder

Submit

☐ Include subfolders

< 1 > ↺ ⋮

📄 Copy files

📁 Create folder

🗑 Delete files

📁 Upload files

📁 Upload folder

Name ▲	Type —	Last Modified —
📁 My First Folder/	Folder	
📁 My Second Folder/	Folder	
📁 Testing-01/	Folder	
📁 Testing-02/	Folder	

AWS Transfer Family Conectores SFTP

Un conector AWS Transfer Family SFTP establece una conexión con un servidor SFTP remoto para transferir archivos entre el almacenamiento de Amazon y un servidor remoto mediante el protocolo SFTP. Puede enviar archivos desde Amazon S3 a un servidor SFTP externo propiedad de un socio, recuperar archivos del servidor SFTP de un socio a Amazon S3 o enumerarlos, eliminar, cambiar el nombre o mover archivos en el servidor remoto. Los conectores SFTP admiten dos tipos de salida: servicio gestionado (mediante infraestructura AWS gestionada) y VPC (enrutamiento a través de la VPC mediante Amazon VPC Lattice). Con los conectores SFTP, puede crear flujos de trabajo de transferencia de archivos automatizados y basados en eventos. AWS

Consulte los [conectores SFTP de AWS Transfer Family](#) para ver una breve introducción a los conectores SFTP Transfer Family.

Temas

- [Creación de conectores SFTP](#)
- [Conectividad de VPC para conectores SFTP](#)
- [Uso de conectores SFTP](#)
- [Supervisión de conectores SFTP](#)
- [Administración de conectores SFTP](#)
- [Escalado y cuotas para los conectores SFTP](#)
- [Arquitecturas de referencia que utilizan conectores SFTP](#)

Creación de conectores SFTP

En este tema se describe cómo crear conectores SFTP. Cada conector ofrece la posibilidad de conectarse con un servidor SFTP remoto. Debe realizar las siguientes tareas de alto nivel para configurar un conector SFTP.

Note

Para ver VPC-based los conectores que enrutan el tráfico a través de su nube privada virtual, consulte [Cree un conector SFTP con salida VPC-based](#).

1. Guarde las credenciales de autenticación del conector en AWS Secrets Manager.
2. Cree el conector especificando el ARN secreto, la URL del servidor remoto o el ARN de configuración de recursos, la política de seguridad que contiene los algoritmos que admitirá el conector y otros ajustes de configuración.
3. Tras crear el conector, puede probarlo para asegurarse de que puede establecer conexiones con el servidor SFTP remoto.

Elegir el tipo de salida del conector SFTP

Al crear un conector SFTP, se elige el tipo de salida entre «Servicio gestionado» y «VPC Lattice».

- Servicio gestionado (predeterminado): el conector utiliza las puertas de enlace NAT y las direcciones IP de su propiedad AWS Transfer Family para enrutar las conexiones a través de la Internet pública. El servicio proporciona 3 direcciones IP estáticas para los conectores que deben figurar en la lista de permitidos de los servidores remotos para poder establecer conexiones.
- VPC Lattice: el conector enruta el tráfico a través de su entorno de VPC mediante Amazon VPC Lattice. Utilice la conectividad de VPC para los conectores SFTP en los siguientes escenarios:
 - Servidores SFTP privados: Conéctese a servidores SFTP a los que solo se puede acceder desde su VPC
 - On-premises conectividad: Conéctese a servidores SFTP locales a través AWS Direct Connect de nuestras conexiones AWS Virtual Private Network
 - Direcciones IP personalizadas: presente sus propias puertas de enlace NAT y direcciones IP elásticas al servidor remoto
 - Controles de seguridad centralizados: dirija las transferencias de archivos a través de los controles centrales ingress/egress de su organización

La siguiente matriz le ayuda a elegir el tipo de conector adecuado para sus casos de uso.

Matriz de tipos de salida del conector SFTP

Funcionalidad	Tipo de salida = Servicio gestionado	Tipo de salida = celosía de VPC
Conectividad a servidores SFTP alojados públicamente (accesibles a Internet)	compatible	Compatible con 1

Funcionalidad	Tipo de salida = Servicio gestionado	Tipo de salida = celosía de VPC
Conectividad a servidores SFTP alojados de forma privada (locales)	No compatible	Compatible con 2
Conectividad a servidores SFTP alojados de forma privada (en la VPC)	No compatible	compatible
Direcciones IP estáticas presentadas al servidor SFTP remoto	Compatible mediante direcciones IP estáticas suministradas por el servicio	Compatible mediante direcciones IP estáticas propiedad del cliente
Ancho de banda disponible	50 MBPS por cuenta	Mayor ancho de banda, disponible en Resource Gateway y NAT Gateway, propiedad del cliente
Enrutamiento del tráfico a Internet a través de pasarelas NAT y firewalls de red propiedad del cliente	No admitido. Las pasarelas NAT son propiedad del servicio Transfer Family y están administradas por él.	compatible

¹ Con el tipo de salida = red de VPC, se admite la conectividad con los servidores alojados de forma pública mediante la configuración de la infraestructura de salida (pasarelas NAT) en las VPC de salida.

² Con el tipo de salida = VPC Lattice, se admite la conectividad con servidores alojados de forma privada mediante las redes existentes en la VPC, como una VPN. AWS Direct Connect

Elegir el modo de direccionamiento IP

Al crear un conector SFTP con salida gestionada por el servicio, puede elegir entre dos modos de direccionamiento IP:

- Solo IPv4 (predeterminado): el conector utiliza direcciones IPv4 exclusivamente para conectarse al servidor SFTP remoto. Este es el modo predeterminado al crear conectores a través de la consola, la AWS CLI o la API.
- Dual-stack: El conector admite direcciones IPv6 e IPv4. En el modo de doble pila, el conector prefiere IPv6 cuando la resolución de DNS devuelve resultados de IPv6 y utiliza IPv4 cuando solo se devuelven resultados de DNS de IPv4.

Note

El modo de direccionamiento IP se aplica únicamente a los conectores con un tipo de salida gestionado por el servicio. Los conectores que utilizan la salida de celosía de VPC no admiten esta configuración.

Temas

- [Almacene las credenciales de autenticación para los conectores SFTP en Secrets Manager](#)
- [Cree un conector SFTP con salida gestionada por el servicio](#)
- [Cree un conector SFTP con salida VPC-based](#)
- [Prueba de un conector SFTP](#)

Almacene las credenciales de autenticación para los conectores SFTP en Secrets Manager

Puede usar Secrets Manager para almacenar las credenciales de usuario de los conectores SFTP. Al crear el secreto, debe proporcionar un nombre de usuario. Además, puede proporcionar una contraseña, una clave privada o ambas. Para obtener más información, consulte [Cuotas para conectores SFTP](#).

Note

Cuando guardas secretos en Secrets Manager, Cuenta de AWS incurres en cargos. Para obtener más información acerca de los precios, consulte [AWS Secrets Manager Precios](#).

Almacenamiento de las credenciales de usuario en Secrets Manager para un conector SFTP

1. Inicia sesión en Consola de administración de AWS y abre la AWS Secrets Manager consola en <https://console.aws.amazon.com/secretsmanager/>.
2. En el panel de navegación izquierdo, seleccione Secretos.
3. En la página Secretos, seleccione Almacenar un nuevo secreto.
4. En la página Seleccionar tipo de secreto, en Tipo de secreto, seleccione Otro tipo de secreto.
5. Proporcione la key/value información de su secreto: debe proporcionar el nombre de usuario y una clave privada o una contraseña.
 - a. En la sección de Key/value parejas, selecciona la Key/value pestaña.
 - Clave: introduzca **Username**.
 - valor: introduzca el nombre del usuario que está autorizado a conectarse al servidor del socio.
 - b. Si quieres proporcionar un key pair, selecciona Añadir fila y, en la sección de Key/value pares, selecciona la Key/value pestaña.
 - Clave: introduzca **PrivateKey**.
 - valor: pega tu clave privada.

Consejo: Los datos de la clave privada que introduzca deben corresponder a la clave pública que está almacenada para este usuario en el servidor SFTP remoto.

Note

No es posible utilizar una clave privada protegida por contraseña para la autenticación con un conector SFTP. AWS Transfer Family

Para obtener más información sobre cómo generar un public/private key pair, consulte [Creación de claves SSH en macOS, Linux o Unix](#).

- c. Si desea proporcionar una contraseña, seleccione Añadir fila y, en la sección de Key/value pares, elija la Key/value pestaña.
 - Clave: introduzca **Password**.

- valor: introduzca una contraseña para el usuario.
6. Elija Siguiente.
 7. En la página Configurar secreto, introduzca un nombre y una descripción para el secreto. Se recomienda utilizar un prefijo de **aws/transfer/** para el nombre. Por ejemplo, puede dar un nombre a su secreto de **aws/transfer/connector-1**.
 8. Seleccione Siguiente y, a continuación, acepte los valores predeterminados de la página Configurar rotación. A continuación, elija Siguiente.
 9. En la página de Revisión, elija Guardar para crear y almacenar el secreto.

Cree un conector SFTP con salida gestionada por el servicio

En este procedimiento se explica cómo crear conectores SFTP mediante la AWS Transfer Family consola o. AWS CLI

Console

Creación de un Conector SFTP

1. Abra la AWS Transfer Family consola en. <https://console.aws.amazon.com/transfer/>
2. En el panel de navegación izquierdo, seleccione Conectores SFTP y, a continuación, seleccione Crear conector SFTP.
3. En la sección de configuración del conector, para el tipo de salida, elija Servicio gestionado. Esta opción utiliza una infraestructura de salida AWS Transfer Family gestionada. El servicio Transfer Family proporciona y administra direcciones IP estáticas para cada conector SFTP.
4. En la sección de Configuración del conector, proporcione la siguiente información:

Connector configuration

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

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

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

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

`sftp://sftp.example.com`

URL of the remote (target) SFTP server

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

Choose an IAM role

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

Choose a logging role

- Para la URL, introduzca la URL de un servidor SFTP remoto. Esta URL debe tener el siguiente formato como `sftp://partner-SFTP-server-url`, por ejemplo, `sftp://AnyCompany.com`.

Note

También tiene la posibilidad de proporcionar un número de puerto en su URL. El formato es `sftp://partner-SFTP-server-url:port-number`. El número de puerto predeterminado (cuando no se especifica ningún puerto) es el puerto 22.

- Para la función de acceso, elija el nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que se va a utilizar.
 - Asegúrese de que este rol proporcione acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`.
 - Asegúrese de que este rol dé permiso a `secretsmanager:GetSecretValue` para acceder al secreto.

Note

En la política, debe especificar el ARN del secreto. El ARN contiene el nombre secreto, pero lo añade con seis caracteres alfanuméricos aleatorios. El ARN de un secreto tiene el siguiente formato.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Asegúrese de que contiene una relación de confianza que permita que el conector tenga acceso a los recursos cuando atienda las solicitudes de transferencia de sus usuarios. Para obtener más información sobre cómo establecer una relación de confianza, consulte [Para establecer una relación de confianza](#).

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

```

    ],
    "Resource": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
  }
]
}

```

 Note

Para el rol de acceso, el ejemplo concede acceso a un único secreto. Sin embargo, puede utilizar un carácter comodín, que puede ahorrarle trabajo si quiere reutilizar el mismo rol de IAM para varios usuarios y secretos. Por ejemplo, la siguiente declaración de recursos concede permisos para todos los secretos cuyos nombres comiencen por `aws/transfer`.

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

También puede almacenar los secretos que contengan sus credenciales de SFTP en otra Cuenta de AWS. Para obtener más información sobre cómo habilitar el acceso secreto entre cuentas, consulta [Permisos a los AWS Secrets Manager secretos para los usuarios de otra](#) cuenta.

5. Complete la configuración del conector:

- (Opcional) Para la función de registro, elija la función de IAM que utilizará el conector para enviar eventos a sus CloudWatch registros. En el siguiente ejemplo de política, se enumeran los permisos necesarios para registrar eventos en los conectores SFTP.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ]
    }
  ]
}

```

```

    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
  }
]
}

```

6. En el panel Configuración SFTP, proporcione la siguiente información:

SFTP configuration [Info](#)

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

aws/transfer/sftp-connector1 [Store a new secret](#)

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

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

ssh-rsa AAAA... [Remove](#)

[Add trusted host key](#)

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

5

- Para las credenciales de Connector, en la lista desplegable, elija el nombre de un código secreto AWS Secrets Manager que contenga la clave privada o la contraseña del usuario de SFTP. Debe crear un secreto y almacenarlo de una manera específica. Para obtener más información, consulte [Almacene las credenciales de autenticación para los conectores SFTP en Secrets Manager](#).
- (Opcional) Tiene la opción de crear su conector y dejar el TrustedHostKeys parámetro vacío. Sin embargo, el conector no podrá transferir archivos con el servidor remoto hasta que proporcione este parámetro en la configuración del conector. Puede introducir las claves de host de confianza al crear el conector o actualizarlo más adelante utilizando la información de la clave de host que devuelve la acción de la TestConnection consola o el comando de la API. Es decir, para el cuadro de texto Trusted host keys, puede realizar una de las siguientes acciones:
 - Proporcione las claves de host de confianza al momento de crear el conector. Pegue la parte pública de la clave de host que se utiliza para identificar el servidor externo. Para añadir más de una clave, seleccione Añadir clave de host de confianza para añadir

una clave adicional. Puede utilizar el comando `ssh-keyscan` en el servidor SFTP para recuperar la clave necesaria. Para obtener más información sobre el formato y el tipo de claves de host de confianza compatibles con Transfer Family, consulte [SFTPConnectorConfig](#).

- Deje vacío el cuadro de texto Claves de host confiables al crear el conector y actualícelo más adelante con esta información. Si no dispone de la información de la clave de host en el momento de crear el conector, puede dejar este parámetro vacío por ahora y continuar con la creación del conector. Una vez creado el conector, utilice el identificador del nuevo conector para ejecutar el `TestConnection` comando, ya sea en la página de detalles del conector AWS CLI o desde ella. Si se ejecuta correctamente, `TestConnection` devolverá la información clave de host necesaria. A continuación, puede editar el conector mediante la consola (o ejecutando el `UpdateConnector` AWS CLI comando) y añadir la información de la clave de host que se devolvió al ejecutarlo `TestConnection`.

 Important

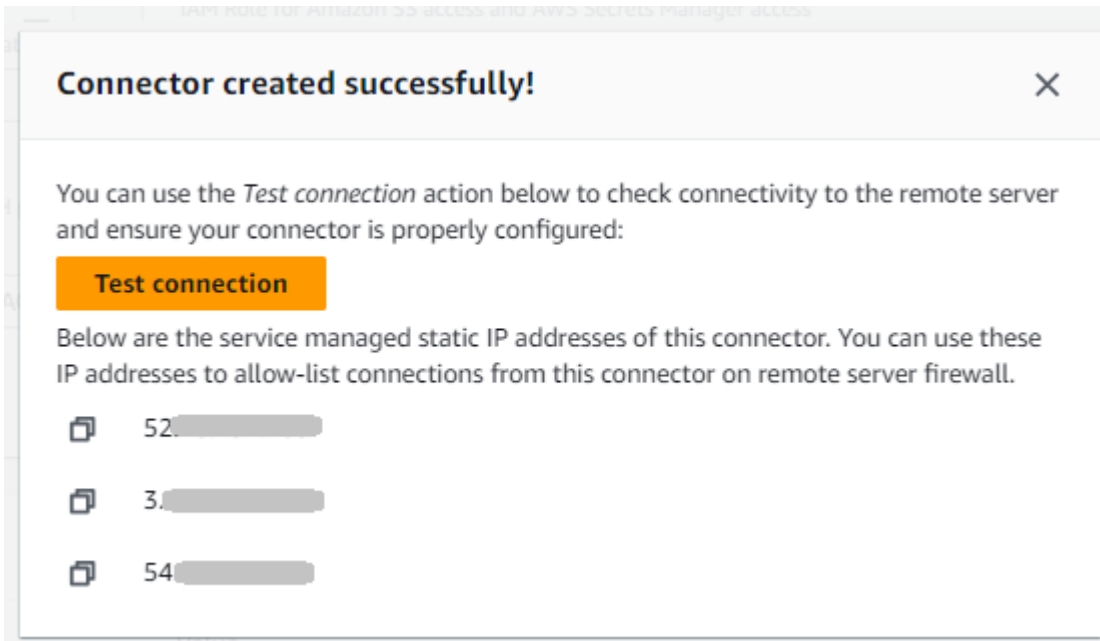
Si recupera la clave de host del servidor remoto ejecutándola `TestConnection`, asegúrese de realizar una validación fuera de banda de la clave que se devuelve. Debe aceptar la nueva clave como de confianza o verificar la huella digital presentada con una huella conocida anteriormente que haya recibido del propietario del servidor SFTP remoto al que se está conectando.

- (Opcional) Para el número máximo de conexiones simultáneas, en la lista desplegable, elija el número de conexiones simultáneas que el conector crea al servidor remoto. La selección predeterminada en la consola es 5.

Esta configuración especifica el número de conexiones activas que el conector puede establecer con el servidor remoto al mismo tiempo. La creación de conexiones simultáneas puede mejorar el rendimiento del conector al permitir operaciones en paralelo.

7. En la sección de opciones de algoritmos criptográficos, elija una política de seguridad de la lista desplegable del campo Política de seguridad. La política de seguridad le permite seleccionar los algoritmos criptográficos que admite su conector. Para obtener más información sobre las políticas y los algoritmos de seguridad disponibles, consulte [Políticas de seguridad para AWS Transfer Family Conectores SFTP](#).
8. (Opcional) En la sección Etiquetas, para Clave y Valor, escriba una o varias etiquetas como pares clave-valor.

- Una vez que haya confirmado todos los ajustes, elija Crear conector SFTP para crear el conector SFTP. Si el conector se ha creado correctamente, aparecerá una pantalla con una lista de las direcciones IP estáticas asignadas y un botón de prueba de conexión. Utilice el botón para probar la configuración del nuevo conector.



Aparece la página Conectores, con el ID del nuevo conector SFTP agregado a la lista. Para ver los detalles de los conectores, consulte [Ver los detalles del conector SFTP](#).

CLI

Utilice el comando [create-connector](#) para crear un conector. Para utilizar este comando para crear un conector SFTP, debe proporcionar la siguiente información.

- La dirección URL de un servidor SFTP remoto. Esta URL debe tener el siguiente formato como `sftp://partner-SFTP-server-url`, por ejemplo, `sftp://AnyCompany.com`.
- Ver Acceso de roles. Seleccione el nombre de recurso de Amazon (ARN) del rol de AWS Identity and Access Management (IAM) que desee utilizar.
 - Asegúrese de que este rol proporcione acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`.
 - Asegúrese de que este rol dé permiso a `secretsmanager:GetSecretValue` para acceder al secreto.

Note

En la política, debe especificar el ARN del secreto. El ARN contiene el nombre secreto, pero lo añade con seis caracteres alfanuméricos aleatorios. El ARN de un secreto tiene el siguiente formato.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Asegúrese de que contiene una relación de confianza que permita que el conector tenga acceso a los recursos cuando atienda las solicitudes de transferencia de sus usuarios. Para obtener más información sobre cómo establecer una relación de confianza, consulte [Para establecer una relación de confianza](#).

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



```

    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
  },
  {
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
  }
]
}

```

Note

Para el rol de acceso, el ejemplo concede acceso a un único secreto. Sin embargo, puede utilizar un carácter comodín, que puede ahorrarle trabajo si quiere reutilizar el mismo rol de IAM para varios usuarios y secretos. Por ejemplo, la siguiente declaración de recursos concede permisos para todos los secretos cuyos nombres comiencen por `aws/transfer`.

```

"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"

```

También puede almacenar los secretos que contengan sus credenciales de SFTP en otra Cuenta de AWS. Para obtener más información sobre cómo habilitar el acceso secreto entre cuentas, consulta [Permisos a los AWS Secrets Manager secretos para los usuarios de otra](#) cuenta.

- (Opcional) Elija la función de IAM que utilizará el conector para enviar eventos a sus CloudWatch registros. En el siguiente ejemplo de política, se enumeran los permisos necesarios para registrar eventos en los conectores SFTP.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",

```

```

        "Action": [
            "logs:CreateLogStream",
            "logs:DescribeLogStreams",
            "logs:CreateLogGroup",
            "logs:PutLogEvents"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
}

```

- Proporcione la siguiente información de configuración de SFTP.
 - El ARN de un secreto AWS Secrets Manager que contiene la clave privada o la contraseña del usuario de SFTP.
 - La parte pública de la clave de host que se utiliza para identificar el servidor externo. Si lo desea, puede proporcionar varias claves de host de confianza.

La forma más sencilla de proporcionar la información del SFTP es guardarla en un archivo. Por ejemplo, copie el siguiente texto de ejemplo en un archivo denominado `testSFTPConfig.json`.

```

// Listing for testSFTPConfig.json
{
    "UserSecretId": "arn:aws::secretsmanager:us-east-2:123456789012:secret:aws/transfer/example-username-key",
    "TrustedHostKeys": [
        "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
    ]
}

```

- Especifique una política de seguridad para el conector e introduzca el nombre de la política de seguridad.

Note

`SecretId` Puede ser el ARN completo o el nombre del secreto (*example-username-key* en la lista anterior).

A continuación, ejecute el siguiente comando para crear el conector:

```
aws transfer create-connector --url "sftp://partner-SFTP-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/
AWSTransferLoggingAccess \
--sftp-config file:///path/to/testSFTPConfig.json \
--security-policy-name security-policy-name \
--maximum-concurrent-connections integer-from-1-to-5
```

Cuando describe un conector de tipo salida de VPC, la respuesta incluye los nuevos campos:

```
{
  "Connector": {
    "AccessRole": "arn:aws:iam::123456789012:role/connector-role",
    "Arn": "arn:aws:transfer:us-east-1:123456789012:connector/
c-1234567890abcdef0",
    "ConnectorId": "c-1234567890abcdef0",
    "Status": "ACTIVE",
    "EgressConfig": {
      "VpcLattice": {
        "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-12345678",
        "PortNumber": 22
      }
    },
    "EgressType": "VPC",
    "ServiceManagedEgressIpAddresses": null,
    "SftpConfig": {
      "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
      "UserSecretId": "aws/transfer/connector-secret"
    },
    "Url": "sftp://my.sftp.server.com:22"
  }
}
```

Tenga en cuenta que `ServiceManagedEgressIpAddresses` es nulo para los conectores de tipo salida de VPC, ya que el tráfico se dirige a través de la VPC en lugar de a través de la infraestructura gestionada. AWS

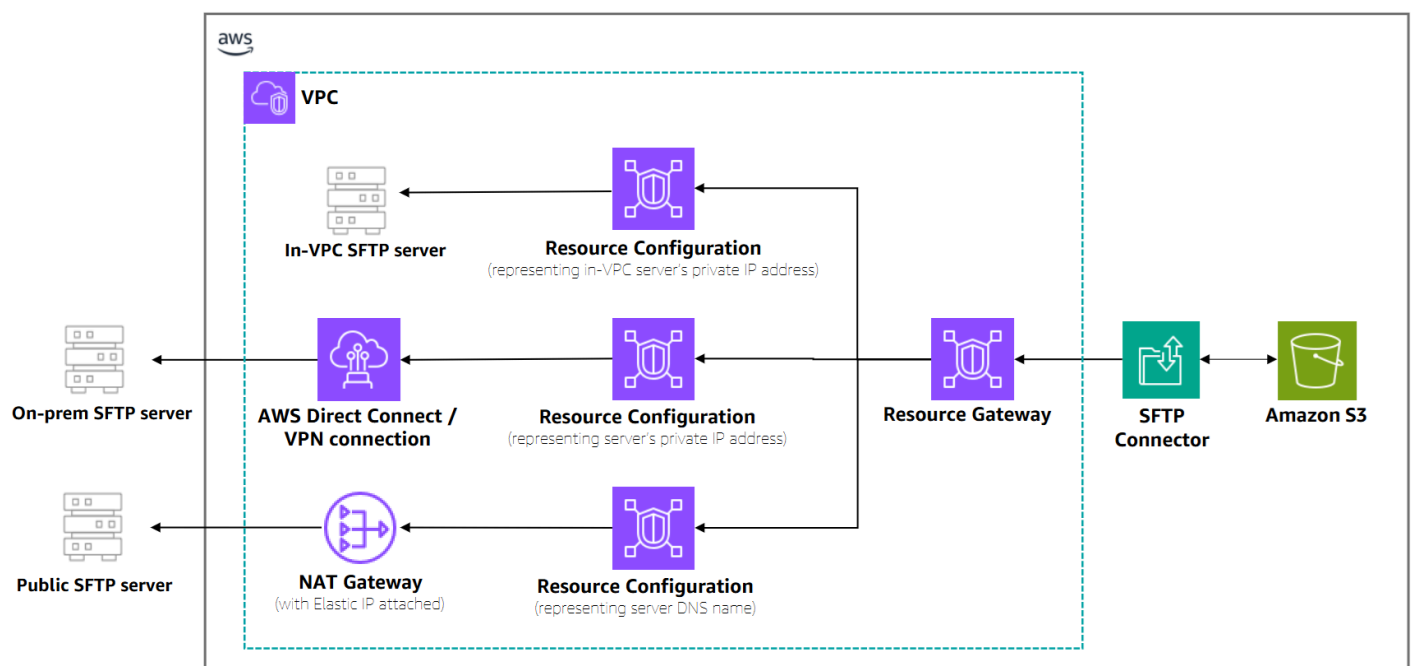
Cree un conector SFTP con salida VPC-based

En este tema se proporcionan instrucciones paso a paso para crear conectores SFTP con conectividad de VPC. LATTICE-enabled Los conectores VPC_ utilizan Amazon VPC Lattice para enrutar el tráfico a través de su nube privada virtual, lo que permite conexiones seguras a puntos de conexión privados o utiliza sus propias puertas de enlace NAT para el acceso a Internet.

Cuándo usar la conectividad de VPC

Utilice la conectividad de VPC para los conectores SFTP en los siguientes escenarios:

- Servidores SFTP privados: Conéctese a servidores SFTP a los que solo se puede acceder desde su VPC.
- On-premises conectividad: conéctese a servidores SFTP locales a través de conexiones AWS Site-to-Site VPN o Direct AWS Connect.
- Direcciones IP personalizadas: utilice sus propias puertas de enlace NAT y direcciones IP elásticas, incluidos los escenarios de BYOIP.
- Controles de seguridad centralizados: dirija las transferencias de archivos a través de los controles centrales de su organización. ingress/egress



Requisitos previos para los conectores SFTP VPC_ LATTICE-enabled

Antes de crear un conector VPC_ LATTICE-enabled SFTP, debe cumplir los siguientes requisitos previos:

VPC-based Cómo funciona la conectividad

VPC Lattice le permite compartir de forma segura los recursos de VPC con otros servicios. AWS AWS Transfer Family utiliza una red de servicios para simplificar el proceso de intercambio de recursos. Los componentes clave son:

- **Resource Gateway:** sirve como punto de acceso a su VPC. Esto se crea en la VPC con un mínimo de dos zonas de disponibilidad.
- **Configuración de recursos:** contiene la dirección IP privada o el nombre DNS público del servidor SFTP al que desea conectarse.

Cuando crea un LATTICE-enabled conector VPC_, AWS Transfer Family utiliza la sesión de acceso directo (FAS) para obtener temporalmente sus credenciales y asociar su configuración de recursos a nuestra red de servicios.

Pasos de configuración necesarios

1. **Infraestructura de VPC:** asegúrese de tener una VPC correctamente configurada con las subredes, tablas de enrutamiento y grupos de seguridad necesarios para los requisitos de conectividad del servidor SFTP.
2. **Puerta de enlace de recursos:** cree una puerta de enlace de recursos en su VPC mediante el comando VPC Lattice. `create-resource-gateway` La puerta de enlace de recursos debe estar asociada a subredes de al menos dos zonas de disponibilidad. Para obtener más información, consulte [Resource Gateways](#) en la Guía del usuario de Amazon VPC Lattice.
3. **Configuración de recursos:** cree una configuración de recursos que represente el servidor SFTP de destino mediante el comando VPC Lattice `create-resource-configuration`. Puede especificar:
 - Una dirección IP privada para puntos finales privados
 - Un nombre DNS público para los puntos finales públicos (las direcciones IP no se admiten en los puntos finales públicos)

4. Credenciales de autenticación: almacene las credenciales de usuario de SFTP AWS Secrets Manager como se describe en. [Almacene las credenciales de autenticación para los conectores SFTP en Secrets Manager](#)

 Important

La puerta de enlace de recursos y la configuración de recursos deben crearse en la misma AWS cuenta. Al crear una configuración de recursos, primero debe disponer de una puerta de enlace de recursos.

Para obtener más información sobre las configuraciones de recursos de VPC, consulte Configuraciones de [recursos en la Guía](#) del usuario de Amazon VPC Lattice.

 Note

La conectividad de VPC para los conectores SFTP está disponible en los lugares donde estén disponibles los recursos de Regiones de AWS Amazon VPC Lattice. Para obtener más información, consulte las preguntas frecuentes sobre [VPC Lattice](#). La compatibilidad con las zonas de disponibilidad varía según la región y las pasarelas de recursos requieren un mínimo de dos zonas de disponibilidad.

Cree un conector VPC_ SFTP LATTICE-enabled

Tras completar los requisitos previos, puede crear un conector SFTP con conectividad de VPC mediante la consola de AWS administración o los AWS CLI SDK. AWS

Console

Para crear un conector VPC_ SFTP LATTICE-enabled

1. Abra la consola en AWS Transfer Family . <https://console.aws.amazon.com/transfer/>
2. En el panel de navegación izquierdo, seleccione Conectores SFTP y, a continuación, seleccione Crear conector SFTP.
3. En la sección Configuración del conector, para el tipo de salida, elija VPC Lattice.

Esta opción enruta el tráfico a través de la VPC mediante Amazon VPC Lattice para el acceso a los recursos entre VPC. Puede usar esta opción para conectarse a puntos finales de servidores alojados de forma privada, enrutar el tráfico a través de los controles de seguridad de su VPC o usar sus propias puertas de enlace NAT y direcciones IP elásticas. La dirección del servidor SFTP remoto se representa como una configuración de recursos en la VPC. Para obtener más información sobre las configuraciones de recursos, consulte [Configuraciones de recursos para recursos de VPC en la Guía](#) del usuario de Amazon VPC Lattice.

4. Complete la configuración del conector:

- Para la función de acceso, elija el nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que se va a utilizar.
- Asegúrese de que este rol proporcione acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`.
- Asegúrese de que este rol dé permiso a `secretsmanager:GetSecretValue` para acceder al secreto.

 Note

En la política, debe especificar el ARN del secreto. El ARN contiene el nombre secreto, pero lo añade con seis caracteres alfanuméricos aleatorios. El ARN de un secreto tiene el siguiente formato.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Asegúrese de que contiene una relación de confianza que permita que el conector tenga acceso a los recursos cuando atienda las solicitudes de transferencia de sus usuarios. Para obtener más información sobre cómo establecer una relación de confianza, consulte [Para establecer una relación de confianza](#).

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

```

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

```

Note

Para el rol de acceso, el ejemplo concede acceso a un único secreto. Sin embargo, puede utilizar un carácter comodín, que puede ahorrarle trabajo si quiere reutilizar el mismo rol de IAM para varios usuarios y secretos. Por ejemplo, la siguiente declaración de recursos concede permisos para todos los secretos cuyos nombres comiencen por `aws/transfer`.


```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

También puede almacenar los secretos que contengan sus credenciales de SFTP en otra Cuenta de AWS. Para obtener más información sobre cómo habilitar el acceso secreto entre cuentas, consulta [Permisos a los AWS Secrets Manager secretos para los usuarios de otra](#) cuenta.

- Para el ARN de configuración de recursos, introduzca el ARN de la configuración de recursos de red de VPC que apunta a su servidor SFTP:

```
arn:aws:vpc-lattice:region:account-id:resourceconfiguration/rcfg-12345678
```

- (Opcional) Para la función de registro, elija la función de IAM para que el conector la utilice para enviar eventos a sus registros. CloudWatch

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

5. En el panel Configuración SFTP, proporcione la siguiente información:

- Para las credenciales de Connector, elija el nombre de un archivo secreto AWS Secrets Manager que contenga la clave privada o la contraseña del usuario de SFTP.

- En el caso de las claves de host confiables, pegue la parte pública de la clave de host que se utiliza para identificar el servidor externo o déjela en blanco para configurarla más adelante mediante el `TestConnection` comando.

Como esta clave de host es para un conector VPC_LATTICE, elimine el nombre de host de la clave

- (Opcional) Para el número máximo de conexiones simultáneas, elija el número de conexiones simultáneas que el conector crea al servidor remoto (el valor predeterminado es 5).
6. En la sección de opciones de algoritmos criptográficos, elija una política de seguridad de la lista desplegable.
 7. (Opcional) En la sección Etiquetas, añada etiquetas como pares clave-valor.
 8. Seleccione Crear conector SFTP para crear el conector SFTP LATTICE-enabled VPC_.

El conector se creará con el estado de PENDING mientras se aprovisiona la asociación de recursos, lo que normalmente tarda varios minutos. Una vez que el estado cambie a ACTIVE, el conector estará listo para su uso.

CLI

Utilice el siguiente comando para crear un conector LATTICE-enabled SFTP VPC_:

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
  --sftp-config UserSecretId=my-secret-id,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  \
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0} \
  --security-policy-name TransferSecurityPolicy-2024-01
```

El parámetro clave para la conectividad de la VPC es `--egress-config` el que especifica el ARN de configuración de recursos que define el destino del servidor SFTP.

Supervisión del estado del conector de VPC

LATTICE-enabled Los conectores VPC_ tienen un proceso de configuración asíncrono. Tras la creación, supervise el estado del conector:

- **PENDIENTE:** Se está aprovisionando el conector. El aprovisionamiento de la red de servicios está en curso, lo que suele tardar varios minutos.
- **ACTIVO:** el conector está listo para su uso y puede transferir archivos.
- **ERROR:** el conector no se pudo aprovisionar. Compruebe los detalles del error para obtener información sobre la solución de problemas.

Compruebe el estado del conector mediante el `describe-connector` comando:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Durante el estado **PENDIENTE**, la `test-connection` API mostrará el mensaje «Conector no disponible» hasta que se complete el aprovisionamiento.

Limitaciones y consideraciones

- **Puntos finales públicos:** al conectarse a puntos finales públicos a través de la VPC, debe proporcionar un nombre DNS en la configuración de recursos. No se admiten las direcciones IP públicas.
- **Disponibilidad regional:** la conectividad de VPC está disponible en una selección. Regiones de AWS Cross-region no se admite el uso compartido de recursos.
- **Requisitos de la zona de disponibilidad:** las pasarelas de recursos deben estar asociadas a subredes de al menos dos zonas de disponibilidad. No todas las zonas de disponibilidad admiten VPC Lattice en todas las regiones.
- **Límites de conexión:** máximo 350 conexiones por recurso con un tiempo de espera de 350 segundos para las conexiones TCP.

Consideraciones sobre costos

No hay cargos adicionales más AWS Transfer Family allá de los cargos de servicio habituales. Sin embargo, los clientes pueden estar sujetos a cargos adicionales por parte de Amazon VPC Lattice relacionados con el uso compartido de sus recursos de Amazon Virtual Private Cloud y a cargos por pasarelas de NAT si utilizan sus propias pasarelas de NAT para acceder a Internet.

[Para obtener información completa sobre AWS Transfer Family los precios, consulte la página de precios.AWS Transfer Family](#)

Ejemplos de conectividad de VPC para conectores SFTP

En esta sección se proporcionan ejemplos de creación de conectores SFTP con conectividad de VPC para varios escenarios. Antes de usar estos ejemplos, asegúrese de haber completado la configuración de la infraestructura de la VPC tal como se describe en la documentación de conectividad de la VPC.

Ejemplo: conexión de punto final privado

En este ejemplo, se muestra cómo crear un conector SFTP que se conecte a un servidor SFTP privado al que solo se pueda acceder desde la VPC.

Requisitos previos

1. Cree una pasarela de recursos en su VPC:

```
aws vpc-lattice create-resource-gateway \  
  --name my-private-server-gateway \  
  --vpc-identifier vpc-1234567890abcdef0 \  
  --subnet-ids subnet-1234567890abcdef0 subnet-0987654321fedcba0
```

2. Cree una configuración de recursos para su servidor SFTP privado:

```
aws vpc-lattice create-resource-configuration \  
  --name my-private-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"} \  
  --port-ranges 22
```

Cree el conector VPC_ LATTICE-enabled

1. Cree el conector SFTP con conectividad de VPC:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-private-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

2. Supervise el estado del conector hasta que se convierta en: ACTIVE

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

El servidor SFTP remoto verá las conexiones procedentes de la dirección IP de Resource Gateway dentro del rango CIDR de la VPC.

Ejemplo: punto final público mediante VPC

En este ejemplo, se muestra cómo enrutar las conexiones a un servidor SFTP público a través de la VPC para aprovechar los controles de seguridad centralizados y utilizar sus propias direcciones IP de NAT Gateway.

Requisitos previos

1. Cree una puerta de enlace de recursos en su VPC (igual que en el ejemplo de un punto final privado).
2. Cree una configuración de recursos para el servidor SFTP público con su nombre DNS:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"} \  
  --port-ranges 22
```

Note

Para los puntos finales públicos, debe usar un nombre DNS, no una dirección IP.

Creación del conector

- Cree el conector SFTP:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-public-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..."
```

```
--egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-0987654321fedcba0,PortNumber=22}
```

El tráfico fluirá desde el conector hasta la puerta de enlace de recursos y, a continuación, a través de la puerta de enlace NAT para llegar al servidor SFTP público. El servidor remoto verá la dirección IP elástica de su puerta de enlace NAT como fuente.

Ejemplo: punto final Cross-account privado

En este ejemplo, se muestra cómo conectarse a un servidor SFTP privado de una AWS cuenta diferente mediante el uso compartido de recursos.

 Note

Si ya ha habilitado el uso compartido de recursos entre VPC mediante otros mecanismos, por ejemplo AWS Transit Gateway, no necesita configurar el uso compartido de recursos que se describe aquí. Los conectores SFTP utilizan automáticamente los mecanismos de enrutamiento existentes, como las tablas de enrutamiento de Transit Gateway. Solo necesita crear una configuración de recursos en la misma cuenta en la que está creando el conector SFTP.

Cuenta A (proveedor de recursos): comparte la configuración de recursos

1. Cree la pasarela de recursos y la configuración de recursos en la cuenta A (igual que en los ejemplos anteriores).
2. Comparta la configuración de recursos con la cuenta B mediante AWS Resource Access Manager:

```
aws ram create-resource-share \  
  --name cross-account-sftp-share \  
  --resource-arns arn:aws:vpc-lattice:us-east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0 \  
  --principals 222222222222
```

Cuenta B (consumidora de recursos): acepta y usa el recurso compartido

1. Acepte la invitación a compartir recursos:

```
aws ram accept-resource-share-invitation \
  --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/invitation-id
```

2. Cree el conector SFTP en la cuenta B:

```
aws transfer create-connector \
  --access-role arn:aws:iam::222222222222:role/TransferConnectorRole \
  --sftp-config UserSecretId=cross-account-server-
credentials,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

El conector de la cuenta B ahora puede acceder al servidor SFTP privado de la cuenta A a través de la configuración de recursos compartidos.

Situaciones comunes de solución de problemas

Estas son las soluciones para los problemas más comunes al crear conectores VPC_LATTICE-enabled :

- Conector bloqueado en estado PENDIENTE: compruebe que su Resource Gateway esté ACTIVA y que tenga subredes en las zonas de disponibilidad compatibles. Si el conector sigue bloqueado con el estado PENDIENTE, llame UpdateConnector con los mismos parámetros de configuración que utilizó inicialmente. Esto desencadena un nuevo evento de estado que podría resolver el problema.
- Tiempos de espera de conexión: compruebe que las reglas del grupo de seguridad permiten el tráfico en el puerto 22 y que el enrutamiento de la VPC es correcto.
- Problemas de resolución de DNS: en el caso de los puntos finales públicos, asegúrese de que su VPC tenga conectividad a Internet a través de una puerta de enlace NAT o una puerta de enlace de Internet.
- Cross-account acceso denegado: compruebe que se acepta el recurso compartido y que el ARN de configuración de recursos es correcto. Si la política de permisos adecuada se adjunta a la configuración del recurso cuando la cuenta de origen crea el recurso compartido, se requieren los siguientes permisos: vpc-lattice:AssociateViaAWSService,, vpc-lattice:AssociateViaAWSService-

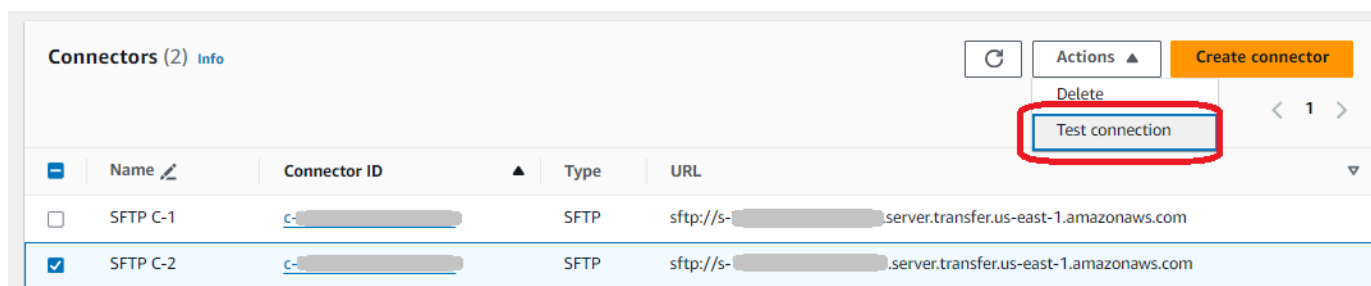
EventsAndStatesvpc-lattice:CreateServiceNetworkResourceAssociation,vpc-lattice:GetResourceConfiguration.

Prueba de un conector SFTP

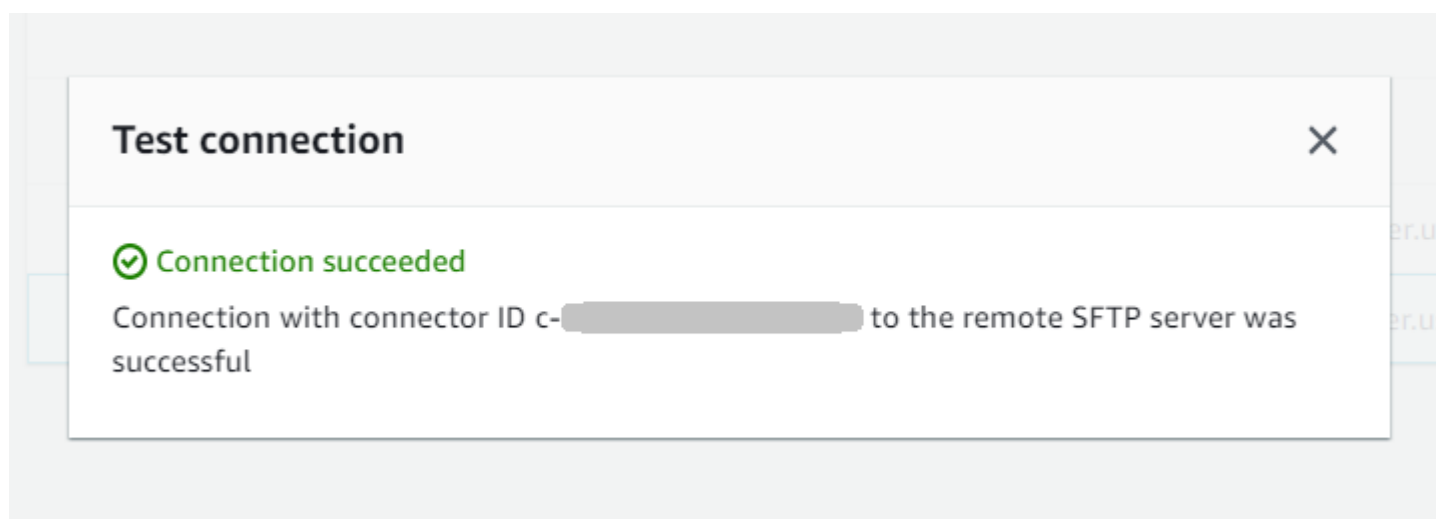
Tras crear un conector SFTP, le recomendamos que lo pruebe antes de intentar transferir cualquier archivo con el nuevo conector.

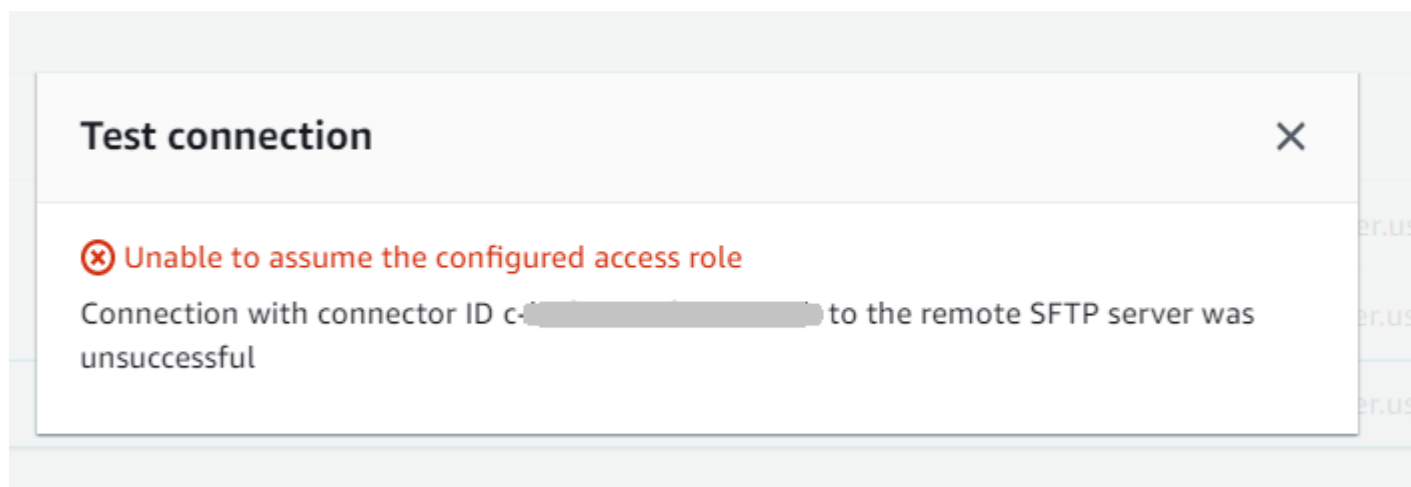
Prueba de un conector SFTP

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>
2. En el panel de navegación izquierdo, elija Conectores SFTP y seleccione un conector.
3. En el menú Acciones, seleccione Evento de prueba.



El sistema devuelve un mensaje que indica si la prueba se supera o no. Si la prueba no es satisfactoria, el sistema muestra un mensaje de error en función del motivo por el que no se ha realizado la prueba.





Note

Para usar la API para probar el conector, consulte la documentación de la API de [TestConnection](#).

Conectividad de VPC para conectores SFTP

AWS Transfer Family Los conectores SFTP admiten la conectividad con servidores SFTP remotos a través de sus entornos de VPC mediante Amazon VPC Lattice. Esto le permite conectarse a servidores SFTP alojados de forma privada o enrutar el tráfico de Internet a través de los controles de seguridad de su VPC y utilizar sus propias puertas de enlace NAT y direcciones IP elásticas.

Tipos de egreso

Los conectores SFTP pueden utilizar uno de los dos tipos de salida:

- Servicio gestionado (predeterminado): el conector utiliza las puertas de enlace NAT y las direcciones IP de su propiedad AWS Transfer Family para enrutar las conexiones a través de la Internet pública.
- VPC_LATTICE: el conector enruta el tráfico a través de su entorno de VPC mediante Resource Access. Cross-VPC

Cuándo usar la conectividad de VPC

Utilice la conectividad de VPC para los conectores SFTP en los siguientes escenarios:

- Servidores SFTP privados: Conéctese a servidores SFTP a los que solo se puede acceder desde su VPC.
- On-premises conectividad: conéctese a servidores SFTP locales a través de conexiones AWS Site-to-Site VPN o Direct AWS Connect.
- Direcciones IP personalizadas: utilice sus propias puertas de enlace NAT y direcciones IP elásticas, incluidos los escenarios de BYOIP.
- Controles de seguridad centralizados: dirija las transferencias de archivos a través de los controles centrales de su organización. ingress/egress

Requisitos

Antes de crear un conector VPC_ LATTICE-enabled SFTP, necesita:

- VPC e infraestructura relacionada (subredes, tablas de enrutamiento, grupos de seguridad)
- Resource Gateway en su VPC (dos zonas de disponibilidad como mínimo)
- Configuración de recursos que especifica el servidor SFTP de destino

Para obtener instrucciones de configuración detalladas, consulte [Cree un conector VPC_ SFTP LATTICE-enabled](#). Y, para ver ejemplos, consulte [Ejemplos de conectividad de VPC para conectores SFTP](#).

Uso de conectores SFTP

En este tema se describe cómo realizar las operaciones de archivos compatibles con el conector SFTP. También puede encontrar ejemplos de comandos para realizar estas operaciones seleccionando los detalles del conector en la AWS Transfer Family consola, en <https://console.aws.amazon.com/transfer/>.

Una vez creado un conector SFTP, puede usarlo para realizar las siguientes operaciones de archivo en el servidor SFTP remoto al que está asociado.

- Envíe archivos desde Amazon S3 al servidor SFTP remoto.
- Recupere archivos del servidor SFTP remoto a Amazon S3.
- Enumere los archivos y subcarpetas de un directorio del servidor SFTP remoto.
- Elimine, cambie el nombre o mueva los archivos y directorios del servidor SFTP remoto.

Para obtener información sobre cómo crear conectores, consulte [Creación de conectores SFTP](#).

Temas

- [Transferencia de archivos](#)
- [Listar el contenido de un directorio remoto](#)
- [Mueva, cambie el nombre o elimine archivos o directorios del servidor remoto](#)

Transferencia de archivos

Temas

- [Enviar y recuperar archivos mediante un conector SFTP](#)

Enviar y recuperar archivos mediante un conector SFTP

Para enviar y recuperar archivos mediante un conector SFTP, utilice la operación [StartFileTransfer](#) API y especifique los siguientes parámetros, en función de si envía archivos (transferencias salientes) o recibe archivos (transferencias entrantes). Ten en cuenta que cada `StartFileTransfer` solicitud puede contener 10 rutas distintas.

Note

De forma predeterminada, los conectores SFTP procesan un archivo a la vez y los transfieren secuencialmente. Tiene la opción de acelerar el rendimiento de las transferencias haciendo que sus conectores creen sesiones simultáneas con servidores remotos que admitan sesiones simultáneas del mismo usuario y procesen hasta 5 archivos en paralelo. Para habilitar las conexiones simultáneas en cualquier conector, puede editar la configuración del número máximo de conexiones simultáneas al crear o actualizar un conector. Para obtener más información, consulte [Cree un conector SFTP con salida gestionada por el servicio](#).

- Transferencias salientes
 - `send-file-paths` contiene de una a diez rutas de archivos de origen, para que los archivos se transfieran al servidor SFTP del socio.
 - `remote-directory-path` es la ruta remota a la que se envía un archivo en el servidor SFTP del cliente.

- **Transferencias entrantes**
 - `retrieve-file-paths` contiene de una a diez rutas remotas. Cada ruta especifica una ubicación para transferir archivos desde el servidor SFTP del socio a su servidor Transfer Family.
 - `local-directory-path` es la ubicación en Amazon S3 (bucket y prefijo opcional) en la que se almacenan los archivos.

Para enviar archivos, debe especificar los parámetros `send-file-paths` y `remote-directory-path`. Puede especificar hasta 10 archivos para el parámetro `send-file-paths`. El siguiente comando de ejemplo envía los archivos denominados `/amzn-s3-demo-source-bucket/file1.txt` y `/amzn-s3-demo-source-bucket/file2.txt`, ubicados en el almacenamiento de Amazon S3, al directorio `/tmp` del servidor SFTP de su socio. Para utilizar este comando de ejemplo, sustituya *amzn-s3-demo-source-bucket* por su propio bucket.

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt /amzn-s3-demo-source-bucket/file2.txt \
--remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

Para recuperar archivos, especifique los parámetros `retrieve-file-paths` y `local-directory-path`. El siguiente ejemplo recupera los archivos `/my/remote/file1.txt` y los guarda `/my/remote/file2.txt` en el servidor SFTP del socio y los coloca en la ubicación `/amzn-s3-demo-bucket/` de Amazon S3. *prefix* Para utilizar este comando de ejemplo, sustituya *user input placeholders* por su propia información.

```
aws transfer start-file-transfer --retrieve-file-paths /my/remote/file1.txt /my/
remote/file2.txt \
--local-directory-path /amzn-s3-demo-bucket/prefix --connector-id
c-2222BBBB3333CCCC4 --region us-east-2
```

Los ejemplos anteriores especifican las rutas absolutas en el servidor SFTP. También puede utilizar rutas relativas, es decir, rutas relativas al directorio de inicio del usuario de SFTP. Por ejemplo, si el usuario de SFTP es `marymajor` y su directorio de inicio en el servidor SFTP es `/users/marymajor/`, el siguiente comando envía `/amzn-s3-demo-source-bucket/file1.txt` a `/users/marymajor/test-connectors/file1.txt`.

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt \
```

```
--remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --  
region us-east-2
```

Listar el contenido de un directorio remoto

Antes de recuperar los archivos de un servidor SFTP remoto, puede recuperar el contenido de un directorio del servidor SFTP remoto. Para ello, utilice la operación [StartDirectoryListing](#) API.

El siguiente ejemplo muestra el contenido de la home carpeta del servidor SFTP remoto, que se especifica en la configuración del conector. Los resultados se colocan en la ubicación `/amzn-s3-demo-bucket/connector-files` de Amazon S3 y en un archivo denominado `c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json`.

```
aws transfer start-directory-listing \\  
  --connector-id c-AAAA1111BBBB2222C \\  
  --output-directory-path /amzn-s3-demo-bucket/example/connector-files \\  
  --remote-directory-path /home
```

Este AWS CLI comando devuelve un identificador de listado y el nombre del archivo que contiene los resultados.

```
{  
  "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",  
  "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"  
}
```

Note

La convención de nomenclatura del archivo de salida es *connector-ID-listing-ID.json*.

El archivo JSON contiene la siguiente información:

- `filePath`: la ruta completa de un archivo remoto, relativa al directorio de la solicitud de listado del conector SFTP en el servidor remoto.
- `modifiedTimestamp`: la última vez que se modificó el archivo, en segundos, en formato de hora universal coordinada (UTC). Este campo es opcional. Si los atributos del archivo remoto no contienen una marca de tiempo, se omite de la lista de archivos.

- **size**: el tamaño del archivo, en bytes. Este campo es opcional. Si los atributos del archivo remoto no contienen un tamaño de archivo, se omite de la lista de archivos.
- **path**: la ruta completa de un directorio remoto, relativa al directorio de la solicitud de listado del conector SFTP del servidor remoto.
- **truncated**: un indicador que indica si el resultado de la lista contiene todos los elementos contenidos en el directorio remoto o no. Si el valor de **truncated** salida es verdadero, puede aumentar el valor proporcionado en el atributo de **max-items** entrada opcional para poder incluir más elementos (hasta el tamaño máximo de lista permitido de 200 000 elementos).

El siguiente es un ejemplo del contenido del archivo de salida (c-
AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json), donde el directorio
remoto contiene dos archivos y dos subdirectorios (rutas).

```
{
  "files": [
    {
      "filePath": "/home/what.txt",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
      "size" : 2323
    },
    {
      "filePath": "/home/how.pgp",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
      "size" : 4691
    }
  ],
  "paths": [
    {
      "path": "/home/magic"
    },
    {
      "path": "/home/aws"
    }
  ],
  "truncated": "false"
}
```

Mueva, cambie el nombre o elimine archivos o directorios del servidor remoto

Temas

- [Mueva o cambie el nombre de los archivos o directorios del servidor SFTP remoto](#)
- [Elimine archivos o directorios del servidor SFTP remoto](#)

Mueva o cambie el nombre de los archivos o directorios del servidor SFTP remoto

Puede utilizar un conector SFTP para mover o cambiar el nombre de los archivos y directorios de un servidor SFTP remoto. Tenga en cuenta que el servidor remoto debe admitir estas operaciones para que el procesamiento mediante conectores se realice correctamente.

Algunos casos de uso comunes son los siguientes.

- Un servidor remoto genera o recibe un archivo nuevo cada hora, con el mismo nombre de archivo pero con una marca de tiempo diferente. Para mantener la carpeta principal actualizada (de forma que solo contenga el archivo más reciente), puede utilizar un conector para mover los archivos más antiguos a una carpeta archivada.
- Se utiliza un conector para enumerar todos los archivos de un directorio remoto y, a continuación, se transfieren todos los archivos al almacenamiento local. A continuación, puede utilizar un conector para mover los archivos a una carpeta archivada en el servidor remoto.

Debe utilizar una `StartRemoteMove` llamada para cada archivo o directorio que desee procesar, ya que el comando utiliza como argumentos un único archivo o directorio de origen y de destino. Sin embargo, puede acelerar el rendimiento haciendo que sus conectores creen sesiones simultáneas con servidores remotos que admitan sesiones simultáneas del mismo usuario y `move/rename` hasta 5 archivos en paralelo.

El siguiente ejemplo mueve un archivo del servidor SFTP remoto de `/source/folder/sourceFile` a `/destination/targetFile` y devuelve un identificador único para la operación.

```
aws transfer --connector-id c-AAAA1111BBBB2222C start-remote-move \  
  --source-path /source/folder/sourceFile --target-path /destination/targetFile
```

 Note

Para las move/rename operaciones, Transfer Family utiliza el SFTP `SSH_FXP_RENAME` comando estándar para realizar la move/rename operación.

Elimine archivos o directorios del servidor SFTP remoto

Puede utilizar un conector SFTP para eliminar archivos o directorios en un servidor SFTP remoto. Tenga en cuenta que el servidor remoto debe admitir estas operaciones para que el procesamiento mediante conectores se realice correctamente.

 Note

Las operaciones de eliminación de directorios remotos solo se admiten en directorios vacíos.

Algunos casos de uso comunes son los siguientes.

- Utiliza un conector para recuperar un archivo de un servidor SFTP remoto, almacenarlo en su bucket de Amazon S3 y, a continuación, cifrarlo. Por último, puede utilizar un conector para eliminar el archivo no cifrado del servidor remoto.
- Utiliza un conector para enumerar todos los archivos de un directorio remoto y, a continuación, los transfiere a su almacenamiento local. A continuación, puede utilizar un conector para eliminar todos los archivos que ha transferido. También puede eliminar el directorio remoto si lo prefiere.

Debe utilizar una `StartRemoteDelete` llamada para cada archivo o directorio que desee eliminar, ya que el comando utiliza un único archivo o directorio como argumento. Sin embargo, puede acelerar el rendimiento haciendo que sus conectores creen sesiones simultáneas con servidores remotos que admitan sesiones simultáneas del mismo usuario y eliminen hasta 5 en files/directories paralelo.

En el siguiente ejemplo, se elimina un archivo del servidor SFTP remoto de la ruta `/delete/folder/deleteFile` y se devuelve un identificador único para la operación.

```
aws transfer start-remote-delete --connector-id c-AAAA1111BBBB2222C \  
--delete-path /delete/folder/deleteFile
```


 Note

Para la operación de eliminación, Transfer Family utiliza el SSH_FXP_REMOVE comando estándar para eliminar un archivo y SSH_FXP_RMDIR un directorio.

Supervisión de conectores SFTP

Puede supervisar el estado de las operaciones del conector mediante cualquiera de las siguientes formas. Elija el enfoque que se adapte a sus necesidades.

Utilice la API del conector para consultar el estado de las solicitudes de transferencia de archivos

Para realizar un seguimiento del progreso de una operación de transferencia de archivos, se utiliza la operación de [ListFileTransferResults](#) API, que devuelve actualizaciones en tiempo real e información detallada sobre el estado de cada archivo individual que se está transfiriendo en una operación de transferencia de archivos específica. Para especificar la transferencia de archivos, proporcione su ID de conector y su ID de transferencia. El siguiente ejemplo devuelve una lista de archivos para el ID del conector a-11112222333344444 y el ID de transferenciaaaa1b2c3d4-5678-90ab-cdef-EXAMPLE11111.

```
aws transfer list-file-transfer-results --connector-id a-11112222333344444 --transfer-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

 Note

Los resultados de la transferencia de archivos están disponibles hasta 7 días después de la llamada a la operación de la ListFileTransferResults API.

También puedes ver los registros y eventos de tus solicitudes de transferencia de archivos que utilizan conectores SFTP. EventBridge Los eventos de Amazon para Transfer Family se describen en [Eventos del conector SFTP](#). Para obtener información sobre cómo ver las entradas del CloudWatch registro de Transfer Family, consulte [Visualización de las transmisiones de registros de Transfer Family](#).

Ver los eventos del conector SFTP en Amazon EventBridge

Para cada operación realizada por los conectores SFTP, Transfer Family genera y envía eventos automáticamente al bus de eventos predeterminado de tu EventBridge cuenta de Amazon. Los eventos contienen metadatos detallados sobre la operación, incluido el estado de la operación. Puede suscribirse a estos eventos en EventBridge, aplicar filtros según criterios de eventos específicos, como el estado de la operación, y activar automáticamente acciones posteriores en función del estado. Para obtener más información sobre los eventos generados por las operaciones del conector SFTP, consulte. [Eventos del conector SFTP](#)

Ver los registros del conector SFTP en Amazon CloudWatch

Todas las operaciones del conector SFTP generan registros detallados. CloudWatch Para ver, por ejemplo, las entradas de registro generadas por los conectores SFTP, consulte. [Ejemplos de entradas de registro para conectores SFTP](#)

Monitorización de conectores de tipo salida de VPC

Los conectores de tipo salida de VPC proporcionan capacidades y consideraciones de monitoreo adicionales más allá de los conectores gestionados por servicio estándar:

Supervisión del estado de los conectores

Los conectores VPC_LATTICE incluyen información adicional para ayudarle a supervisar el aprovisionamiento y el estado operativo:

- EgressType campo: Muestra VPC los conectores de tipo salida VPC_LATTICE
- EgressConfig campo: contiene el ARN de la configuración del recurso y la información del puerto

Supervise el estado del conector mediante la `describe-connector` API:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Monitorización de costes de VPC Lattice

Los conectores de tipo salida de VPC incurren en cargos de celosía de VPC adicionales que debe monitorear:

- Cargos del proveedor de recursos: se le facturan 0\$. 006/GB para el procesamiento de datos como proveedor de recursos (facturado directamente por VPC Lattice)
- Cargos por consumo de recursos: AWS Transfer Family absorbe los 0 dólares. 01/GB costos por consumo de recursos (primer 1 PB)
- Cargos de NAT Gateway: en el caso de los puntos finales públicos a los que se accede mediante VPC, se pueden aplicar cargos adicionales por transferencia de datos y pasarelas NAT
- Cargos de Transfer Family: 0 dólares estándar. 40/GB Se siguen aplicando las tarifas de procesamiento de datos

Supervise el uso y los costos de VPC Lattice a través de la consola de AWS costos y facturación, filtrando por el servicio VPC Lattice.

Supervisión de red para conectores de VPC

Supervise la actividad y el rendimiento de la red para los conectores de tipo salida de VPC:

- Registros de flujo de VPC: habilite los registros de flujo de VPC para monitorear los patrones de tráfico de red entre Resource Gateways y servidores SFTP
- Registros de acceso de VPC Lattice: VPC Lattice proporciona registros de acceso que muestran las direcciones source/destination IP, el tiempo de conexión y los volúmenes de transferencia de datos
- Supervisión de los grupos de seguridad: supervise las reglas y los patrones de tráfico de los grupos de seguridad para garantizar los controles de acceso a la red adecuados
- Supervisión de la resolución del DNS: supervise los tiempos y los fallos de resolución del DNS en los puntos finales de la red de servicio

Ejemplo de entrada de registro de acceso a VPC Lattice:

```
{
  "eventTimestamp": "2025-01-16T20:59:08.531Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-1:123456789012:servicenetwork/sn-1234567890abcdef0",
  "sourceVpcArn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-12345678",
  "resourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-12345678",
  "protocol": "tcp",
  "sourceIpPort": "10.0.1.100:33760",
```

```
"destinationIpPort": "10.0.2.200:22",  
"gatewayIpPort": "10.0.1.150:1769",  
"resourceIpPort": "10.0.2.200:22"  
}
```

Solución de problemas mediante la supervisión

Utilice los datos de supervisión para solucionar problemas comunes de los conectores de VPC:

- Estado PENDIENTE: supervisa el progreso de la resolución del DNS y espera al estado ACTIVO antes de intentar realizar las transferencias
- Tiempos de espera de conexión: compruebe los registros de flujo de la VPC y las reglas del grupo de seguridad para ver si hay tráfico bloqueado en el puerto 22
- Fallos de transferencia: revise CloudWatch los registros para ver los mensajes de error detallados y los registros de acceso de VPC Lattice para detectar problemas a nivel de red
- Problemas de rendimiento: supervise los registros de acceso de VPC Lattice para conocer el tiempo de conexión y las métricas de rendimiento

Administración de conectores SFTP

En este tema se describe cómo ver y actualizar los conectores SFTP.

Note

A cada conector se le asignan automáticamente direcciones IP estáticas que permanecen inalteradas durante la vida útil del conector. Esto le permite conectarse con servidores SFTP remotos que solo aceptan conexiones entrantes desde direcciones IP conocidas. A sus conectores se les asigna un conjunto de direcciones IP estáticas que comparten todos los conectores que utilizan el mismo protocolo (SFTP o AS2) que el suyo. Cuenta de AWS Estas direcciones no están dedicadas exclusivamente a su cuenta.

Si necesita direcciones IP dedicadas y predecibles, configure sus conectores con VPC-based salida. Para obtener más información, consulte [the section called “Cree un conector SFTP con salida VPC-based”](#).

Actualizar conectores SFTP

Para cambiar los valores de los parámetros existentes de los conectores, puede ejecutar el comando `update-connector`. El siguiente comando actualiza el secreto del conector *connector-id*, en la región *region-id* a *secret-ARN*. Para utilizar este comando de ejemplo, sustituya *user input placeholders* por su propia información.

```
aws transfer update-connector --sftp-config '{"UserSecretId":"secret-ARN"}' \
  --connector-id connector-id --region region-id
```

Actualización de la configuración de conectividad de la VPC

Puede actualizar la configuración de conectividad de la VPC para los conectores existentes, lo que incluye cambiar entre los tipos de salida de VPC y gestionados por el servicio o cambiar el ARN de la configuración de recursos.

Para cambiar un conector de servicio gestionado a uno de salida de VPC:

```
aws transfer update-connector \
  --connector-id connector-id \
  --egress-type VPC \
  --egress-config ResourceConfigurationArn=resource-configuration-arn
```

Para actualizar el ARN de configuración de recursos de un conector LATTICE-enabled VPC_:

```
aws transfer update-connector \
  --connector-id connector-id \
  --egress-config ResourceConfigurationArn=new-resource-configuration-arn
```

Note

Al actualizar la configuración de conectividad de la VPC, el estado del conector cambiará a PENDING durante el proceso de reconfiguración. Supervise el estado del conector mediante el `describe-connector` comando.

Ver los detalles del conector SFTP

Puede encontrar una lista de detalles y propiedades de un conector SFTP en la consola AWS Transfer Family .

Visualización de los detalles del conector

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Connectors (Conectores).
3. Elija el identificador en la columna ID del conector para ver la página de detalles del conector seleccionado.

Puede cambiar las propiedades del conector SFTP seleccionando Editar en la página de detalles del conector.

Supervisión del estado del conector de VPC

LATTICE-enabled Los conectores VPC_ incluyen información de estado adicional para ayudarle a supervisar el proceso de aprovisionamiento:

- Estado: muestra PENDING, o ACTIVE ERROR
- EgressType: Muestra VPC o SERVICE_MANAGED
- EgressConfig: Contiene el ARN de configuración de recursos para los conectores de VPC
- Error: proporciona información detallada sobre los errores si el conector está en ese estado ERROR

En el caso de los conectores de VPC, el ServiceManagedEgressIpAddresses campo será nulo, ya que el tráfico utilizará las direcciones IP de la VPC en su lugar.

Note

Puede obtener gran parte de esta información, aunque en un formato diferente, ejecutando el siguiente comando AWS Command Line Interface (AWS CLI). Para utilizar este comando de ejemplo, sustituya *user input placeholders* por su propia información.

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

Para obtener más información, consulte [DescribeConnector](#) en la referencia de la API.

Escalado y cuotas para los conectores SFTP

Temas

- [Cuotas para conectores SFTP](#)
- [Escalar sus conectores SFTP](#)

Cuotas para conectores SFTP

Existen las siguientes cuotas para los conectores SFTP.

Note

Se muestran más cuotas de servicio para los conectores SFTP en los [AWS Transfer Family puntos finales y las cuotas](#) en. Referencia general de Amazon Web Services

Cuotas de conectores SFTP

Name	Predeterminado	Ajustable
Máximo de transacciones de conexión de prueba por segundo (TPS)	1 solicitud por segundo por cuenta	No
Tamaño máximo de cola para las transferencias de archivos pendientes	1 000	No
Tamaño máximo de archivo	150 gibibytes (GiB)	No
Tiempo máximo de transferencia por archivo	12 horas	No

Name	Predeterminado	Ajustable
Tiempo máximo de espera de solicitudes por archivo	12 horas	No
Ancho de banda máximo para los conectores por cuenta (los conectores SFTP y AS2 contribuyen a este valor)	50 MBps	No
Número máximo de elementos para las operaciones de listado de directorios	200.000	No

Note

De forma predeterminada, los conectores SFTP procesan un archivo a la vez y los transfieren secuencialmente. Tiene la opción de acelerar el rendimiento de las transferencias haciendo que sus conectores creen sesiones simultáneas con servidores remotos que admitan sesiones simultáneas del mismo usuario y procesen hasta 5 archivos en paralelo. Para habilitar las conexiones simultáneas en cualquier conector, puede editar la configuración del número máximo de conexiones simultáneas al crear o actualizar un conector. Para obtener más información, consulte [Cree un conector SFTP con salida gestionada por el servicio](#).

Para almacenar las credenciales de los conectores SFTP, hay cuotas asociadas a cada secreto de Secrets Manager. Si usa el mismo secreto para almacenar varios tipos de claves y para varios propósitos, es posible que encuentre estas cuotas.

- Longitud total de un único secreto: 12 000 caracteres
- Longitud máxima de la **Password** cadena: 1024 caracteres
- Longitud máxima de la **PrivateKey** cadena: 8192 caracteres
- Longitud máxima de la **Username** cadena: 100 caracteres

Escalar sus conectores SFTP

En esta sección se describen las consideraciones sobre cómo escalar las cargas de trabajo de los conectores AWS Transfer Family SFTP. Debe tener en cuenta las tres cuotas siguientes que se aplican cuando desee escalar sus cargas de trabajo con conectores SFTP.

- El tamaño máximo de la cola. Se refiere al número máximo de operaciones pendientes solicitadas en la cola de un conector. Una operación pendiente se refiere a cualquier solicitud de transferencia enviada anteriormente que aún no se haya completado, ya sea con éxito o sin éxito.

La profundidad máxima de cola para las solicitudes pendientes se establece actualmente en 1000 por conector (según se define en [las cuotas de AWS Transfer Family servicio](#)). Sus cargas de trabajo pueden superar este límite de servicio si solicita miles de operaciones de transferencia durante un período breve, y recibirá un mensaje `ThrottlingException` con el mensaje Se ha superado el máximo de solicitudes pendientes. Si sus cargas de trabajo están sujetas a esta cuota, póngase en contacto con el equipo de servicio de Transfer Family a través AWS Support de su equipo de cuentas para analizar sus requisitos de escalabilidad.

También puedes realizar una de las siguientes acciones o ambas.

- Distribuya los volúmenes de archivos en varios conectores.
- Haga que sus conectores creen sesiones simultáneas con el servidor remoto para procesar varias solicitudes de la cola en paralelo.
- El número de sesiones simultáneas. De forma predeterminada, un conector SFTP transfiere un archivo a la vez, transfiriendo los archivos secuencialmente desde su cola.

Tiene la opción de acelerar el rendimiento de la transferencia haciendo que sus conectores transfieran varios archivos en paralelo. Puede crear sesiones simultáneas con servidores remotos que admitan sesiones simultáneas del mismo usuario y procesar hasta 5 archivos en paralelo. Al crear un conector SFTP, elija un valor de hasta 5 para la configuración Máximo de conexiones simultáneas al crear o actualizar el conector. Para obtener más información, consulte [Cree un conector SFTP con salida gestionada por el servicio](#).

- La tasa de solicitudes. **StartFileTransfer** Puede solicitar hasta 100 rutas de archivos por segundo para su transferencia con cada conector SFTP. Las rutas de archivo solicitadas se añaden a la cola de sus conectores para su procesamiento. Puede utilizar el `StartFileTransfer` comando de forma recursiva para solicitar hasta 100 rutas de archivos por segundo por conector, independientemente del número de archivos que se proporcione en un comando individual. `StartFileTransfer`

Arquitecturas de referencia que utilizan conectores SFTP

En esta sección se enumeran los materiales de referencia disponibles para configurar los flujos de trabajo de transferencia automática de archivos mediante conectores SFTP. Puede diseñar sus propias arquitecturas basadas en eventos mediante el conector SFTP de Amazon EventBridge, para organizar entre la acción de transferencia de archivos y las acciones previas y posteriores al procesamiento. AWS

Publicaciones de blog

La siguiente entrada del blog proporciona una arquitectura de referencia para crear un flujo de trabajo de MFT con conectores SFTP, que incluye el cifrado de archivos mediante PGP antes de enviarlos a un servidor SFTP remoto mediante conectores SFTP: [diseñar transferencias de archivos gestionadas seguras y compatibles con conectores SFTP y cifrado PGP](#). AWS Transfer Family

Talleres

- El siguiente taller ofrece laboratorios prácticos para configurar los conectores SFTP y usar los conectores para enviar o recuperar archivos de servidores SFTP remotos: [Transfer Family: taller de SFTP](#).
- [El siguiente taller ofrece laboratorios prácticos para crear flujos de trabajo totalmente automatizados y basados en eventos que implican la transferencia de archivos hacia o desde servidores SFTP externos a Amazon S3, y el procesamiento previo y posterior común de esos archivos: taller de MFT. Event-driven](#)

Este vídeo ofrece un recorrido por este taller.

Soluciones

AWS Transfer Family ofrece las siguientes soluciones:

- La [solución de sincronización de transferencias de archivos](#) proporciona una arquitectura de referencia para automatizar el proceso de sincronización de directorios SFTP remotos (incluidas estructuras de carpetas completas) con los buckets locales de Amazon S3 mediante un conector SFTP. Organiza el proceso de enumerar los directorios remotos, detectar cambios y transferir archivos nuevos o modificados.

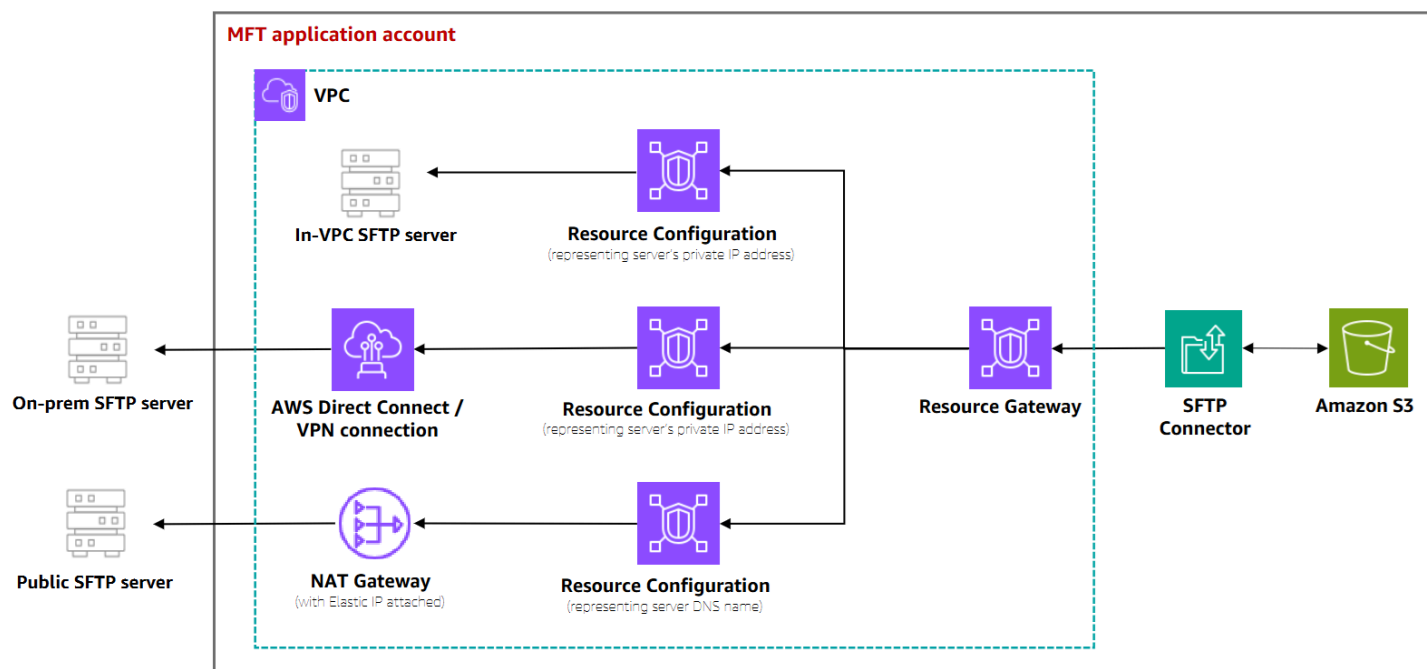
- [Serverlessland: transferencia selectiva de archivos entre un servidor SFTP remoto y S3; su uso AWS Transfer Family](#) proporciona un patrón de muestra para enumerar los archivos almacenados en ubicaciones SFTP remotas y transferir archivos selectivos a Amazon S3.

Arquitecturas de referencia de VPC

Las siguientes arquitecturas de referencia muestran patrones comunes para implementar conectores LATTICE-enabled VPC_ SFTP. Estos ejemplos le ayudan a comprender dónde deben crearse los recursos de VPC Lattice en su arquitectura general. AWS

Cuenta única con infraestructura de salida compartida

En esta arquitectura, la infraestructura de salida (puerta de enlace NAT, túnel VPN o Direct Connect) se configura en una VPC dentro de la misma cuenta que los conectores SFTP. Todos los conectores pueden compartir la misma puerta de enlace de recursos y la misma puerta de enlace NAT.

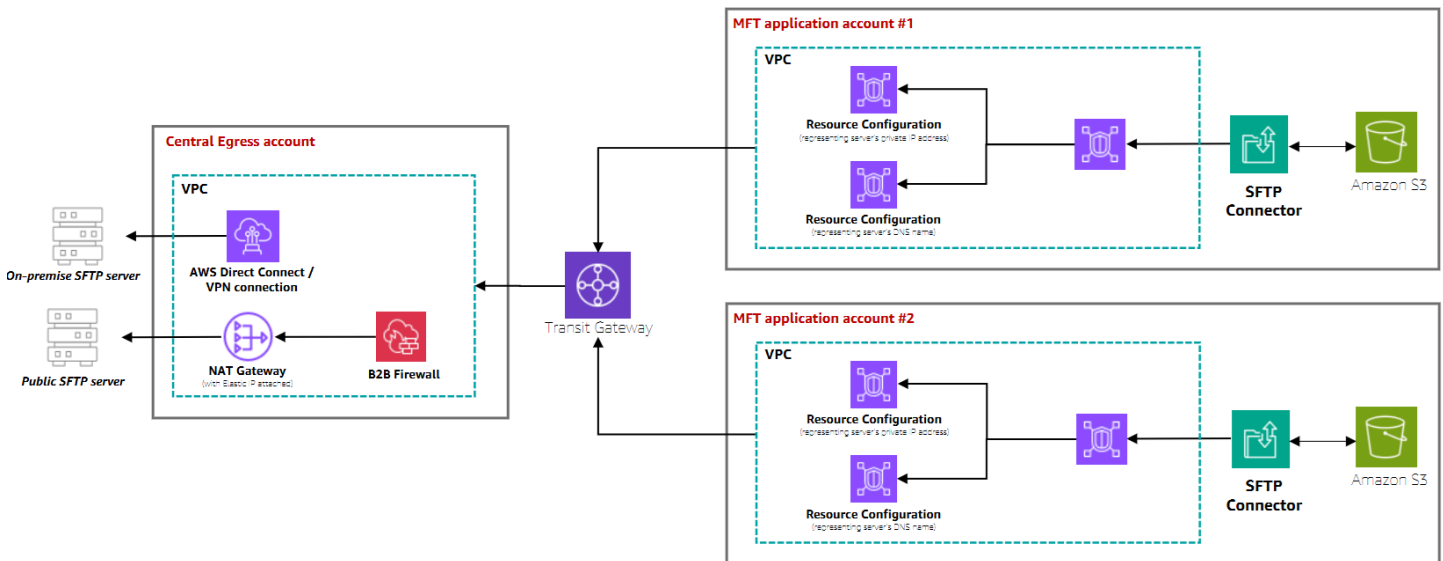


Este patrón es ideal cuando:

- Todos los conectores SFTP se administran en un solo conector Cuenta de AWS
- La infraestructura de salida se configura en una VPC dentro de la misma cuenta que los conectores SFTP.

Cross-account con una infraestructura de salida centralizada

En esta arquitectura, la infraestructura de salida (puerta de enlace NAT, túnel VPN, Direct Connect o firewalls B2B) se configura en una cuenta de salida central administrada por el equipo de redes. Los conectores SFTP se crean en la cuenta de la aplicación MFT administrada por el equipo de administración de MFT. Cross-account la creación de redes se establece mediante Transit Gateway para cumplir con las normas de red existentes.



Este patrón es ideal cuando:

- La infraestructura de red la administra un equipo independiente en una cuenta dedicada
- Tiene rutas existentes (por ejemplo AWS Transit Gateway) entre la cuenta en la que se crean los conectores SFTP y la cuenta en la que se configura la infraestructura de salida. Los conectores SFTP podrán aprovechar las rutas existentes que conectan las dos cuentas.
- Se requieren controles de seguridad centralizados y firewalls B2B
- Debe mantener la separación de funciones entre los equipos de redes y aplicaciones

AWS Transfer Family para AS2

La declaración de aplicabilidad 2 (AS2) es una especificación de RFC-definida transmisión de archivos que incluye sólidos mecanismos de verificación y protección de mensajes. La protección de una carga útil AS2 en tránsito utiliza la sintaxis de mensajes criptográficos (CMS) con cifrado y firmas digitales para proporcionar protección de datos y autenticación por pares. Una carga útil de respuesta a un aviso de disposición de mensajes (MDN) firmada permite comprobar (sin repudiar) que el mensaje se ha recibido y se ha descifrado correctamente.

El protocolo AS2 es fundamental para los flujos de trabajo con requisitos de conformidad que dependen de contar con funciones de seguridad y protección de datos integradas en el protocolo. AWS Transfer Family Los terminales AS2 cuentan con la [certificación de Drummond](#), lo que permite a los clientes de sectores como el comercio minorista, las ciencias de la vida, la fabricación, los servicios financieros y los servicios públicos realizar transacciones de forma segura con sus socios comerciales.

Cuando se utiliza AS2 con Transfer Family, se puede acceder de forma nativa a los datos de la transacción en: AWS

- Procesamiento, análisis y aprendizaje automático
- Integración con los sistemas de planificación de recursos empresariales (ERP)
- Integración con los sistemas de gestión de relaciones con los clientes (CRM)

Para intercambiar archivos con un socio que tenga un AS2-enabled servidor, debe:

- Generar un key pair de claves público-privadas para el cifrado
- Generar un key pair de claves público-privadas para firmar
- Intercambia las claves públicas con tu pareja

Important

Actualmente no se admiten los puntos de conexión del servidor HTTPS AS2. Usted es responsable de la rescisión del TLS.

Transfer Family ofrece un taller al que puede asistir, en el que puede configurar un terminal Transfer Family con AS2 activado y un conector Transfer Family AS2. Puede ver los detalles de este taller [aquí](#).

Para obtener instrucciones paso a paso para configurar AS2 en Transfer Family, consulte lo siguiente:

1. [Importar certificados AS2](#)
2. [Creación de perfiles de AS2](#)
3. [Crear un servidor AS2](#)
4. [Cree un acuerdo AS2](#)
5. [Configure los conectores AS2](#)

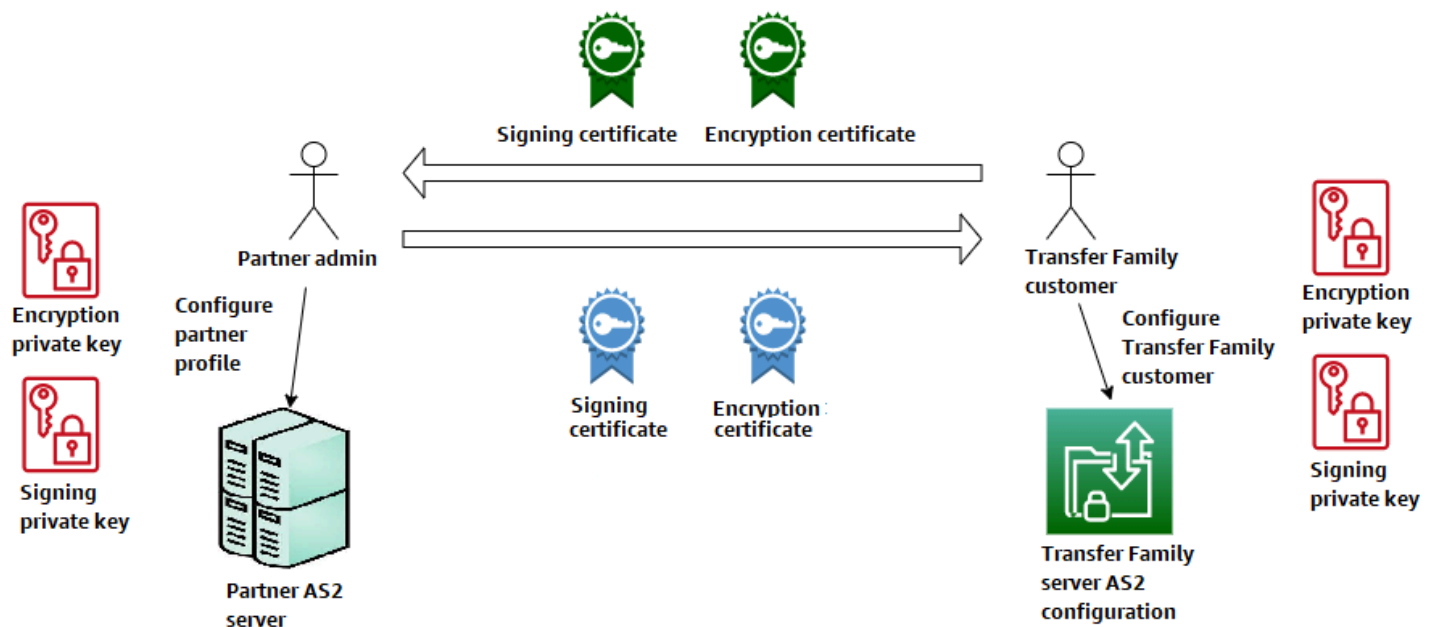
Para ver un ejemplo completo, consulte [Configuración de una configuración AS2](#).

Note

Para mostrar la compatibilidad con las plantillas de Terraform de AS2, añada una reacción de aprobación (#) a la solicitud de funciones de plantillas [Terraform de Transfer Family](#). También puedes añadir un comentario que describa tu caso de uso.

Casos de uso de AS2

Si es un AWS Transfer Family cliente que desea intercambiar archivos con un socio que tiene un AS2-enabled servidor, la parte más compleja de la configuración consiste en generar un par de claves público-privadas para el cifrado y otro para firmar e intercambiar las claves públicas con el socio.



Tenga en cuenta las siguientes variantes para su uso AWS Transfer Family con el AS2.

Note

El socio comercial es el socio asociado a ese perfil de socio.
En todas las menciones de MDN en la siguiente tabla se presupone que los MDN están firmados.

Casos de uso de AS2

Inbound-only casos de uso

- Transfiera mensajes AS2 cifrados de un socio comercial a un servidor de Transfer Family.

En este caso, haga lo siguiente:

1. Cree perfiles para su socio comercial y para usted.
2. Cree un servidor Transfer Family que utilice el protocolo AS2.
3. Cree un acuerdo y agregarlo a su servidor.
4. Importe un certificado con una clave privada y agréguelo a su perfil y, a continuación, importe la clave pública al perfil de su socio para cifrarlo.
5. Una vez tenga estos elementos, envíe la clave pública de su certificado a su socio comercial.

Ahora su socio puede enviarle mensajes cifrados y usted puede descifrarlos y almacenarlos en su bucket de Amazon S3.

- Transfiera mensajes AS2 cifrados de un socio comercial a un servidor de Transfer Family y añada firmas.

En este escenario, sigue realizando solo transferencias entrantes, pero ahora quiere que su socio firme los mensajes que envía. En este caso, importe la clave pública de firma del socio comercial (como un certificado de firma añadido al perfil de su socio).

- Transfiere mensajes AS2 cifrados de un socio comercial a un servidor de Transfer Family y añade la firma y el envío de una respuesta de MDN.

En este escenario, sigue realizando únicamente transferencias entrantes, pero ahora, además de recibir cargas útiles firmadas, su socio comercial quiere recibir una respuesta MDN firmada.

1. Importe sus claves de firma públicas y privadas (como un certificado de firma para su perfil).
2. Envía la clave de firma pública a tu socio comercial.

Outbound-only casos de uso

- Transfiera mensajes AS2 cifrados desde un servidor de Transfer Family a un socio comercial.

Este caso es similar al caso de uso de transferencias solo entrantes, excepto que en lugar de añadir un acuerdo al servidor AS2, se crea un conector. En este caso, importas la clave pública de tu socio comercial a su perfil.

- Transfiera mensajes AS2 cifrados de un servidor de Transfer Family a un socio comercial y añada firmas.

Sigues realizando únicamente transferencias salientes, pero ahora tu socio comercial quiere que firmes el mensaje que le envías.

1. Importe su clave privada de firma (como un certificado de firma agregado a su perfil).
2. Envíe a su socio comercial su clave pública.

- Transfiere mensajes AS2 cifrados desde un servidor de Transfer Family a un socio comercial, añade firmas y envía una respuesta de MDN.

Sigues realizando únicamente transferencias salientes, pero ahora, además de enviar cargas útiles firmadas, quieres recibir una respuesta de MDN firmada de tu socio comercial.

1. Tu socio comercial te envía su clave de firma pública.
2. Importe la clave pública de su socio comercial (como un certificado de firma añadido a su perfil de socio).

Casos de uso entrantes y salientes

- Transfiera mensajes AS2 cifrados en ambas direcciones entre un servidor Transfer Family y un socio comercial.

En este caso, haga lo siguiente:

1. Cree perfiles para su socio comercial y para usted.
2. Cree un servidor Transfer Family que utilice el protocolo AS2.
3. Cree un acuerdo y agregarlo a su servidor.
4. Cree un conector.
5. Importe un certificado con una clave privada y agréguelo a su perfil y, a continuación, importe la clave pública al perfil de su socio para cifrarlo.
6. Reciba una clave pública de su socio comercial y agréguela a su perfil para cifrarla.
7. Una vez tenga estos elementos, envíe la clave pública de su certificado a su socio comercial.

Ahora usted y su socio comercial pueden intercambiar mensajes cifrados, y ambos pueden descifrarlos. Puede almacenar los mensajes que recibe en su bucket de Amazon S3 y su socio puede descifrar y almacenar los mensajes que le envíe.

- Transfiera mensajes AS2 cifrados en ambas direcciones entre un servidor Transfer Family y un socio comercial y añada firmas.

Ahora usted y su socio quieren mensajes firmados.

1. Importe su clave privada de firma (como un certificado de firma agregado a su perfil).
 2. Envía tu clave pública a tu socio comercial.
 3. Importe la clave pública de firma de su socio comercial y agréguela a su perfil.
- Transfiera mensajes AS2 cifrados en ambas direcciones entre un servidor Transfer Family y un socio comercial, añada firmas y envíe una respuesta de MDN.

Ahora quieres intercambiar cargas útiles firmadas, y tanto tú como tu socio comercial queréis respuestas en MDN.

1. Tu socio comercial te envía su clave de firma pública.
2. Importe la clave pública de su socio comercial (como certificado de firma a su perfil de socio).
3. Envíe su clave pública a su socio comercial.

Plantillas AS2 CloudFormation

En este tema se proporciona información sobre AWS CloudFormation las plantillas que puede utilizar para implementar rápidamente servidores y configuraciones AS2. AWS Transfer Family Estas plantillas automatizan el proceso de configuración y ayudan a implementar las mejores prácticas para las transferencias de archivos AS2.

- La plantilla AS2 básica se describe en [Uso de una plantilla para crear una pila AS2 de Transfer Family de demostración](#)
- La plantilla AS2 para personalizar los encabezados HTTP se describe en. [Personalice los encabezados HTTP para los mensajes AS2](#)

Personalización de plantillas AS2

Puede personalizar las plantillas proporcionadas para que se ajusten a sus requisitos específicos:

1. Descarga la plantilla desde la URL de S3.
2. Modifique el código YAML para ajustar configuraciones como:
 - Ajustes de seguridad y configuraciones de certificados
 - Arquitectura de red y configuración de VPC
 - Opciones de almacenamiento y manejo de archivos
 - Preferencias de supervisión y notificación
3. Cargue la plantilla modificada en su propio bucket de S3.
4. Implemente la plantilla personalizada mediante la CloudFormation consola o AWS CLI.

Important

Al personalizar las plantillas, asegúrese de mantener las dependencias entre los recursos y de seguir las prácticas recomendadas de seguridad.

Probar su implementación de AS2

Tras implementar un servidor AS2 mediante una plantilla, puede probar la configuración:

1. Consulte los resultados de la CloudFormation pila para ver ejemplos de comandos e información sobre los puntos finales.
2. Utilice el AWS CLI para enviar un archivo de prueba:

```
aws s3api put-object --bucket your-bucket-name --key test.txt --body test.txt  
aws transfer start-file-transfer --connector-id your-connector-id --send-file-  
paths /your-bucket-name/test.txt
```

3. Verifique la entrega del archivo en el depósito S3 de destino.
4. Compruebe CloudWatch los registros para ver si el procesamiento es correcto y si las respuestas de MDN son correctas.

Para realizar pruebas más exhaustivas, considere la posibilidad de utilizar clientes AS2 de terceros para enviar archivos a su servidor AS2 de Transfer Family.

Mejores prácticas para el despliegue de plantillas AS2

Siga estas prácticas recomendadas cuando utilice plantillas AS2: CloudFormation

Seguridad

Utilice certificados seguros y cámbielos periódicamente.

Implemente políticas de IAM con privilegios mínimos.

Restrinja el acceso a la red mediante grupos de seguridad.

Fiabilidad

Implemente en varias zonas de disponibilidad.

Implemente la supervisión y las alertas en caso de transferencias fallidas.

Configura reintentos automatizados para las transferencias fallidas.

Desempeño

Elige los tipos de instancia adecuados para tu volumen de transferencias.

Implemente políticas de ciclo de vida de S3 para una administración de archivos eficiente.

Supervise y optimice las configuraciones de red.

Optimización de costes

Usa el autoscalamiento para cargas de trabajo variables.

Implemente clases de almacenamiento S3 para archivos antiguos.

Supervise y ajuste los recursos en función del uso real.

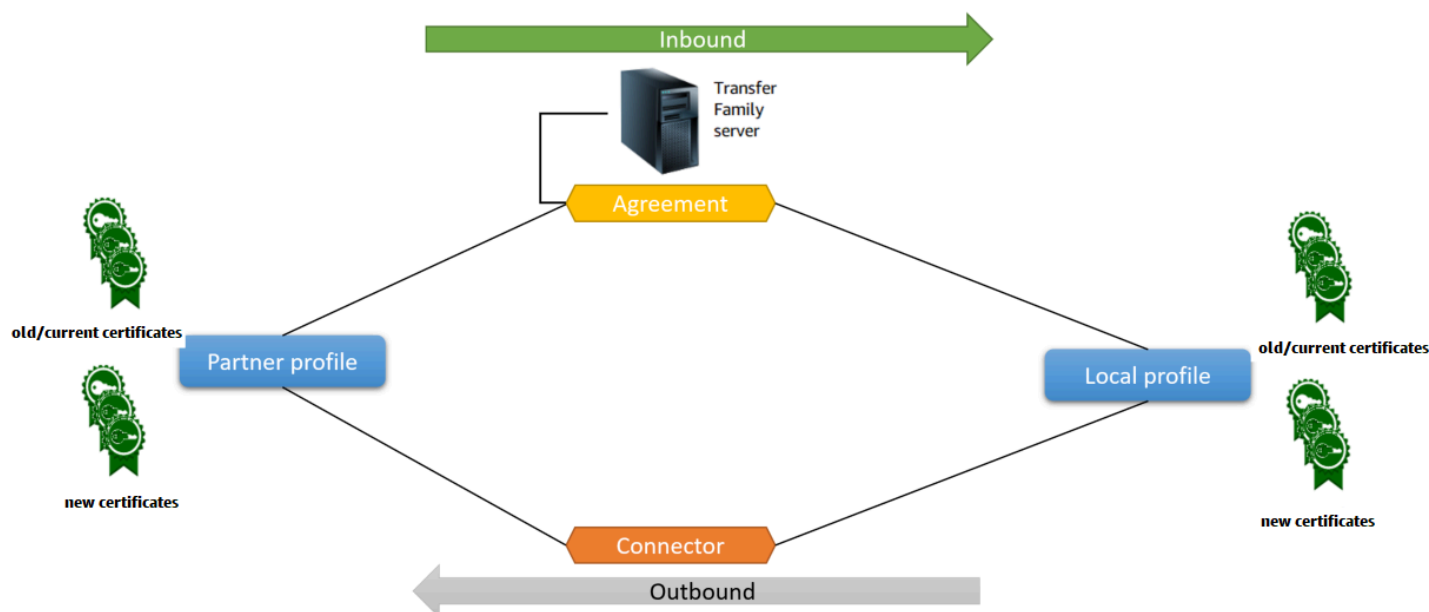
Configuración de AS2

Para crear un AS2-enabled servidor, también debe especificar los siguientes componentes:

- **Acuerdos:** los acuerdos bilaterales con socios comerciales o asociaciones definen la relación entre las dos partes que intercambian mensajes (archivos). Para definir un acuerdo, Transfer Family combina un servidor, un perfil local, un perfil de socio, un certificado y otros atributos. Transfer Family AS2-inbound procesa acuerdos de uso.
- **Certificados:** los certificados de clave pública (X.509) se utilizan en la comunicación AS2 para el cifrado y la verificación de los mensajes. Los certificados también se utilizan para los puntos de conexión de los conectores.
- **Perfiles locales y perfiles de socios:** un perfil local define la organización o «parte» local (servidor AS2-enabled Transfer Family). Del mismo modo, un perfil de socio define la empresa asociada remota, externa a Transfer Family.

Si bien no es obligatorio para todos los AS2-enabled servidores, para las transferencias salientes se necesita un conector. Un conector captura los parámetros de una conexión de salida. El conector es necesario para enviar archivos a un servidor externo, ajeno al AWS servidor, del cliente.

El siguiente diagrama muestra la relación entre los objetos AS2 que participan en los procesos de entrada y salida.



Para obtener un ejemplo integral de una configuración de AS2, consulte [Configuración de una configuración AS2](#).

Temas

- [Configuraciones AS2](#)
- [Cuotas y limitaciones de AS2](#)
- [Características y funciones básicas de AS2](#)

Configuraciones AS2

En este tema, se describen las configuraciones, características y capacidades admitidas para las transferencias que utilizan el protocolo Applicability Statement 2 (AS2), incluidos los cifrados y resúmenes aceptados.

Firma, cifrado, compresión, MDN

Tanto para las transferencias entrantes como para las salientes, los siguientes elementos son obligatorios u opcionales:

- Cifrado: obligatorio (para el transporte HTTP, que es el único método de transporte compatible actualmente). Los mensajes no cifrados solo se aceptan si los reenvía un TLS-terminating proxy, como un Application Load Balancer (ALB), y X-Forwarded-Proto: https el encabezado está presente.

- Firma: opcional
- Compresión: opcional (el único algoritmo de compresión compatible actualmente es ZLIB)
- Aviso de disposición de mensajes (MDN): opcional

Cifrados

Se admiten los siguientes cifrados para las transferencias entrantes y salientes:

- AES128_CBC
- AES192_CBC
- AES256_CBC
- 3DES (solo para compatibilidad con versiones anteriores)

Resúmenes

Se admiten los siguientes resúmenes:

- Firma entrante y MDN: SHA1, SHA256, SHA384, SHA512
- Firma saliente y MDN: SHA1, SHA256, SHA384, SHA512

MDN

Para las respuestas de MDN, se admiten ciertos tipos, como los siguientes:

- Transferencias entrantes: síncronas y asíncronas
- Transferencias salientes: síncronas y asíncronas
- Simple Mail Transfer Protocol (SMTP) (correo electrónico MDN): no se admite.

Transporte

- Transferencias entrantes: HTTP es el único transporte admitido actualmente y debe especificarlo de forma explícita.

Note

Si necesita usar HTTPS para las transferencias entrantes, puede cancelar TLS en un equilibrador de carga de aplicación o un equilibrador de carga de red. Esto se describe en [Recibir mensajes de AS2 a través de HTTPS](#).

- Transferencias salientes: si proporciona una URL HTTP, también debe especificar un algoritmo de cifrado. Si proporciona una dirección HTTPS, tiene la opción de especificar NINGUNA para el algoritmo de cifrado.

Cuotas y limitaciones de AS2

En esta sección, se analizan las cuotas y limitaciones de AS2

Temas

- [Cuotas de AS2](#)
- [Cuotas de manejo de secretos](#)
- [Limitaciones conocidas](#)

Cuotas de AS2

Existen las siguientes cuotas para el AS2 file transfer. Para solicitar un aumento de una cuota ajustable, consulte las [Servicio de AWS cuotas](#) en Referencia general de AWS.

Cuotas de AS2

Name	Predeterminado	Ajustable
Número máximo de archivos por solicitud saliente	10	No
Número máximo de solicitudes salientes por segundo	100	No
Número máximo de solicitudes entrantes por segundo	100	No

Name	Predeterminado	Ajustable
Ancho de banda saliente máximo por cuenta (las solicitudes SFTP y AS2 salientes contribuyen a este valor)	50 MB por segundo	No

Cuotas de manejo de secretos

AWS Transfer Family realiza llamadas AWS Secrets Manager en nombre de los clientes de AS2 que utilizan la autenticación básica. Además, Secrets Manager hace llamadas a AWS KMS.

Note

Estas cuotas no son específicas del uso que hagas de los secretos para Transfer Family: se comparten entre todos tus servicios Cuenta de AWS.

En el caso de Secrets Manager `GetSecretValue`, la cuota que se aplica es la tasa combinada de solicitudes `DescribeSecret` y `GetSecretValue` API, tal y como se describe en [AWS Secrets Manager las cuotas](#).

Secrets Manager **GetSecretValue**

Name	Valor	Description (Descripción)
Tasa combinada de solicitudes <code>DescribeSecret</code> y <code>GetSecretValue</code> de API	Cada región admitida: 10 000 por segundo	El máximo de transacciones por segundo para las operaciones de <code>GetSecretValue</code> API <code>DescribeSecret</code> y las operaciones de API combinadas.

Para AWS KMS ello, se aplican las siguientes cuotas `Decrypt`. Para obtener más información, consulta [Solicitar cuotas para cada operación de la AWS KMS API](#)

AWS KMS **Decrypt**

Nombre de la cuota	Límite predeterminado (solicitudes por segundo)
Cuota de tasas de solicitud de operaciones criptográficas (simétricas)	Estas cuotas compartidas varían según el tipo de AWS KMS clave utilizada en la solicitud Región de AWS y el tipo de clave. Cada cuota se calcula por separado. • 5500 (compartidas) • 10 000 (compartidas) en las siguientes regiones: • EE. UU. Este (Ohio), us-east-2 • Asia Pacífico (Singapur), ap-southeast-1 • Asia Pacífico (Sídney), ap-southeast-2 • Asia Pacífico (Tokio), ap-northeast-1 • Europa (Fráncfort), eu-central-1 • Europa (Londres), eu-west-2 • 50 000 (compartidas) en las siguientes Regiones: • EE.UU. Este (Norte de Virginia) (us-east-1) • EE.UU. Oeste (Oregón) (us-west-2) • Europa (Irlanda), eu-west-1
Cuotas de solicitudes del almacén de claves personalizado  Note Esta cuota solo se aplica si se utiliza un almacén de claves externo.	Las cuotas de solicitudes del almacén de claves personalizado se calculan por separado para cada almacén de claves personalizado. • 1800 (compartidas) por cada almacén de AWS CloudHSM claves • 1800 (compartidas) para cada almacén de claves externo.

Limitaciones conocidas

- Server-side No se admite el protocolo Keep-Alive de TCP. La conexión se agota después de 350 segundos de inactividad, a menos que el cliente envíe paquetes keep-alive.
- Para que el servicio acepte un acuerdo activo y aparezca en los CloudWatch registros de Amazon, los mensajes deben contener encabezados AS2 válidos.
- [El servidor desde el que se reciben los mensajes AWS Transfer Family para el AS2 debe admitir el atributo de protección del algoritmo de sintaxis de mensajes criptográficos \(CMS\) para validar las firmas de los mensajes, tal como se define en el RFC 6211.](#) Este atributo no es compatible con algunos productos anteriores de IBM Sterling.
- Los identificadores de mensaje duplicados dan como resultado un mensaje de documento duplicado. processed/Warning
- La longitud de la clave de los certificados AS2 debe ser de al menos 2048 bits y, como máximo, de 4096.
- Al enviar mensajes AS2 o mDNS asíncronos al punto de conexión HTTPS de un socio comercial, los mensajes o mDNS deben utilizar un certificado SSL válido firmado por una autoridad de certificación (CA) de confianza pública. Self-signed Actualmente, los certificados solo se admiten para transferencias salientes.
- El punto de conexión debe ser compatible con el protocolo TLS de la versión 1.2 y con un algoritmo criptográfico permitido por la política de seguridad (tal y como se describe en [Políticas de seguridad para AWS Transfer Family servidores](#)).
- Actualmente, no se admiten varios archivos adjuntos ni la mensajería de intercambio de certificados (CEM) de la versión 1.2 de AS2.
- Actualmente, la autenticación básica solo se admite para los mensajes salientes.
- Puede adjuntar un flujo de trabajo de procesamiento de archivos a un servidor Transfer Family que utilice el protocolo AS2; sin embargo, los mensajes AS2 no ejecutan los flujos de trabajo adjuntos al servidor.

Características y funciones básicas de AS2

En las siguientes tablas, se enumeran las características y las capacidades disponibles para los recursos de Transfer Family que utilizan AS2.

Características de AS2

Transfer Family ofrece las siguientes características para AS2.

Característica	Compatible con AWS Transfer Family
Certificación Drummond	Sí
AWS CloudFormation apoyo	Sí
CloudWatchMétricas de Amazon	Sí
SHA-2 algoritmos criptográficos	Sí
Support para Amazon S3	Sí
Compatibilidad con Amazon EFS	No
Mensajes programados	Sí ¹
AWS Transfer Family Flujos de trabajo administrados	No
Mensajería de intercambio de certificados (CEM)	No
TLS mutuo (mTLS)	No
Support para certificados autofirmados	Sí

1. Mensajes programados salientes disponibles [mediante AWS Lambda las funciones de programación](#) de Amazon EventBridge

Capacidades de envío y recepción de AS2

La siguiente tabla proporciona una lista de las capacidades de envío y recepción de AWS Transfer Family AS2.

Funcionalidad	Entrante: recepción con servidor	Saliente: envío con conector
Transporte cifrado TLS (HTTPS)	Sí ¹	Sí
Non-TLS Transporte (HTTP)	Sí	Sí ²
MDN síncrono	Sí	Sí
Compresión de mensajes	Sí	Sí
MDN asíncrono	Sí	Sí
Dirección IP estática	Sí	Sí
Traiga su propia dirección IP	Sí	No
Varios archivos adjuntos	No	No
Autenticación básica	No	Sí
Reinicio de AS2	No aplicable	No
Fiabilidad de AS2	No	No
Asunto personalizado por mensaje	No aplicable	No

1. Transporte cifrado TLS entrante disponible con Network Load Balancer (NLB) o Application Load Balancer (ALB)

2. El transporte saliente sin TLS solo está disponible cuando el cifrado está activado

Administre los certificados AS2

En este tema se explica cómo importar y administrar los certificados AS2. La importación de certificados es el primer paso del proceso AS2 de Transfer Family.

1. Importar certificados

2. [Creación de perfiles de AS2](#)
3. [Crear un servidor AS2](#)
4. [Cree un acuerdo AS2](#)
5. [Configure los conectores AS2](#)

Importar certificados AS2

El proceso AS2 de Transfer Family utiliza claves de certificado tanto para el cifrado como para la firma de la información transferida. Los socios pueden usar la misma clave con ambos fines o una clave independiente para cada uno. Si tiene claves de cifrado comunes que un tercero de confianza guarda en custodia para poder descifrar los datos en caso de desastre o violación de la seguridad, le recomendamos que tenga claves de firma independientes. Al utilizar claves de firma independientes (que no deposite en custodia), no compromete las características de no repudio de sus firmas digitales.

Note

La longitud de la clave de los certificados AS2 debe ser de al menos 2048 bits y, como máximo, de 4096.

Los siguientes puntos detallan cómo se utilizan los certificados AS2 durante el proceso.

- AS2 entrante
 - El socio comercial envía su clave pública para el certificado de firma y esta clave se importa al perfil del socio.
 - La parte local envía la clave pública para sus certificados de cifrado y firma. A continuación, el socio importa la(s) clave(s) privada(s). La parte local puede enviar claves de certificado independientes para firmarlas y cifrarlas, o puede optar por utilizar la misma clave con ambos fines.
- AS2 saliente
 - El socio envía la clave pública de su certificado de cifrado y esta clave se importa al perfil del socio.
 - La parte local envía la clave pública del certificado para firmarlo e importa la clave privada del certificado para firmarlo.

- Si utiliza HTTPS, puede importar un certificado de seguridad de capa de transporte (TLS) autofirmado.

Para obtener información detallada acerca de la forma de crear certificados, consulte [the section called “Paso 1: creación de los certificados para AS2”](#).

En este procedimiento, se explica cómo importar certificados mediante la consola Transfer Family. Si desea utilizar el en su AWS CLI lugar, consulte. [the section called “Paso 2: Importar certificados como recursos de certificados de Transfer Family”](#)

Para especificar un AS2-enabled certificado

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, en AS2 Trading Partners, elija Certificados.
3. Seleccione Importar certificado.
4. En la sección Configuración del certificado, en la sección Descripción del certificado, introduzca un nombre fácilmente identificable para el certificado. Asegúrese de poder identificar el propósito del certificado por su descripción. Además, elija el rol del certificado.
5. En la sección Uso del certificado, elija el propósito de este certificado. Se puede usar para cifrar, firmar o ambas cosas.

Consejo: Si eliges el cifrado y la firma para el uso, Transfer Family crea dos certificados idénticos (cada uno con su propio identificador): uno con un valor de uso ENCRYPTION y otro con un valor de uso deSIGNING.

6. En la sección Contenido del certificado, proporcione un certificado público de un socio comercial o las claves pública y privada de un certificado local.

Rellene la sección Contenido del certificado con los detalles correspondientes.

- Si elige Self-signed un certificado, no proporcionará la cadena de certificados.
 - Pegue el texto del certificado y su cadena en el campo Certificado y cadena de certificados.
 - Si este certificado es un certificado local, pegue su clave privada.
7. Elija Importar certificado para completar el proceso y guardar los detalles del certificado importado.

 Note

Los certificados TLS solo se pueden importar como certificado público de un socio. Si selecciona un certificado público de un socio y, a continuación, selecciona Transport Layer Security (TLS) para su uso, recibirá una advertencia. Además, los certificados TLS deben estar autofirmados (es decir, debe seleccionar el certificado autofirmado para importar un certificado TLS).

Rotación de certificado AS2

Los certificados suelen ser válidos durante un período de seis meses a un año. Es posible que haya configurado perfiles que desee conservar durante más tiempo. Para facilitar esto, Transfer Family ofrece la rotación de certificados. Puede especificar varios certificados para un perfil, lo que le permitirá seguir utilizando el perfil durante varios años. Transfer Family utiliza certificados para la firma (opcional) y el cifrado (obligatorio). Si lo desea, puede especificar un único certificado con ambos fines.

La rotación de certificados es el proceso de reemplazar un certificado antiguo que ha caducado por uno más nuevo. La transición es gradual para evitar interrumpir las transferencias cuando una de las partes del acuerdo aún no ha configurado un nuevo certificado para las transferencias salientes o puede que esté enviando cargas útiles firmadas o cifradas con un certificado antiguo durante un período en el que también se esté utilizando un certificado más nuevo. El período intermedio en el que son válidos tanto los certificados antiguos como los nuevos se denomina período de gracia.

X.509 los certificados tienen y fechas `Not Before`. `Not After` Sin embargo, es posible que estos parámetros no proporcionen un control suficiente a los administradores. Transfer Family proporciona `Active Date` y `Inactive Date` configuración para controlar qué certificado se usa para las cargas útiles salientes y cuál se acepta para las cargas útiles entrantes.

Control de caducidad de los certificados

Transfer Family publica una CloudWatch métrica `DaysUntilExpiry` de Amazon tras importar un certificado. La métrica emite el número de días entre la fecha actual y la fecha especificada `InactiveDate` en el certificado. La métrica se encuentra en el espacio de Transfer AWS nombres del panel de métricas. CloudWatch

Esta métrica siempre tendrá una dimensión métrica `CertificateId`, de forma opcional, incluirá una dimensión de descripción si el cliente la proporciona en el certificado. Para obtener más información

sobre las dimensiones CloudWatch métricas, consulte [Dimensión](#) en la referencia de la CloudWatch API.

 Note

Una vez importado un certificado, Transfer Family puede tardar hasta un día completo en emitir esta métrica a la cuenta del cliente.

Puede usar esta métrica para crear CloudWatch alarmas que le notifiquen cuando los certificados estén a punto de caducar.

La selección del certificado de salida utiliza el valor máximo anterior a la fecha de la transferencia como `Inactive Date`. Los procesos entrantes aceptan certificados dentro del rango de `Not Before` y `Not After` y dentro del rango de `Active Date` y `Inactive Date`.

Ejemplo de rotación de certificados

En la siguiente tabla, se describe una forma posible de configurar dos certificados para un único perfil.

Dos certificados en rotación

Name	NOT BEFORE (controlado por la autoridad de certificación)	ACTIVE DATE (producida por Transfer Family)	INACTIVE DATE (producida por Transfer Family)	NOT AFTER (producida por una entidad de certificación)
Cert1 (certificado anterior)	2019-11-01	2020-01-01	2020-12-31	2024-01-01
Cert2 (certificado más reciente)	2020-11-01	2020-06-01	2021-06-01	2025-01-01

Tenga en cuenta lo siguiente:

- Al especificar un certificado `Active Date` y `Inactive Date` para un certificado, el rango debe estar dentro del rango entre `Not Before` y `Not After`.

- Se recomienda configurar varios certificados para cada perfil, asegurándose de que el intervalo de fechas activo de todos los certificados combinados abarque el período de tiempo durante el que desea utilizar el perfil.
- Le recomendamos que especifique un período de gracia entre el momento en que el certificado anterior pasa a estar inactivo y el certificado más nuevo se activa. En el ejemplo anterior, el primer certificado no queda inactivo hasta el 31/12/2020, mientras que el segundo se activa el 1/06/2020, lo que proporciona un período de gracia de 6 meses. Durante el período comprendido entre el 1/06/2020 y el 31/12/2020, ambos certificados estarán activos.

Creación de perfiles de AS2

En este tema se explica cómo crear perfiles para usarlos en el proceso AS2. Un perfil local define la organización o «parte» local (servidor AS2-enabled Transfer Family). Del mismo modo, un perfil de socio define la empresa asociada remota, externa a Transfer Family.

1. [Importar certificados AS2](#)
2. Creación de perfiles de AS2
3. [Crear un servidor AS2](#)
4. [Cree un acuerdo AS2](#)
5. [Configure los conectores AS2](#)

Utilice este procedimiento para crear perfiles locales y de socios. Este procedimiento explica cómo crear perfiles AS2 mediante la consola Transfer Family. Si desea utilizar la AWS CLI en su lugar, consulte la [the section called “Paso 3: Cree perfiles para usted y su socio comercial”](#).

Creación de un perfil de AS2

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, en AS2 Trading Partners, elija Perfiles y, a continuación, elija Crear perfil.
3. En la sección de configuración del perfil, introduzca el ID de AS2 del perfil. Este valor se utiliza para los encabezados HTTP específicos del protocolo AS2 as2-from y as2-to para identificar la asociación comercial, que determina los certificados que se van a utilizar, etc.
4. En la sección Tipo de perfil, elija Perfil local o Perfil de socio.
5. En la sección Certificados, elija uno o más certificados en el menú desplegable.

Consejo: Si desea importar un certificado que no aparece en el menú desplegable, seleccione Importar un certificado nuevo. Esto abre una nueva ventana del navegador en la pantalla de importación de certificados. Para obtener información sobre el procedimiento de importación de certificados, consulte [Importar certificados AS2](#).

6. (Opcional) En la sección Etiquetas, especifique uno o más pares de clave-valor para ayudar a identificar este perfil.
7. Seleccione Crear perfil para completar el proceso y guardar el nuevo perfil.

Crear un servidor AS2

En este tema se proporcionan instrucciones para crear un servidor AS2-enabled Transfer Family mediante la consola o una CloudFormation plantilla. Para obtener un ejemplo integral de una configuración de AS2, consulte [Configuración de una configuración AS2](#). Tras crear un servidor AS2, puede añadir un acuerdo al servidor.

1. [Importar certificados AS2](#)
2. [Creación de perfiles de AS2](#)
3. Cree un servidor AS2
4. [Cree un acuerdo AS2](#)
5. [Configure los conectores AS2](#)

Temas

- [Cree un servidor AS2 mediante la consola Transfer Family](#)
- [Uso de una plantilla para crear una pila AS2 de Transfer Family de demostración](#)
- [Cree un acuerdo AS2](#)

Cree un servidor AS2 mediante la consola Transfer Family

Este procedimiento explica cómo crear un AS2-enabled servidor mediante la consola Transfer Family. Si desea utilizar la AWS CLI en su lugar, consulte [the section called “Paso 4: Crear un servidor Transfer Family que utilice el protocolo AS2”](#).

 Note

Puede adjuntar un flujo de trabajo de procesamiento de archivos a un servidor Transfer Family que utilice el protocolo AS2; sin embargo, los mensajes AS2 no ejecutan los flujos de trabajo adjuntos al servidor.

Para crear un servidor AS2-enabled

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Servidores y, a continuación, Crear servidor.
3. En la página Elegir protocolos, seleccione AS2 (Declaración de aplicabilidad 2) y, a continuación, elija Siguiente.
4. En la página Elija un proveedor de identidad, elija Siguiente.

 Note

En el caso del AS2, no puede elegir un proveedor de identidad porque el protocolo AS2 no admite la autenticación básica. En su lugar, usted controla el acceso a través de grupos de seguridad de nube privada virtual (VPC).

5. En la página Elegir un punto de conexión haga lo siguiente:

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID

[Create a VPC](#)

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

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

- a. En el tipo de punto de conexión, seleccione el punto de conexión alojado en la VPC para alojar el punto de conexión de su servidor. Para obtener información sobre la configuración de su VPC-hosted terminal, consulte [Creación de un servidor en una nube privada virtual \(VPC\)](#).

Note

Los puntos de conexión de acceso público no son compatibles con el protocolo AS2. Para que su punto de conexión de VPC sea accesible a través de Internet, elija Internet Facing en Acceso y, a continuación, proporcione sus direcciones IP elásticas.

- b. En Acceso, elija una de las siguientes opciones:

- Interno: elija esta opción para proporcionar acceso desde su VPC y sus VPC-connected entornos, como un centro de datos local a través Direct Connect de una VPN.
- Orientado a Internet: elija esta opción para proporcionar acceso a través de Internet y desde su VPC y sus VPC-connected entornos, como un centro de datos local a través Direct Connect de una VPN.

Si elige Internet, proporcione sus direcciones IP elásticas cuando se le pida.

- c. Para una VPC, elija una VPC existente o elija Crear VPC para crear una nueva VPC.
- d. En el caso de FIPS activado, mantenga desactivada la casilla de verificación del punto de conexión con FIPS activado.

 Note

FIPS-enabled Los puntos finales no son compatibles con el protocolo AS2.

- e. Elija Siguiente.
6. En la página Elija un dominio, elija Amazon S3 para almacenar sus archivos y acceder a ellos como objetos mediante el protocolo seleccionado.

Elija Siguiente.

7. En la página Configurar detalles adicionales, elija los ajustes que necesite.

 Note

Si va a configurar otros protocolos junto con el AS2, se aplicarán todos los ajustes de detalle adicionales. Sin embargo, en el caso del protocolo AS2, los únicos ajustes que se aplican son los de las secciones de CloudWatch registro y etiquetas.

Aunque la configuración de una función de CloudWatch registro es opcional, le recomendamos encarecidamente que la configure de forma que pueda ver el estado de los mensajes y solucionar los problemas de configuración.

8. En la página Revisar y crear, revise sus opciones para asegurarse de que son correctas.

- Si quiere editar alguna de sus configuraciones, seleccione Editar junto al paso que desea cambiar.

 Note

Si editas un paso, le recomendamos que revises cada paso después del paso que decidiste editar.

- Si no ha realizado cambios, seleccione Crear servidor para crear el suyo. Así llegará a la página Servers (Servidores), mostrada a continuación, donde ya aparece el nuevo servidor.

Pueden transcurrir algunos minutos antes de que el estado del nuevo servidor SFTP cambie a Online. En ese momento, el servidor ya puede realizar operaciones con archivos para los usuarios.

Uso de una plantilla para crear una pila AS2 de Transfer Family de demostración

Proporcionamos una CloudFormation plantilla independiente para crear rápidamente un servidor AS2-enabled Transfer Family. La plantilla configura el servidor con un punto de conexión de VPC de Amazon público, certificados, perfiles locales y de socios, un acuerdo y un conector.

La plantilla básica del servidor AS2 crea los siguientes recursos:

- Un servidor AS2-enabled Transfer Family con un terminal de VPC
- Perfiles AS2 locales y de socios con certificados
- Un acuerdo entre los perfiles
- Un bucket de Amazon S3 para almacenamiento de archivos
- Funciones y políticas de IAM obligatorias
- CloudWatch configuración de registro

Antes de usar esta plantilla, debe tener en cuenta lo siguiente:

- Se le facturarán los recursos de AWS que utilice si crea una pila a partir de esta plantilla.
- La plantilla crea varios certificados y los coloca AWS Secrets Manager para almacenarlos de forma segura. Si lo desea, puede eliminar estos certificados de Secrets Manager, puesto que se le cobrará por usar este servicio. La eliminación de estos certificados en Secrets Manager no lo realiza el servidor de Transfer Family. Por tanto, la funcionalidad de la pila de demostración no se

ve afectada. Sin embargo, en el caso de certificados que vaya a utilizar con un servidor AS2 de producción, puede utilizar Secrets Manager para administrar y rotar periódicamente los certificados almacenados.

- Le recomendamos que utilice la plantilla solo como base y, sobre todo, con fines de demostración. Si quiere utilizar esta pila de demostración en producción, le recomendamos que modifique el código YAML de la plantilla para crear una pila más sólida. Por ejemplo, cree certificados de nivel de producción y cree una función AWS Lambda que pueda usar en producción.

Para crear un servidor AS2-enabled Transfer Family a partir de una CloudFormation plantilla

1. Abra la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
2. En el panel de navegación izquierdo, elija Pilas.
3. Elija Create stack (Crear pila), y, a continuación, elija With new resources (standard) (Con nuevos recursos [estándar]).
4. En la sección Requisitos previos: preparar una plantilla, elija Elegir una plantilla existente.
5. Copie este enlace, [plantilla de demostración de AS2](#), y péguelo en el campo URL de Amazon S3.
6. Elija Siguiente.
7. En la página Especificar los detalles de la pila, asigne un nombre a la pila y, a continuación, especifique los siguientes parámetros:
 - En AS2, introduzca los valores para el ID de AS2 local y el ID de AS2 del socio, o acepte los valores predeterminados `local` y `partner` respectivamente.
 - En Red, introduzca un valor para la IP CIDR de entrada de grupos de seguridad o acepte el valor predeterminado, `0.0.0.0/0`.

 Note

Este valor, en formato CIDR, especifica las direcciones IP que están permitidas para el tráfico entrante al servidor AS2. El valor predeterminado, `0.0.0.0/0`, permite todas las direcciones IP.

- En General, introduzca un valor para Prefijo, o acepte el valor predeterminado, `transfer-as2`. Este prefijo se coloca antes de cualquier nombre de recurso creado por la pila. Por ejemplo, si utiliza el prefijo predeterminado, su bucket de Amazon S3 se llamará `transfer-as2-amzn-s3-demo-bucket`.

8. Elija Siguiente. En la página Configurar opciones de pila, elija Siguiente.
9. Revise los detalles de la pila que está creando y, a continuación, seleccione Crear pila.

 Note

En la parte inferior de la página, en Capacidades, debes reconocer que CloudFormation podrías crear recursos AWS Identity and Access Management (IAM).

Una vez creada la pila, puede enviar un mensaje AS2 de prueba desde el servidor asociado a su servidor Transfer Family local mediante AWS Command Line Interface (AWS CLI). Se crea un AWS CLI comando de muestra para enviar un mensaje de prueba junto con todos los demás recursos de la pila.

Para usar este comando de ejemplo, ve a la pestaña Salidas de tu pila y copia el `TransferExampleAs2Command`. A continuación, puede ejecutar el comando mediante AWS CLI. Si aún no lo ha instalado AWS CLI, consulte [Instalación o actualización de la última versión de AWS CLI en la](#) Guía del AWS Command Line Interface usuario.

El comando de ejemplo tiene el siguiente formato:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt && aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId --send-file-paths /amzn-s3-demo-bucket/test.txt
```

 Note

Su versión de este comando contiene los valores reales para los recursos *amzn-s3-demo-bucket* y *TransferConnectorId* de su pila.

Este comando de ejemplo consta de dos comandos independientes que se encadenan mediante la cadena `&&`.

El primer comando crea un archivo de texto nuevo y vacío en el bucket:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt
```

A continuación, el segundo comando utiliza el conector para enviar el archivo del perfil asociado al perfil local. El servidor de Transfer Family tiene un acuerdo establecido que permite que el perfil local acepte mensajes del perfil del socio.

```
aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId
--send-file-paths /amzn-s3-demo-bucket/test.txt
```

Tras ejecutar el comando, puede ir a su bucket de Amazon S3 (*amzn-s3-demo-bucket*) y ver el contenido. Si el comando se ejecuta correctamente, debería ver los siguientes objetos en el bucket:

- *processed/*: esta carpeta contiene un archivo JSON que describe el archivo transferido y la respuesta de MDN.
- *processing/*: esta carpeta contiene temporalmente los archivos a medida que se procesan; pero, una vez finalizada la transferencia, esta carpeta debería estar vacía.
- *server-id/*: el nombre de esta carpeta se basa en el ID de servidor de Transfer Family. Contiene *from-partner* (esta carpeta recibe un nombre dinámico, en función del ID AS2 del socio) que, a su vez, contiene las carpetas *failed/*, *processed/* y *processing/*. La carpeta */server-id/from-partner/processed/* contiene una copia del archivo de texto transferido y los archivos JSON y MDN correspondientes.
- *test.txt*: este objeto es el archivo (vacío) que se transfirió.

Cree un acuerdo AS2

Los acuerdos están asociados a los servidores Transfer Family. Especifican los detalles de los socios comerciales que utilizan el protocolo AS2 para intercambiar mensajes o archivos mediante Transfer Family, para las transferencias entrantes, es decir, el envío de archivos AS2 desde una fuente externa propiedad del socio a un servidor de Transfer Family.

Este procedimiento explica cómo crear acuerdos AS2 mediante la consola Transfer Family. Si desea utilizar el AWS CLI en su lugar, consulte [the section called “Paso 5: creación de un acuerdo entre usted y su socio”](#).

Creación de un acuerdo para un servidor de Transfer Family

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Servidores y, a continuación, seleccione un servidor que utilice el protocolo AS2.

Como alternativa, siempre que tenga al menos un servidor Transfer Family que utilice el protocolo AS2, seleccione Acuerdos para recibir mensajes del menú AS2 Trading Partners. A continuación, en la pantalla Crear acuerdo, seleccione el servidor AS2 al que desee asociar este acuerdo.

3. En la página de detalles del servidor, desplácese hacia abajo hasta la sección Acuerdos.
4. Seleccione Añadir acuerdo.
5. Complete los parámetros del acuerdo de la siguiente manera:
 - a. En la sección Configuración del acuerdo, introduzca un nombre descriptivo. Asegúrese de poder identificar el propósito del acuerdo por su nombre. Además, defina el estado del acuerdo: Activo (seleccionado de forma predeterminada) o Inactivo.
 - b. En la sección Configuración de la comunicación, elija un perfil local y un perfil de socio. Además, elija si desea forzar o no la firma de los mensajes.
 - De forma predeterminada, Exigir la firma de mensajes está habilitada, lo que significa que Transfer Family rechaza los mensajes no firmados de su socio comercial para este acuerdo.
 - Desactive esta configuración para permitir que Transfer Family acepte mensajes no firmados de su socio comercial para este acuerdo.
 - c. En la sección de configuración del directorio de la bandeja de entrada, proporcione la siguiente información.
 - Determine si desea o no seleccionar Especificar directorios independientes para almacenar los mensajes AS2, los archivos MDN y los archivos de estado JSON.
 - Si seleccionas esta opción, especificas ubicaciones distintas para los archivos de carga útil, los archivos con errores, los archivos MDN, los archivos de estado y los archivos temporales.
 - Si desactiva esta opción, todos los archivos AS2 irán a la ubicación que especifique para el directorio base.
 - Para S3 Bucket, elija un bucket de Amazon S3.
 - En Prefix, puede introducir un prefijo (carpeta) para almacenar los archivos en el bucket.

Por ejemplo, si escribes **amzn-s3-demo-bucket** para el depósito y **incoming** el prefijo, los archivos AS2 se guardarán en la carpeta. **/amzn-s3-demo-bucket/incoming**

- Para el rol de AWS IAM, elija un rol que pueda acceder al depósito que especificó.

- En Conservar el nombre de archivo, elija si desea conservar los nombres de archivo originales para las cargas útiles de los mensajes AS2 entrantes.
 - Si selecciona esta configuración, el nombre de archivo proporcionado por su socio comercial se conserva cuando el archivo se guarda en Amazon S3.
 - Si desactiva esta configuración, cuando Transfer Family guarde el archivo, se ajustará el nombre del archivo, tal y como se describe en [Nombres y ubicaciones de los archivos](#).
- d. (Opcional) En la sección Etiquetas, agregue etiquetas a su secreto.
- e. Una vez haya introducido toda la información del acuerdo, elija Crear acuerdo.

El nuevo acuerdo aparece en la sección Acuerdos de la página de detalles del servidor.

Configure los conectores AS2

El propósito de un conector es establecer una relación entre los socios comerciales para las transferencias salientes, es decir, enviar archivos AS2 desde un servidor de Transfer Family a un destino externo propiedad del socio. Para el conector, debe especificar la parte local, el socio remoto y sus certificados (mediante la creación de perfiles locales y de socios).

Una vez haya instalado un conector, podrá transferir información a sus socios comerciales. A cada servidor AS2 se le asignan tres direcciones IP estáticas. Los conectores AS2 utilizan estas direcciones IP para enviar mDNS asíncronos a sus socios comerciales a través de AS2.

Note

El tamaño del mensaje recibido por un socio comercial no coincidirá con el tamaño del objeto en Amazon S3. Esta discrepancia se debe a que el mensaje AS2 envuelve el archivo en un sobre antes de enviarlo. Por tanto, el tamaño del archivo puede aumentar, incluso si el archivo se envía comprimido. Por tanto, asegúrese de que el tamaño máximo de archivo del socio comercial sea mayor que el tamaño del archivo que está enviando.

1. [Importar certificados AS2](#)
2. [Creación de perfiles de AS2](#)
3. [Crear un servidor AS2](#)
4. [Cree un acuerdo AS2](#)

5. Cree un conector AS2

Cree un conector AS2

En este procedimiento se explica cómo crear conectores AS2 desde la consola de AWS Transfer Family . Si desea utilizar el AWS CLI en su lugar, consulte [the section called “Paso 6: creación de un conector entre usted y su socio”](#).

Creación de un conector AS2

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Conectores para enviar mensajes en el menú AS2 Trading Partners y, a continuación, seleccione Crear conector AS2.
3. En la sección de configuración del conector, especifique la siguiente información:
 - URL: introduzca la URL de las conexiones salientes.
 - Modo de direccionamiento IP: elija solo IPv4 (predeterminado) para usar direcciones IPv4 exclusivamente o Dual-stack para admitir IPv6 e IPv4. En el modo de doble pila, el conector prefiere IPv6 cuando la resolución de DNS devuelve resultados de IPv6 y utiliza IPv4 cuando solo se devuelven resultados de DNS de IPv4.
 - Función de acceso: elija el nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que se va a utilizar. Asegúrese de que este rol proporcione acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`. Además, asegúrese de que el rol proporcione acceso de lectura y escritura al directorio principal de los archivos que desea enviar con `StartFileTransfer`.

Note

Si utiliza la autenticación básica para su conector, el rol de acceso requiere el permiso `secretsmanager:GetSecretValue` del secreto. Si el secreto se cifra mediante una clave gestionada por el cliente Clave administrada de AWS en lugar de la clave de AWS Secrets Manager entrada, el rol también necesitará el `kms:Decrypt` permiso para esa clave. Si nombra su secreto con el prefijo `aws/transfer/`, puede añadir el permiso necesario con un carácter comodín (*), como se muestra en el [Ejemplo de permiso para crear secretos](#).

- Función de registro (opcional): elija la función de IAM para que el conector la utilice para enviar eventos a sus CloudWatch registros.
4. En la sección de configuración de AS2, elija los perfiles locales y de los socios, los algoritmos de cifrado y firma y decida si desea comprimir la información transferida. Tenga en cuenta lo siguiente:

- El Content-Type parámetro Preserve S3 está activado de forma predeterminada.

Cuando se establece, Transfer Family utiliza Amazon S3 Content-Type que está asociado a los objetos de S3 en lugar de asignar el tipo de contenido en función de la extensión del archivo. Desactive esta configuración si desea que el servicio asigne el tipo de contenido de sus mensajes AS2 en función de la extensión del archivo, en lugar de utilizar el tipo de contenido del objeto S3.

- No elija el algoritmo de cifrado DES_EDE3_CBC a menos que sea compatible con un cliente antiguo que lo requiera, ya que se trata de un algoritmo de cifrado débil.
 - El Asunto se utiliza como atributo de encabezado subject HTTP en los mensajes de AS2 que se envían con el conector.
 - Si opta por crear un conector sin un algoritmo de cifrado, debe HTTPS especificarlo como protocolo.
5. En la sección Autenticación básica, especifique la siguiente información.
- Para enviar las credenciales de inicio de sesión junto con los mensajes salientes, seleccione Habilitar la autenticación básica. Si no quiere enviar ninguna credencial con los mensajes salientes, mantén desactivada la opción Habilitar la autenticación básica.
 - Si utiliza la autenticación, elija o cree un secreto.
 - Para crear un secreto nuevo, seleccione Crear un secreto nuevo y, a continuación, introduzca un nombre de usuario y una contraseña. Estas credenciales deben coincidir con el usuario que se conecta al punto de conexión del socio.

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☒ Create a new secret
☐ Choose an existing secret

Username
test-user

Password

[i](#) Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

- Para utilizar un secreto, elija Usar secreto existente y, a continuación, elija un secreto de la lista. Para obtener información detallada acerca de la forma de crear un secreto con el formato correcto en Secrets Manager, consulte [Habilite la autenticación básica para los conectores AS2](#).

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret
☒ Choose an existing secret

Choose a secret

aws/transfer/...
SFTP connector...

aws/transfer/sftp-connector1
Secret key ...

aws/transfer/c...

[i](#) Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

6. En la sección de Configuración MDN, especifique la siguiente información:

- Solicite un MDN: tiene la opción de solicitar a su socio comercial que le envíe un MDN una vez que haya recibido correctamente su mensaje a través de AS2.

- MDN firmado: tiene la opción de solicitar que el mDNS esté firmado. Esta opción solo está disponible si has seleccionado Solicitar MDN.
7. Una vez que hayas confirmado todos los ajustes, selecciona Crear conector AS2 para crear el conector.

Aparece la página Conectores, con el identificador del nuevo conector agregado a la lista. Para ver los detalles de los conectores, consulte [Visualización de los detalles del conector AS2](#).

Algoritmos de conector AS2

Al crear un conector AS2, se adjuntan al conector los siguientes algoritmos de seguridad.

Tipo	Algoritmo
Cifrados TLS	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Autenticación básica para conectores AS2

Al crear o actualizar un servidor de Transfer Family que utiliza el protocolo AS2, puede añadir la autenticación básica para los mensajes salientes. Para ello, añada la información de autenticación a un conector.

Note

La autenticación básica solo está disponible si utiliza HTTPS.

Para utilizar la autenticación para el conector, seleccione **Habilitar la autenticación básica** en la sección **Autenticación básica**. Tras habilitar la autenticación básica, puede optar por crear un secreto nuevo o utilizar uno existente. En cualquier caso, las credenciales del secreto se envían con los mensajes salientes que utilizan este conector. Las credenciales deben coincidir con las del usuario que intenta conectarse al punto de conexión remoto del socio comercial.

En la siguiente captura de pantalla se muestra la opción **Activar la autenticación básica** y la opción **Crear un secreto nuevo**. Tras realizar estas selecciones, puede introducir un nombre de usuario y una contraseña para el secreto.

Basic authentication [Info](#)
☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.
☒ **Create a new secret**
☐ Choose an existing secret

Username

Password

[Info](#) Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

En la siguiente captura de pantalla se muestra la opción Activar la autenticación básica y la opción Seleccionar un secreto existente. El secreto debe tener el formato correcto, tal y como se explica en [Habilite la autenticación básica para los conectores AS2](#).

Habilite la autenticación básica para los conectores AS2

Al habilitar la autenticación básica para los conectores AS2, puede crear un secreto nuevo en la consola Transfer Family o usar uno que haya creado en AWS Secrets Manager. En cualquier caso, su secreto se guarda en Secrets Manager.

Temas

- [Creación de un nuevo secreto en la consola](#)
- [Usar un secreto de existente](#)
- [Crea un secreto en AWS Secrets Manager](#)

Creación de un nuevo secreto en la consola

Al crear un conector en la consola, puede crear un secreto nuevo.

Para crear un secreto nuevo, seleccione Crear un secreto nuevo y, a continuación, introduzca un nombre de usuario y una contraseña. Estas credenciales deben coincidir con el usuario que se conecta al punto de conexión del socio.

Basic authentication [Info](#)

☒ Enable Basic authentication - *optional*

Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)

Choose the username and password credentials that will be used to authenticate with your trading partner's host.

- ☒ Create a new secret
- ☐ Choose an existing secret

Username

Password

[i](#) Update the [access role associated with your connector](#) [🔗](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

[i](#) Note

Al crear un nuevo secreto en la consola, el nombre del secreto sigue esta convención de nomenclatura: `/aws/transfer/connector-id`, donde **connector-id** está el ID del conector que se está creando. Ten esto en cuenta cuando intentes localizar el secreto AWS Secrets Manager.

Usar un secreto de existente

Al crear un conector en la consola, puede especificar un secreto existente.

Para utilizar un secreto, elija Usar secreto existente y, a continuación, elija un secreto de la lista. Para obtener información detallada acerca de la forma de crear un secreto con el formato correcto en Secrets Manager, consulte [Crea un secreto en AWS Secrets Manager](#).

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret

☒ Choose an existing secret

Choose a secret

aws/transfer/...
SFTP connector...

aws/transfer/sftp-connector1
Secret key ...

aws/transfer/c...

or to provide AWS Transfer Family with permission to credentials.

Crea un secreto en AWS Secrets Manager

En el siguiente procedimiento, se describe cómo crear un secreto apropiado para usarlo con el conector AS2.

Note

La autenticación básica solo está disponible si utiliza HTTPS.

Almacenamiento de las credenciales de usuario en Secrets Manager para la autenticación AS2 Basic

1. Inicia sesión en Consola de administración de AWS y abre la AWS Secrets Manager consola en <https://console.aws.amazon.com/secretsmanager/>.
2. En el panel de navegación izquierdo, seleccione Secretos.
3. En la página Secretos, seleccione Almacenar un nuevo secreto.
4. En la página Seleccionar tipo de secreto, en Tipo de secreto, seleccione Otro tipo de secreto.
5. En la sección de Key/value parejas, selecciona la Key/valuepestaña.
 - Clave: introduzca **Username**.
 - valor: introduzca el nombre del usuario que está autorizado a conectarse al servidor del socio.

6. Si desea proporcionar una contraseña, elija Agregar fila y, en la sección de Key/value pares, elija la Key/valuepestaña.

Seleccione Añadir fila y, en la sección de Key/value pares, elija la Key/valuepestaña.

- Clave: introduzca **Password**.
 - valor: introduzca una contraseña para el usuario.
7. Si desea proporcionar una clave privada, elija Agregar fila y, en la sección de Key/value pares, elija la Key/valuepestaña.
 - Clave: introduzca **PrivateKey**.
 - valor: introduzca una clave privada para el usuario. Este valor debe almacenarse en formato OpenSSH y debe corresponder a la clave pública que se almacena para este usuario en el servidor remoto.
 8. Elija Siguiente.
 9. En la página Configurar secreto, introduzca un nombre y una descripción para el secreto. Se recomienda utilizar un prefijo de **aws/transfer/** para el nombre. Por ejemplo, puede dar un nombre a su secreto de **aws/transfer/connector-1**.
 10. Seleccione Siguiente y, a continuación, acepte los valores predeterminados de la página Configurar rotación. A continuación, elija Siguiente.
 11. En la página de Revisión, elija Guardar para crear y almacenar el secreto.

Tras crear el secreto, puede elegirlo al crear un conector (consulte [Configure los conectores AS2](#)). En el paso en el que habilita la autenticación básica, elija el secreto de la lista desplegable de todos los secretos disponibles.

Visualización de los detalles del conector AS2

Encontrará una lista de detalles y propiedades de un AWS Transfer Family conector AS2 en la AWS Transfer Family consola. Las propiedades de un conector AS2 incluyen sus URL, roles, perfiles, MDN, etiquetas y métricas de supervisión.

Este es el procedimiento para ver los detalles del conector.

Visualización de los detalles del conector

1. Abra la AWS Transfer Family consola en. <https://console.aws.amazon.com/transfer/>

2. En el panel de navegación izquierdo, seleccione Connectors (Conectores).
3. Elija el identificador en la columna ID del conector para ver la página de detalles del conector seleccionado.

Puede cambiar las propiedades del conector AS2 en la página de detalles del conector seleccionando Editar.

C-

Delete

Connector configuration

Info

Edit

Name

my-as2-connector

Access role

URL

<https://www.example.com>

Logging role

[AWSTransferLoggingAccess](#)

Communication settings

Info

AS2-From header

AS2-To header

AS2 configuration

Info

Edit

Local profile

Compression

Enabled

Encryption algorithm

AES128_CBC

Partner profile

Message Subject

View

Signing algorithm

SHA384

Preserve S3 Content-Type

Enabled

MDN configuration

Info

Edit

Request MDN

Enabled

Signed MDN

Default to message signing algorithm: SHA384

Synchronization

Enabled

Basic authentication [Info](#)[Edit](#)**Basic authentication**
✔ Enabled**Secret**
aws/transfer/c- [redacted] [Copy](#)**Egress IP details** [Info](#)

Service managed static IP addresses of this connector

[Copy](#) 23.23.130.9[Copy](#) 44.196.109.11[Copy](#) 3.219.16.7**Tags (1)**[Manage tags](#)

Use tags to organize, search, and filter your Connectors. We recommend adding a tag with 'Name' as the key and a unique string as the value to easily identify your Connector.

< 1 >

Key	Value
Name	my-as2-connector

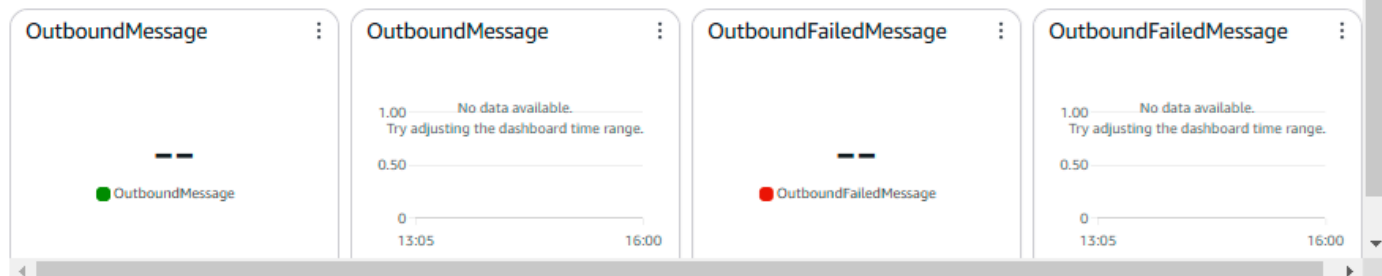
AS2 Monitoring

3h 1d 1w

UTC timezone

[Refresh](#)

⋮

**Note**

Puede obtener gran parte de esta información, aunque en un formato diferente, ejecutando el siguiente comando AWS Command Line Interface (AWS CLI comando):

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

Para obtener más información, consulte [DescribeConnector](#) en la referencia de la API.

Envío y recepción de mensajes AS2

En esta sección se describen los procesos de envío y recepción de mensajes AS2. También proporciona detalles sobre los nombres de archivo y las ubicaciones asociadas a los mensajes AS2.

En la siguiente tabla se enumeran los algoritmos de cifrado disponibles para los mensajes AS2 y cuándo se pueden utilizar.

Algoritmo de cifrado	HTTP	HTTPS	Notas
AES128_CBC	Sí	Sí	
AES192_CBC	Sí	Sí	
AES256_CBC	Sí	Sí	
DES_EDE3_CBC	Sí	Sí	Utilice este algoritmo únicamente si debe admitir un cliente antiguo que lo requiera, ya que es un algoritmo de cifrado débil.
NONE	No	Sí	Si envía mensajes a un servidor de Transfer Family, solo puede seleccionar NONE si utiliza un Application Load Balancer (ALB).

Temas

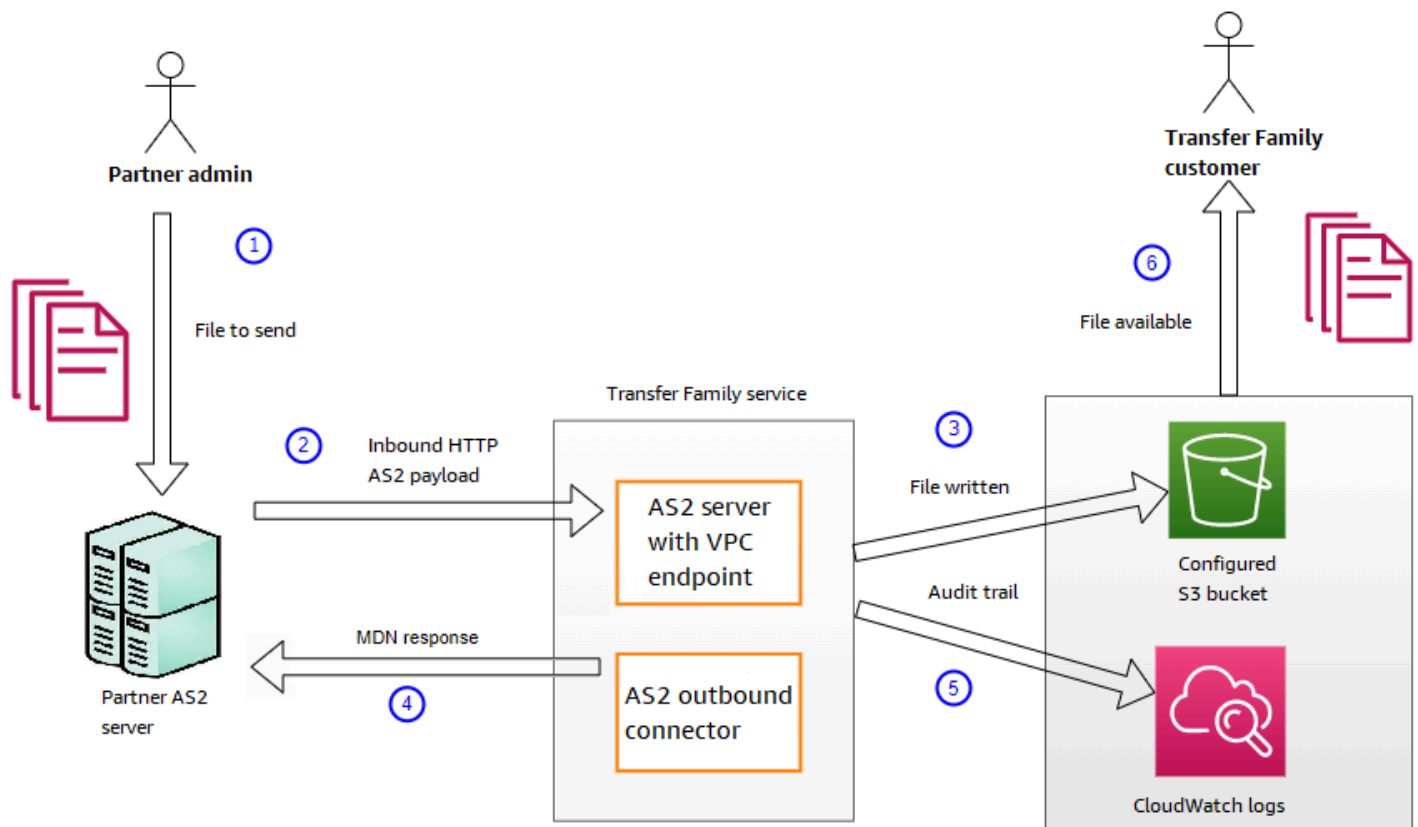
- [Proceso de recepción de mensajes AS2](#)
- [Enviar y recibir mensajes de AS2 a través de HTTPS](#)
- [Transferencia de archivos mediante un conector AS2](#)
- [Nombres y ubicaciones de los archivos](#)

- [Códigos de estado](#)
- [Ejemplos de archivos de JSON](#)

Proceso de recepción de mensajes AS2

El proceso entrante se define como un mensaje o un archivo que se transfiere a su AWS Transfer Family servidor. La secuencia de los mensajes entrantes es la siguiente:

1. Un proceso automatizado o de administración inicia un AS2 file transfer en el servidor AS2 remoto del socio.
2. El servidor AS2 remoto del socio firma y cifra el contenido del archivo y, a continuación, envía una solicitud HTTP POST a un punto de conexión de entrada AS2 alojado en Transfer Family.
3. Mediante los valores configurados para el servidor, los socios, los certificados y el acuerdo, Transfer Family descifra y verifica la carga útil del AS2. El contenido del archivo se almacena en el almacén de archivos configurado de Amazon S3.
4. La respuesta MDN firmada se devuelve en línea con la respuesta HTTP o de forma asíncrona mediante una solicitud HTTP POST independiente al servidor de origen.
5. Se escribe un registro de auditoría a Amazon CloudWatch con detalles sobre el intercambio.
6. El archivo descifrado está disponible en una carpeta llamada `inbox/processed`.



Enviar y recibir mensajes de AS2 a través de HTTPS

En esta sección, se describe cómo configurar un servidor Transfer Family que utiliza el protocolo AS2 para enviar y recibir mensajes a través de HTTPS.

Temas

- [Enviar mensajes de AS2 a través de HTTPS](#)
- [Recibir mensajes de AS2 a través de HTTPS](#)

Enviar mensajes de AS2 a través de HTTPS

Para enviar mensajes de AS2 mediante HTTPS, cree un conector con la siguiente información:

- Para la URL, especifique una URL HTTPS
- Para el algoritmo de cifrado, selecciona cualquiera de los algoritmos disponibles.

 Note

Para enviar mensajes a un servidor Transfer Family sin utilizar el cifrado (es decir, si selecciona el algoritmo NONE de cifrado), debe utilizar un Application Load Balancer (ALB).

- Proporcione los valores restantes para el conector tal y como se describe en [Configure los conectores AS2](#).

Recibir mensajes de AS2 a través de HTTPS

AWS Transfer Family Actualmente, los servidores AS2 solo proporcionan transporte HTTP a través del puerto 5080. Sin embargo, puede finalizar el TLS en un balanceador de carga de redes o aplicaciones frente al punto final de VPC del servidor Transfer Family mediante el puerto y el certificado que prefiera. Con este método, puede hacer que los mensajes de AS2 entrantes utilicen HTTPS.

Requisitos previos

- La VPC debe estar en el mismo lugar que su Región de AWS servidor Transfer Family.
- Las subredes de la VPC deben estar dentro de las zonas de disponibilidad en las que desee utilizar el servidor.

 Note

Cada servidor Transfer Family admite hasta tres zonas de disponibilidad.

- Asigne hasta tres direcciones IP elásticas en la misma región que su servidor. O puede optar por traer su propio intervalo de direcciones IP (BYOIP).

 Note

La cantidad de direcciones IP elásticas debe coincidir con la cantidad de zonas de disponibilidad que utilice con los puntos de conexión del servidor.

Puede configurar un Network Load Balance (NLB) o un Application Load Balancer (ALB). En la siguiente tabla se enumeran las ventajas y desventajas de cada enfoque.

En la siguiente tabla se muestran las diferencias en las capacidades cuando se utiliza un NLB y un ALB para finalizar el TLS.

Característica	Network Load Balancer (NLB)	Application Load Balancer (ALB)
Latencia	Menor latencia, ya que funciona en la capa de red.	Mayor latencia, ya que funciona en la capa de aplicación.
Compatibilidad con direcciones IP estáticas	Puede adjuntar direcciones IP elásticas que pueden ser estáticas.	No se pueden adjuntar direcciones IP elásticas: proporciona un dominio cuyas direcciones IP subyacentes pueden cambiar.
Enrutamiento avanzado	No admite el enrutamiento avanzado.	Admite el enrutamiento avanzado. Puede inyectar el X-Forwarded-Proto encabezado necesario para el AS2 sin cifrado. Este encabezado se describe en el sitio web X-Forwarded-Proto de Protodeveloper.mozilla.org .
TLS/SSL rescisión	Admite la TLS/SSL rescisión	Soporta TLS/SSL la terminación
TLS mutuo (mTLS)	Actualmente, Transfer Family no admite el uso de un NLB para los mTLS	Support for mTLS

Configure NLB

Este procedimiento describe cómo configurar un Network Load Balancer (NLB) con acceso a Internet en la VPC.

Creación de un equilibrador de carga de red y definición del punto de conexión de VPC del servidor como destino del equilibrador de carga

1. Abra la consola de Amazon Elastic Compute Cloud en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Equilibradores de carga y, a continuación, elija Crear equilibrador de carga.
3. En equilibrador de carga de red, seleccione Crear.
4. En la sección Configuración básica, introduzca la siguiente información:
 - En Nombre, escriba el nombre del equilibrador de carga.
 - En Scheme, elija Internet-facing.
 - En Tipo de dirección IP, elija ipv4.
5. En la sección Asignaciones de red, escriba la siguiente información:
 - En VPC, elija la nube privada virtual (VPC) que haya creado.
 - En Asignaciones, elija las zonas de disponibilidad asociadas a las subredes públicas que están disponibles en la misma VPC que utiliza con los puntos de conexión del servidor.
 - Para la dirección IPv4 de cada subred, elija una de las direcciones IP elásticas que haya asignado.
6. En la sección Oyentes y rutas, escriba la siguiente información:
 - En Protocol, elija TLS.
 - En Puerto, escriba **5080**.
 - En Acción predeterminada, elija Crear grupo objetivo. Para obtener información detallada sobre la creación de un nuevo grupo objetivo, consulte [Creación de un grupo de destino](#).

Tras crear un grupo objetivo, introduzca su nombre en el campo Acción predeterminada.

7. En la sección Configuración del agente de escucha seguro, elija su certificado en el área de SSL/TLS certificados predeterminados.
8. Elija Crear un equilibrador de carga para crear el equilibrador de carga de red.
9. (Opcional, pero recomendado) Active los registros de acceso del equilibrador de carga de red para mantener un registro de auditoría completo, tal y como se describe en [los registros de acceso del equilibrador de carga de red](#).

Recomendamos este paso porque la conexión TLS finaliza en el NLB. Por lo tanto, la dirección IP de origen que se refleja en sus grupos de CloudWatch registros AS2 de Transfer Family es la dirección IP privada del NLB, en lugar de la dirección IP externa de su socio comercial.

Configure ALB

Este procedimiento describe cómo configurar un Application Load Balancer (ALB) en la VPC.

Para crear un Application Load Balancer y definir el punto final de VPC del servidor como destino del balanceador de carga

1. Abra la consola de Amazon Elastic Compute Cloud en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Equilibradores de carga y, a continuación, elija Crear equilibrador de carga.
3. En Equilibrador de carga de aplicación, elija Create (Crear).
4. En la consola ALB, cree un nuevo agente de escucha HTTP en el puerto 443 (HTTPS).
5. (Opcional). Si desea configurar la autenticación mutua (mTLS), configure los ajustes de seguridad y un almacén de confianza.
 - a. Adjunte su SSL/TLS certificado al listener.
 - b. En Gestión de certificados de cliente, selecciona Autenticación mutua (mTLS).
 - c. Elige Verificar con un almacén de confianza.
 - d. En Configuración avanzada de mTLS, elija o cree un almacén de confianza cargando sus certificados de CA.
6. Cree un nuevo grupo de destino y añada las direcciones IP privadas de los puntos finales del servidor AS2 de Transfer Family como destinos en el puerto 5080. Para obtener información detallada sobre la creación de un nuevo grupo objetivo, consulte [Creación de un grupo de destino](#).
7. Configure las comprobaciones de estado para que el grupo de destino utilice el protocolo HTTP en el puerto 5080.
8. Cree una nueva regla para reenviar el tráfico HTTPS del agente de escucha al grupo de destino.
9. Configure el agente de escucha para que use su certificado. SSL/TLS

Tras configurar el equilibrador de carga, los clientes se comunican con el equilibrador de carga a través del receptor de puertos personalizado. A continuación, el equilibrador de carga se comunica con el servidor a través del puerto 5080.

Creación de un grupo de destino

1. Tras seleccionar Crear grupo de destino en el procedimiento anterior, accederá a la página Especificar los detalles del grupo para un nuevo grupo objetivo.
2. En la sección Configuración básica, introduzca la siguiente información:
 - En Elegir un tipo de destino, elija Direcciones IP.
 - En Nombre del grupo de destino, escriba el nombre del grupo de destino.
 - En cuanto al protocolo, su selección depende de si utiliza un ALB o un NLB.
 - Para un Network Load Balancer (NLB), elija TCP
 - Para un Application Load Balancer (ALB), elija HTTP
 - En Puerto, escriba **5080**.
 - En Tipo de dirección IP, elija ipv4.
 - En VPC, elija la VPC que ha creado para el servidor AS2 de Transfer Family.
3. En la sección Health checks, elige el protocolo Health Check.
 - Para un ALB, elija HTTP
 - Para un NLB, elija TCP
4. Elija Siguiente.
5. En la página Registrar objetivos, escriba la siguiente información:
 - Para Red, confirme que esté especificada la VPC que creó para el servidor AS2 de Transfer Family.
 - Para Dirección IPv4, introduzca la dirección IPv4 privada de los puntos de conexión de su servidor Transfer Family AS2.

Si tiene más de un punto de conexión para su servidor, elija Agregar dirección IPv4 para agregar otra fila e introducir otra dirección IPv4. Repita este proceso hasta que haya introducido las direcciones IP privadas de todos los puntos de conexión del servidor.

- Asegúrese de que Puertos esté configurado en **5080**.

- Seleccione Incluir como pendiente a continuación para añadir sus entradas a la sección Revisar objetivos.
6. En la sección Revisar objetivos, revise sus objetivos de IP.
 7. Seleccione Crear grupo de destino y, a continuación, vuelva al procedimiento anterior para crear su NLB e introduzca el nuevo grupo objetivo donde se indica.

Prueba del acceso al servidor desde una dirección IP elástica

Conéctese al servidor a través del puerto personalizado mediante una dirección IP elástica o el nombre DNS del equilibrador de carga de red.

Important

Administre el acceso al servidor desde las direcciones IP de los clientes mediante las [listas de control de acceso de la red \(ACL de la red\)](#) de las subredes configuradas en el equilibrador de carga. Los permisos de las ACL de red se establecen a nivel de subred, por lo que las reglas se aplican a todos los recursos que utilizan la subred. No puede controlar el acceso desde las direcciones IP de los clientes mediante grupos de seguridad, ya que el tipo de destino del equilibrador de carga se establece en Direcciones IP en lugar de en instancias. Por tanto, el equilibrador de carga no conserva las direcciones IP de origen. Si las [comprobaciones de estado del equilibrador de carga de red](#) fallan, significa que el equilibrador de carga no puede conectarse al punto de conexión del servidor. Para solucionar este problema, compruebe lo siguiente:

- Confirme que el [grupo de seguridad asociado al punto de conexión del](#) servidor permita las conexiones entrantes desde las subredes que están configuradas en el equilibrador de carga. El equilibrador de carga debe poder conectarse al punto de conexión del servidor a través del puerto 5080.
- Confirme que el Estado esté en línea.

Transferencia de archivos mediante un conector AS2

Los conectores AS2 establecen una relación entre los socios comerciales para las transferencias de mensajes de AS2 desde un servidor Transfer Family a un destino externo propiedad del socio.

Puedes usar Transfer Family para enviar mensajes AS2 haciendo referencia al ID del conector y a las rutas de acceso a los archivos, como se muestra en el siguiente comando `start-file-transfer` AWS Command Line Interface (AWS CLI):

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

Para obtener los detalles de los conectores, ejecute el siguiente comando:

```
aws transfer list-connectors
```

El comando `list-connectors` devuelve los ID de los conectores, las URL y los nombres de recursos de Amazon (ARN) de los conectores.

Para devolver las propiedades de un conector concreto, ejecute el siguiente comando con el ID que desee usar:

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

El comando `describe-connector` devuelve todas las propiedades del conector, incluidas la URL, los roles, los perfiles, los avisos de disposición de mensajes (MDNs), las etiquetas y las métricas de supervisión.

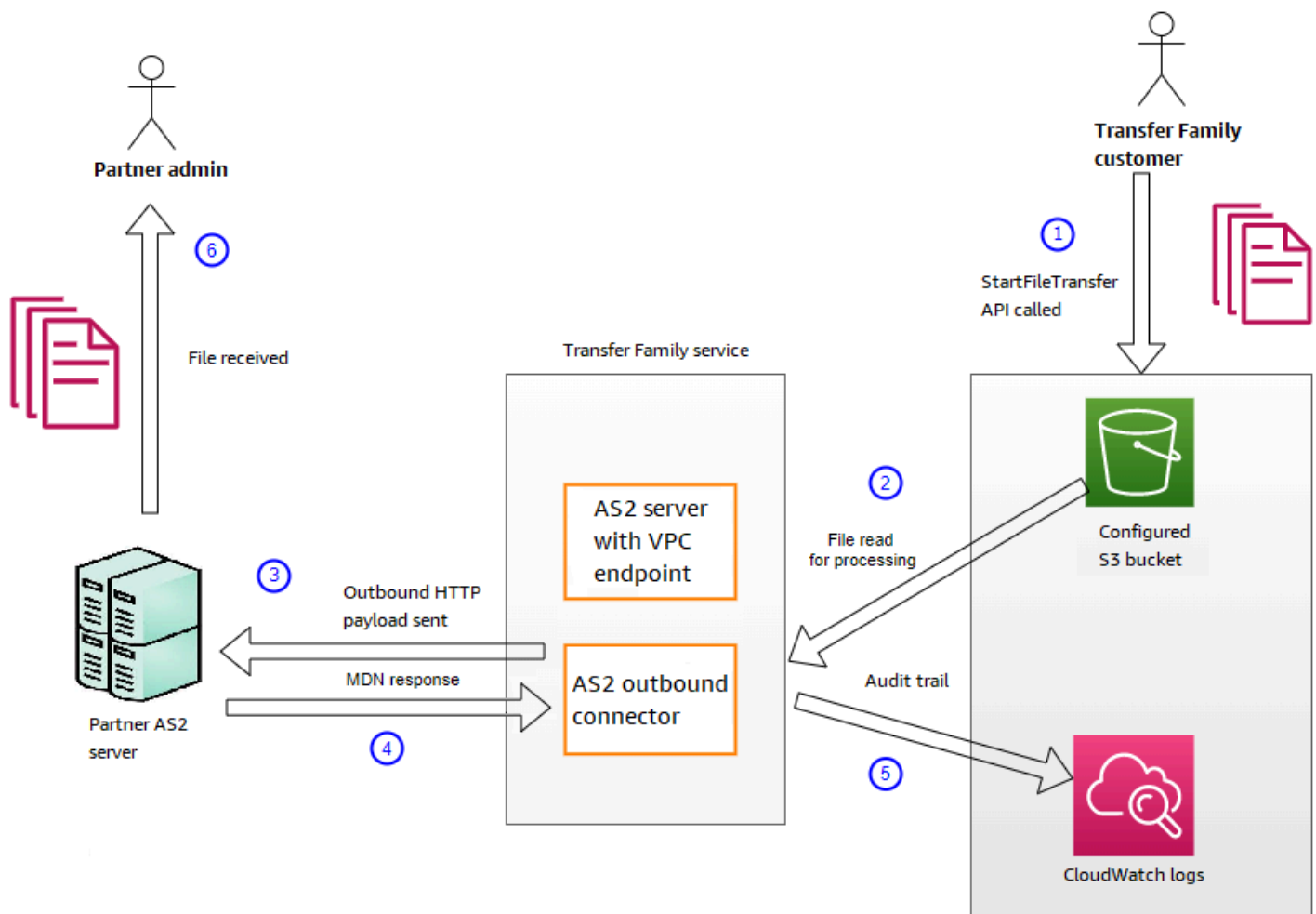
Para confirmar que el socio recibió correctamente los archivos, consulte los archivos JSON y MDN. Estos archivos se nombran de acuerdo con las convenciones descritas en [Nombres y ubicaciones de los archivos](#). Si configuró una función de registro al crear el conector, también puede comprobar en sus CloudWatch registros el estado de los mensajes AS2.

Para ver los detalles del conector AS2, consulte [Visualización de los detalles del conector AS2](#). Para obtener más información acerca de cómo crear un conector AS2, consulte [Configure los conectores AS2](#).

Para enviar un mensaje saliente de AS2

El proceso de salida se define como un mensaje o un archivo que se envía AWS a un cliente o servicio externo. La secuencia de los mensajes salientes es la siguiente:

1. Un administrador llama al comando `start-file-transfer` AWS Command Line Interface (AWS CLI) o a la operación de la `StartFileTransfer` API. Esta operación hace referencia a una configuración `connector`.
2. Transfer Family detecta una nueva solicitud de archivo y localiza el archivo. El archivo está comprimido, firmado y cifrado.
3. Un cliente HTTP de transferencia realiza una solicitud HTTP POST para transmitir la carga útil al servidor AS2 del socio.
4. El proceso devuelve la respuesta MDN firmada, ya sea en línea con la respuesta HTTP (MDN síncrona o asíncrona).
5. A medida que el archivo pasa de una fase a otra de la transmisión, el proceso entrega al cliente el recibo de respuesta MDN y los detalles del procesamiento.
6. El servidor AS2 remoto pone el archivo descifrado y verificado a disposición del administrador asociado.



El procesamiento AS2 es compatible con muchos de los protocolos RFC 4130 y se centra en los casos de uso comunes y en la integración con las implementaciones de servidores existentes. AS2-enabled Para más información sobre las configuraciones compatibles, consulte [Configuraciones AS2](#).

Nombres y ubicaciones de los archivos

En esta sección, se analizan las convenciones de nomenclatura de archivos para las transferencias de AS2.

En cuanto a las transferencias de archivos entrantes, tenga en cuenta lo siguiente:

- El directorio base se especifica en un acuerdo. El directorio base es el nombre del bucket de Amazon S3 combinado con un prefijo, si lo hubiera. Por ejemplo, **/amzn-s3-demo-bucket/AS2-folder**.
- Si un archivo entrante se procesa correctamente, el archivo (y el archivo JSON correspondiente) se guardan en la carpeta **/processed**. Por ejemplo, **/amzn-s3-demo-bucket/AS2-folder/processed**.

El archivo JSON contiene los siguientes campos:

- `agreement-id`
- `as2-from`
- `as2-to`
- `as2-message-id`
- `transfer-id`
- `client-ip`
- `connector-id`
- `failure-message`
- `file-path`
- `message-subject`
- `mdn-message-id`
- `mdn-subject`
- `requester-file-name`
- `requester-content-type`
- `server-id`
- `status-code`

- `failure-code`
- `transfer-size`
- Si un archivo entrante no se puede procesar correctamente, el archivo (y el archivo JSON correspondiente) se guardan en la carpeta `/failed`. Por ejemplo, `/amzn-s3-demo-bucket/AS2-folder/failed`.
- El archivo transferido se guarda en la carpeta `processed` como *`original_filename.messageId.original_extension`*. Es decir, el identificador del mensaje de la transferencia se añade al nombre del archivo, antes de su extensión original.
- Se crea un archivo JSON y se guarda como *`original_filename.messageId.original_extension`*.json. Además de añadir el identificador del mensaje, la cadena `.json` se añade al nombre del archivo transferido.
- Se crea un archivo de aviso de disposición de mensajes (MDN) y se guarda como *`original_filename.messageId.original_extension`*.mdn. Además de añadir el identificador del mensaje, la cadena `.mdn` se añade al nombre del archivo transferido.
- Si hay un archivo entrante con el nombre `ExampleFileInS3Payload.dat`, se crean los siguientes archivos:
 - File:
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
 - JSON:
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
 - MDN:
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`

En el caso de las transferencias salientes, el nombre es similar, con la diferencia de que no hay ningún archivo de mensajes entrantes y, además, el identificador de transferencia del mensaje transferido se añade al nombre del archivo. La operación de la `StartFileTransfer` API devuelve el identificador de transferencia (o cuando otro proceso o script llama a esta operación).

- El `transfer-id` es un identificador que está asociado a una transferencia de archivos. Todas las solicitudes que forman parte de una llamada `StartFileTransfer` comparten un `transfer-id`.
- El directorio base es el mismo que la ruta que se utiliza para el archivo fuente. Es decir, el directorio base es la ruta que se especifica en la operación o el comando de la `StartFileTransfer` API. `start-file-transfer` AWS CLI Por ejemplo:

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-bucket/AS2-folder/
file-to-send.txt
```

Si ejecutas este comando, los archivos MDN y JSON se guardan en /amzn-s3-demo-bucket/AS2-folder/processed (si las transferencias se realizan correctamente) o /amzn-s3-demo-bucket/AS2-folder/failed (si las transferencias no se realizan correctamente).

- Se crea un archivo JSON y se guarda como *original_filename.transferId.messageId.original_extension.json*.
- Se crea un archivo MDN y se guarda como *original_filename.transferId.messageId.original_extension.mdn*.
- Si hay un archivo de salida con nombre `ExampleFileOutTestOutboundSyncMdn.dat`, se crean los siguientes archivos:
 - JSON: `ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.json`
 - MDN: `ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.mdn`

También puedes consultar los CloudWatch registros para ver los detalles de tus transferencias, incluidas las que hayan fallado.

Códigos de estado

En la siguiente tabla se enumeran todos los códigos de estado que se pueden registrar en los CloudWatch registros cuando tú o tu pareja enviáis un mensaje AS2. Los diferentes pasos de procesamiento de mensajes se aplican a diferentes tipos de mensajes y están destinados únicamente a la supervisión. Los estados COMPLETADO y FALLIDO representan el paso final del procesamiento y están visibles en los archivos JSON.

Código	Description (Descripción)	¿Se ha completado el procesamiento?
PROCESAMIENTO	El mensaje está en proceso de convertirse a su formato final. Por ejemplo, los pasos	No

Código	Description (Descripción)	¿Se ha completado el procesamiento?
	de descompresión y descifrado o tienen este estado.	
MDN_TRANSMIT	El procesamiento de mensajes envía una respuesta de MDN.	No
MDN_RECEIVE	El procesamiento de mensajes recibe una respuesta de MDN.	No
COMPLETED	El procesamiento del mensaje se ha completado correctamente. Este estado incluye cuando se envía un MDN para un mensaje entrante o para la verificación por MDN de los mensajes salientes.	Sí
ERROR	Se ha producido un error en el procesamiento del mensaje. Para obtener una lista de códigos de error, consulte Códigos de error de AS2 .	Sí

Ejemplos de archivos de JSON

En esta sección, se enumeran los archivos JSON de muestra para las transferencias entrantes y salientes, incluidos los archivos de muestra para las transferencias correctas y las transferencias que no se realizan correctamente.

Ejemplo de archivo saliente que se transfirió correctamente:

```
{
  "requester-content-type": "application/octet-stream",
  "message-subject": "File xyzTest from MyCompany_OID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
```

```

"as2-from": "MyCompany_OID",
"connector-id": "c-c21c63ceaaf34d99b",
"status-code": "COMPLETED",
"disposition": "automatic-action/MDN-sent-automatically; processed",
"transfer-size": 3198,
"mdn-message-id": "OPENAS2-11072022063009+0000-df865189-1450-435b-9b8d-
d8bc0cee97fd@PartnerA_OID_MyCompany_OID",
"mdn-subject": "Message be18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa has been
accepted",
"as2-to": "PartnerA_OID",
"transfer-id": "dedf4601-4e90-4043-b16b-579af35e0d83",
"file-path": "/amzn-s3-demo-bucket/as2testcell10000/openAs2/
TestOutboundSyncMdn-9lmCr79hV.dat",
"as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa",
"timestamp": "2022-07-11T06:30:10.791274Z"
}

```

Ejemplo de archivo saliente que se transfirió sin éxito:

```

{
  "failure-code": "HTTP_ERROR_RESPONSE_FROM_PARTNER",
  "status-code": "FAILED",
  "requester-content-type": "application/octet-stream",
  "subject": "Test run from Id da86e74d6e57464aae1a55b8596bad0a to partner
9f8474d7714e476e8a46ce8c93a48c6c",
  "transfer-size": 3198,
  "requester-file-name": "openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "as2-message-id": "9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "failure-message": "http://Test123456789.us-east-1.elb.amazonaws.com:10080 returned
status 500 for message with ID 9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "transfer-id": "07bd3e07-a652-4cc6-9412-73ffdb97ab92",
  "connector-id": "c-056e15cc851f4b2e9",
  "file-path": "/amzn-s3-demo-bucket-4c1tq6ohjt9y/as2IntegCell10002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "timestamp": "2022-07-11T21:17:24.802378Z"
}

```

Ejemplo de archivo entrante que se ha transferido correctamente:

```

{
  "requester-content-type": "application/EDI-X12",
  "subject": "File openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat sent from MyCompany
to PartnerA",

```

```

"client-ip": "10.0.109.105",
"requester-file-name": "openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat",
"as2-from": "MyCompany_OID",
"status-code": "COMPLETED",
"disposition": "automatic-action/MDN-sent-automatically; processed",
"transfer-size": 1050,
"mdn-subject": "Message Disposition Notification",
"as2-message-id": "OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-fba84effff3c@MyCompany_OID_PartnerA_OID",
"as2-to": "PartnerA_OID",
"agreement-id": "a-f5c5cbea5f7741988",
"file-path": "processed/openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-fba84effff3c@MyCompany_OID_PartnerA_OID.dat",
"server-id": "s-5f7422b04c2447ef9",
"timestamp": "2022-07-11T23:36:36.105030Z"
}

```

Ejemplo de archivo entrante que se transfirió sin éxito:

```

{
  "failure-code": "INVALID_REQUEST",
  "status-code": "FAILED",
  "subject": "Sending a request from InboundHttpClientTests",
  "client-ip": "10.0.117.27",
  "as2-message-id": "testFailedLogs-TestRunConfig-Default-inbound-direct-integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "as2-to": "0beff6af56c548f28b0e78841dce44f9",
  "failure-message": "Unsupported date format: 2022/123/456T",
  "agreement-id": "a-0ceec8ca0a3348d6a",
  "as2-from": "ab91a398aed0422d9dd1362710213880",
  "file-path": "failed/01187f15-523c-43ac-9fd6-51b5ad2b08f3.testFailedLogs-TestRunConfig-Default-inbound-direct-integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "server-id": "s-0582af12e44540b9b",
  "timestamp": "2022-07-11T06:30:03.662939Z"
}

```

Personalice los encabezados HTTP para los mensajes AS2

Al enviar mensajes AS2 a socios comerciales, es posible que necesite personalizar los encabezados HTTP para cumplir requisitos específicos o mejorar la compatibilidad con la configuración del servidor AS2 de su socio. Esta CloudFormation plantilla crea una infraestructura que permite

personalizar los encabezados HTTP para los mensajes AS2 que se envíen. AWS Transfer Family Configura una función Amazon API Gateway y Lambda para que actúen como proxy, lo que permite la modificación dinámica de los encabezados requeridos por los servidores AS2 de los socios comerciales.

Utilice esta plantilla para hacer lo siguiente:

- Agregue encabezados HTTP personalizados a los mensajes AS2 salientes
- Reemplace los valores de encabezado predeterminados con valores personalizados

 Important

Tenga cuidado al anular los valores de encabezado predeterminados, ya que puede provocar errores de envío: se requieren algunos encabezados AS2.

- Garantice la compatibilidad con los socios comerciales que tienen requisitos de encabezado específicos

Descripción general de la plantilla

La plantilla crea los siguientes componentes principales:

- Función Lambda que procesa y reenvía mensajes AS2
- Una Amazon API Gateway para exponer la función Lambda
- Funciones y permisos de IAM para la función Lambda
- Recursos condicionales para la compatibilidad con HTTPS

El archivo de plantilla está disponible aquí: [Plantilla de encabezados HTTP dinámicos](#).

Cómo funciona

1. Amazon API Gateway recibe los mensajes AS2 entrantes de AWS Transfer Family.
2. La solicitud se reenvía a la función Lambda.
3. La función Lambda procesa la solicitud, añadiendo o modificando encabezados según sea necesario.
4. A continuación, la solicitud modificada se reenvía al servidor AS2 del socio.

5. La respuesta del servidor del socio se devuelve a través de Lambda y Amazon API Gateway a. AWS Transfer Family

Características principales de

- Modificación dinámica del encabezado: permite personalizar el encabezado del asunto y agregar otros encabezados necesarios.
- Soporte de protocolos: funciona con los protocolos HTTP y HTTPS.
- Configuración flexible: permite especificar el host, el puerto y la ruta del socio.

Detalles de la implementación

La plantilla implementa los siguientes componentes clave:

Función Lambda

El núcleo de la solución es una función Node.js Lambda que:

- Recibe solicitudes de Amazon API Gateway
- Modifica los encabezados en función de la configuración y los datos de las solicitudes entrantes
- Reenvía la solicitud modificada al servidor AS2 del socio
- Maneja los protocolos HTTP y HTTPS
- Incluye la gestión y el registro de errores

Amazon API Gateway

Una API HTTP está configurada para:

- Recibir mensajes AS2 entrantes
- Enrutar las solicitudes a la función Lambda
- Devuelva las respuestas a AWS Transfer Family

Parámetros de plantilla

Introduzca la información de los parámetros de la plantilla de la siguiente manera. Tenga en cuenta que todos estos parámetros son cadenas.

- **Environment:** este parámetro se usa para nombrar los recursos que crea la plantilla, independientemente de si están destinados a un entorno de desarrollo o producción. Los valores válidos son dev y prod.
- **PartnerHost:** la dirección IP o el nombre de host del servidor asociado de AS2.
- **PartnerPort:** el número de puerto del servidor asociado de AS2. Si no se especifica, el valor predeterminado es 80 para HTTP y 443 para HTTPS.
- **PartnerPath:** la ruta al punto final AS2 en el servidor asociado
- **ProtocolType:** el protocolo que se utilizará para la comunicación AS2: los valores válidos son HTTP y HTTPS.

Recursos condicionales

Para ser compatible con HTTPS, la plantilla crea de forma condicional:

- Una capa Lambda para certificados de CA
- HTTPS-specific configuración en la función Lambda

Despliegue y uso

Para personalizar los encabezados HTTP AS2 mediante una plantilla CloudFormation

1. Abra la CloudFormation consola en. <https://console.aws.amazon.com/cloudformation>
2. En el panel de navegación izquierdo, elija Pilas.
3. Elija Create stack (Crear pila), y, a continuación, elija With new resources (standard) (Con nuevos recursos [estándar]).
4. En la sección Requisitos previos: preparar una plantilla, elija Elegir una plantilla existente.
5. Copie este enlace, [plantilla de encabezados HTTP dinámicos](#), y péguelo en el campo URL de Amazon S3.
6. Elija Siguiente.
7. Rellene los detalles de los parámetros con su información. Estos se detallan en [Parámetros de plantilla](#).
8. Elija Siguiente. En la página Configurar opciones de pila, elija Siguiente.
9. Revise los detalles de la pila que está creando y, a continuación, seleccione Crear pila.

 Note

Al final de la página, en la sección Capacidades, debes reconocer que CloudFormation podrían crear recursos AWS Identity and Access Management (IAM).

Tras implementar esta CloudFormation pila:

1. Anote la URL del punto de conexión de Amazon API Gateway proporcionada en los resultados de la pila.
2. Actualice su AWS Transfer Family conector actual para usar este nuevo punto de conexión de Amazon API Gateway.
3. La solución ahora gestionará los mensajes AS2 y añadirá o modificará los encabezados según lo configurado.

 Warning

Modifique únicamente el encabezado del asunto o añada los encabezados que su pareja espere explícitamente. Cambiar otros encabezados puede provocar errores en la transferencia.

Monitorización del uso de AS2

Puede supervisar la actividad de AS2 mediante Amazon CloudWatch y AWS CloudTrail. Para ver otras métricas del servidor de Transfer Family, consulte [CloudWatch Registro de Amazon para AWS Transfer Family servidores](#).

métricas de AS2

Métrica	Description (Descripción)
InboundMessage	El número total de mensajes AS2 recibidos correctamente de un socio comercial. Unidades: recuento

Métrica	Description (Descripción)
	Periodo: 5 minutos
InboundFailedMessage	El número total de mensajes AS2 que se recibieron sin éxito de un socio comercial. Es decir, un socio comercial envió un mensaje, pero el servidor de Transfer Family no pudo procesarlo correctamente. Unidades: recuento Periodo: 5 minutos
OutboundMessage	Número total de mensajes AS2 enviados correctamente desde el servidor de Transfer Family a un socio comercial. Unidades: recuento Periodo: 5 minutos
OutboundFailedMessage	El número total de mensajes AS2 que se enviaron sin éxito a un socio comercial. Es decir, se enviaron desde el servidor de Transfer Family, pero el socio comercial no los recibió correctamente. Unidades: recuento Periodo: 5 minutos

Métrica	Description (Descripción)
DaysUntilExpiry	El número de días que faltan para que caduque un certificado se determina según lo <code>InactiveDate</code> establecido en el certificado en el momento de la importación. Unidades: recuento Dimensiones: <code>CertificateId</code> <code>Description</code> (si se proporcionan) Periodo: 1 día Para obtener más información, consulte Rotación de certificado AS2.

Códigos de estado AS2

En la siguiente tabla se enumeran todos los códigos de estado que se pueden registrar en los CloudWatch registros cuando usted o su pareja envían un mensaje AS2. Los diferentes pasos de procesamiento de mensajes se aplican a diferentes tipos de mensajes y están destinados únicamente a la supervisión. Los estados COMPLETADO y FALLIDO representan el paso final del procesamiento y están visibles en los archivos JSON.

Código	Description (Descripción)	¿Se ha completado el procesamiento?
PROCESAMIENTO	El mensaje está en proceso de convertirse a su formato final. Por ejemplo, los pasos de descompresión y descifrado tienen este estado.	No
MDN_TRANSMIT	El procesamiento de mensajes envía una respuesta de MDN.	No

Código	Description (Descripción)	¿Se ha completado el procesamiento?
MDN_RECEIVE	El procesamiento de mensajes recibe una respuesta de MDN.	No
COMPLETED	El procesamiento del mensaje se ha completado correctamente. Este estado incluye cuando se envía un MDN para un mensaje entrante o para la verificación por MDN de los mensajes salientes.	Sí
ERROR	Se ha producido un error en el procesamiento del mensaje. Para obtener una lista de códigos de error, consulte Códigos de error de AS2 .	Sí

Códigos de error de AS2

En la siguiente tabla se enumeran y describen los códigos de error que puede recibir de las transferencias de archivos AS2.

Códigos de error de AS2

Código	Error	Descripción y resolución
ACCESS_DENIED	- Acceso denegado. Compruebe si su rol de acceso tiene los permisos necesarios. - Ruta de archivo no válida <i>send-file-path</i>	Se produce al gestionar una solicitud StartFile Transfer en la que alguna de SendFilePaths no es válido o tiene un formato incorrecto. Es decir, a la ruta, le falta el nombre del bucket de Amazon S3 o la

Código	Error	Descripción y resolución
	No se pudieron obtener las credenciales con ErrorCode : <i>error-code</i>	ruta incluye caracteres que no son válidos. También ocurre si Transfer Family no asume el rol de acceso o el rol de registro. Asegúrese de que la ruta contiene un nombre de bucket de Amazon S3 y un nombre de clave válidos.
AGREEMENT_NOT_FOUND	No se ha encontrado el acuerdo.	No se ha encontrado el acuerdo o está asociado a un perfil inactivo. Actualice el acuerdo en el servidor Transfer Family para incluir los perfiles activos.
CONNECTOR_NOT_FOUND	No se ha encontrado el conector o la configuración relacionada.	No se ha encontrado el conector o está asociado a un perfil inactivo. Actualice el conector para incluir los perfiles activos.

Código	Error	Descripción y resolución
CREDENTIALS_RETRIEVAL_FAILED	1. No se ha encontrado el secreto en Secrets Manager. 2. No se puede acceder a Secrets Manager. 3. Error al eliminar el secreto en Secrets Manager. 4. No se puede obtener el valor secreto debido a la limitación.	Para la autenticación AS2 Basic, el secreto debe tener el formato correcto. Las siguientes resoluciones corresponden a los errores enumerados en la columna anterior. 1. Asegúrese de que el identificador secreto sea correcto. 2. Asegúrese de que el rol de acceso tenga los permisos adecuados para leer el secreto. Por tanto, debe proporcionar acceso de lectura y escritura al directorio principal de la ubicación del archivo que se usa en la solicitud <code>StartFileTransfer</code> . Además, asegúrese de que el rol proporcione acceso de lectura y escritura al directorio principal de los archivos que desea enviar con <code>StartFileTransfer</code> . 3. Si se utiliza una clave administrada por el cliente como secreto, asegúrese de que el rol de acceso tenga permisos para la clave AWS Key

Código	Error	Descripción y resolución
		Management Service (AWS KMS). 4. Para conocer las cuotas aplicables, consulte Cuotas de manejo de secretos.
DECOMPRESSION_FAILED	No se pudo descomprimir el mensaje.	El archivo enviado está dañado o el algoritmo de compresión no es válido. Vuelva a enviar el mensaje y compruebe que se utiliza la compresión ZLIB o vuelva a enviar el mensaje sin la compresión habilitada.
DECRYPT_FAILED	No se pudo descifrar el mensaje <i>message-ID</i> . Asegúrese de que el socio tenga la clave de cifrado pública correcta.	Falló el descifrado. Confirme que el socio envió una carga útil mediante un certificado válido y que el cifrado se realizó mediante un algoritmo de cifrado válido.
DECRYPT_FAILED_INVALID_SMIME_FORMAT	No se pudo analizar el mimePart envuelto.	La carga MIME está dañada o tiene un formato SMIME que no es compatible. El remitente debe asegurarse de que el formato que está utilizando es compatible y, a continuación, volver a enviar la carga útil.

Código	Error	Descripción y resolución
DECRYPT_FAILED_NO_DECRYPTION_KEY_FOUND	No se ha encontrado ninguna clave de descifrado coincidente.	El perfil del socio no tenía asignado un certificado que coincidiera con el mensaje, o los certificados que coincidían con el mensaje han caducado o han dejado de ser válidos. Debe actualizar el perfil del socio y asegurarse de que contiene un certificado válido.
DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG	El descifrado de la carga útil SMIME se solicitó mediante un algoritmo no compatible con el identificador: <i>encryption-ID</i>	El remitente remoto ha enviado una carga útil de AS2 con un algoritmo de cifrado no compatible. El remitente debe elegir un algoritmo de cifrado compatible con AWS Transfer Family.
DUPLICATE_MESSAGE	Paso duplicado o procesado dos veces.	La carga útil tiene un paso de procesamiento duplicado. Por ejemplo, hay dos pasos de cifrado. Vuelva a enviar el mensaje con un solo paso para firmarlo, comprimirlo y cifrarlo.

Código	Error	Descripción y resolución
ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND	No se encontraron certificados de cifrado públicos válidos en el perfil: <i>local-profile-ID</i>	Transfer Family está intentand o cifrar un mensaje saliente, pero no se encuentra ningún certificado de cifrado para el perfil local. Opciones de resolución: • Asegúrese de que el perfil local tenga adjuntos un certificado y una clave privada para el cifrado. • Asegúrese de que el certificado de cifrado esté activo actualmente.
ENCRYPTION_FAILED	No se pudo cifrar el archivo <i>file-name</i> .	El archivo que se va a enviar no está disponible para el cifrado. Compruebe que el archivo se encuentra en la ubicación AS2 esperada y que AWS Transfer Family tiene permiso para leerlo.
FILE_SIZE_TOO_LARGE	El tamaño del archivo es demasiado grande.	Esto ocurre al enviar o recibir un archivo que supera el límite de tamaño de archivo.

Código	Error	Descripción y resolución
HTTP_ERROR_RESPONSE_FROM_PARTNER	<i>partner-URL</i> devolvió el estado 400 para un mensaje con <i>message-ID</i> ID=.	La comunicación con el servidor AS2 del socio devolvió un código de respuesta HTTP inesperado. Es posible que el socio pueda proporcionar más diagnósticos a partir de los registros de su servidor AS2.
INSUFFICIENT_MESSAGE_SECURITY_UNENCRYPTED	Se requiere el cifrado.	El socio envió un mensaje sin cifrar a Transfer Family, lo cual no es compatible. El remitente debe usar una carga cifrada.
INVALID_ENDPOINT_PROTOCOL	Solo se admiten HTTP y HTTPS.	Debe especificar HTTP o HTTPS como protocolo en la configuración de su conector de AS2.

Código	Error	Descripción y resolución
INVALID_REQUEST	- Hay un problema con el encabezado de un mensaje. - No se han podido analizar el JSON secreto. El JSON secreto no coincidía con el formato esperado. - Secret debe ser una cadena JSON. - El nombre de usuario no debe contener dos puntos. El nombre de usuario no debe contener caracteres de control. El nombre de usuario solo debe contener caracteres ASCII. La contraseña no debe contener caracteres de control. La contraseña solo debe contener caracteres ASCII.	Este error se debe a varias causas. Las siguientes resoluciones corresponden a los errores enumerados en la columna anterior. - Compruebe los campos as2-from y as2-to. Asegúrese de que la ID del mensaje original sea correcta para el formato MDN. Asegúrese también de que al formato de ID del mensaje no le falte ningún encabezado de AS2. - Asegúrese de que el valor secreto coincida con el formato documentado, tal y como se describe en Habilite la autenticación básica para los conectores AS2. - Asegúrese de que el secreto se proporciona como cadena y no como binario. - Realice las correcciones necesarias en el nombre de usuario o la contraseña.

Código	Error	Descripción y resolución
INVALID_URL_FORMAT	Formato de URL no válido: <i>URL</i>	Esto ocurre cuando se envía un mensaje saliente mediante un conector configurado con una URL mal formada. Asegúrese de que el conector está configurado con una dirección HTTP o HTTPS válida.
MDN_RESPONSE_INDICATIONS_AUTHENTICATION_FAILED	No aplicable	El receptor no puede autenticar al remitente. El socio comercial devuelve un MDN a Transfer Family con el modificador de disposición Error: authentication-failed.
MDN_RESPONSE_INDICATIONS_DECOMPRESSION_FAILED	No aplicable	Esto ocurre cuando el receptor no puede descomprimir el contenido del mensaje. El socio comercial devuelve un MDN a Transfer Family con el modificador de disposición Error: decompression-failed.
MDN_RESPONSE_INDICATIONS_DECRYPTION_FAILED	No aplicable	El receptor no puede descifrar el contenido del mensaje. El socio comercial devuelve un MDN a Transfer Family con el modificador de disposición Error: authentication-failed.

Código	Error	Descripción y resolución
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	No aplicable	El destinatario espera que el mensaje esté firmado o cifrado, pero no es así. El socio comercial devuelve un MDN a Transfer Family con el modificador de disposición Error: insufficient-message-security. Habilite el and/or cifrado de firmas en el conector para que se ajuste a las expectativas del socio comercial.
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	No aplicable	El receptor no puede verificar la integridad del contenido. El socio comercial devuelve un MDN a Transfer Family con el modificador de disposición Error: integrity-checkfailed.
PATH_NOT_FOUND	No se pudo crear el directorio o <i>file-path</i> . No se ha encontrado la ruta principal.	Transfer Family está intentando crear un directorio en el bucket de Amazon S3 del cliente, pero no lo encuentra. Asegúrese de que cada ruta mencionada en el comando <code>StartFileTransfer</code> contiene el nombre de un bucket existente.

Código	Error	Descripción y resolución
SEND_FILE_NOT_FOUND	<i>file-path</i> No se encontró la ruta del archivo.	Transfer Family no encuentra el archivo en la operación de envío de archivos. Compruebe que el directorio de inicio y la ruta configurados sean válidos y que Transfer Family tenga permisos de lectura para el archivo.
SERVER_NOT_FOUND	No se encuentra el servidor asociado al mensaje.	Transfer Family no pudo encontrar el servidor al recibir un mensaje. Esto puede suceder si se elimina el servidor durante el procesamiento de un mensaje entrante.
SERVER_NOT_ONLINE	<i>server-ID</i> El servidor no está en línea.	El servidor Transfer Family está desconectado. Inicie el servidor para que pueda recibir y procesar mensajes.
SIGNING_FAILED	No se ha podido firmar el archivo.	El archivo que se va a enviar no está disponible para su firma o no se pudo realizar la firma. Compruebe que el archivo se encuentra en la ubicación AS2 esperada y que AWS Transfer Family tiene permiso para leerlo.

Código	Error	Descripción y resolución
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	No se encontró ningún certificado para el perfil: <i>local-profile-ID</i> .	Se está intentando firmar un mensaje saliente, pero no se encuentra ningún certificado de firma para el perfil local. Opciones de resolución: • Asegúrese de que el perfil local tenga adjuntos un certificado y una clave privada para el firma. • Asegúrese de que el certificado de firma esté activo actualmente.
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	No se puede resolver el nombre de host en las direcciones IP.	Transfer Family no puede realizar la resolución de DNS a dirección IP en el servidor DNS público que está configurado en el conector de AS2. Actualice el conector para que apunte a una URL asociada válida.
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	Se agotó el tiempo de espera de la conexión al punto de conexión.	Transfer Family no puede establecer una conexión de socket con el servidor AS2 del socio configurado. Compruebe que el servidor AS2 del socio esté disponible en la dirección IP configurada.

Código	Error	Descripción y resolución
UNABLE_TO_RESOLVE_HOSTNAME	No se puede resolver el nombre de host <i>hostname</i> .	El servidor Transfer Family no pudo resolver el nombre de host del socio mediante un servidor DNS público. Compruebe que el host configurado esté registrado y que el registro DNS haya tenido tiempo de publicarse.
VERIFICATION_FAILED	No se pudo comprobar la firma del mensaje AS2 <i>message-ID</i> o el código MIC no coincidía.	Compruebe que el certificado de firma del remitente coincide con los certificados de firma del perfil remoto. Compruebe también que los algoritmos MIC sean compatibles con AWS Transfer Family.

Código	Error	Descripción y resolución
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	- No se encontró ningún certificado público que coincida con la firma del mensaje en el perfil:<i>partner-profile-ID</i> . - No se pueden obtener certificados para un perfil inexistente:<i>partner-profile-ID</i> . - No se encontró ningún certificado válido en el perfil:<i>partner-profile-ID</i> .	AWS Transfer Family está intentando verificar la firma de un mensaje recibido, pero no se ha encontrado ningún certificado de firma que coincida con el perfil del socio. Opciones de resolución: - Asegúrese de que el perfil del socio tenga un certificado de firma adjunto. - Asegúrese de que el certificado esté activo actualmente. - Asegúrese de que el certificado sea el certificado de firma correcto para el socio.

Supervisión de caducidad de certificados

AWS Transfer Family supervisa automáticamente las fechas de caducidad de los certificados AS2 y publica una CloudWatch métrica de Amazon para ayudarte a hacer un seguimiento de cuándo los certificados se acercan a su fecha de caducidad. Esto le permite gestionar de forma proactiva las renovaciones de certificados y evitar interrupciones en el servicio.

DaysUntilExpiry métrica

Al importar un certificado para su uso en AS2, Transfer Family crea automáticamente una CloudWatch métrica llamada `DaysUntilExpiry`. Esta métrica registra el número de días que quedan hasta que caduque el certificado en función de `InactiveDate` lo que especificó al importar el certificado.

Detalles de la métrica:

- Nombre de la métrica: `DaysUntilExpiry`
- Espacio de nombres: `AWS/Transfer`
- Dimensiones: `CertificateId` (siempre presentes), `Description` (si se proporcionaron durante la importación del certificado)
- Unidades: Recuento (días)
- Frecuencia: Se publica a diario

 Important

Transfer Family puede tardar hasta un día completo en emitir esta métrica a tu cuenta después de importar un certificado.

El valor de la métrica disminuye en uno cada día a medida que el certificado se acerca a su fecha de inactividad. Por ejemplo, si un certificado tiene 30 días hasta su caducidad, la métrica mostrará 30, 29 al día siguiente y así sucesivamente.

Prácticas recomendadas para la supervisión de certificados

Siga estas prácticas recomendadas al configurar la supervisión de la caducidad de los certificados:

- Establezca varios umbrales de alerta: cree alarmas para distintos períodos de tiempo (por ejemplo, 30 días, 14 días y 7 días antes del vencimiento) a fin de disponer del tiempo suficiente para la renovación del certificado.
- Utilice las estadísticas adecuadas: utilice la `Maximum` estadística al crear alarmas para asegurarse de capturar el valor de la métrica más reciente.
- Configure las acciones de alarma adecuadas: configure las notificaciones para alertar a los miembros del equipo correspondientes sobre la posibilidad de renovar los certificados.
- Pruebe sus alertas: pruebe periódicamente su sistema de notificaciones para asegurarse de que las alertas se envíen correctamente.
- Documente su proceso: conserve la documentación sobre el proceso de renovación de su certificado y sobre quién es responsable de los distintos certificados.

Ejemplos de configuraciones de alarma

Estos son algunos ejemplos de configuraciones de alarma para diferentes escenarios de notificación:

Advertencia de caducidad de 30 días

Cree una alarma que se active cuando un certificado tenga 30 días o menos hasta que caduque:

- Métrica: DaysUntilExpiry
- Estadística: Maximum
- Periodo: 1 día
- Umbral: 30
- Comparación: inferior o igual al umbral
- Tratamiento de datos faltantes: trate los datos faltantes como buenos (sin infringirlos)

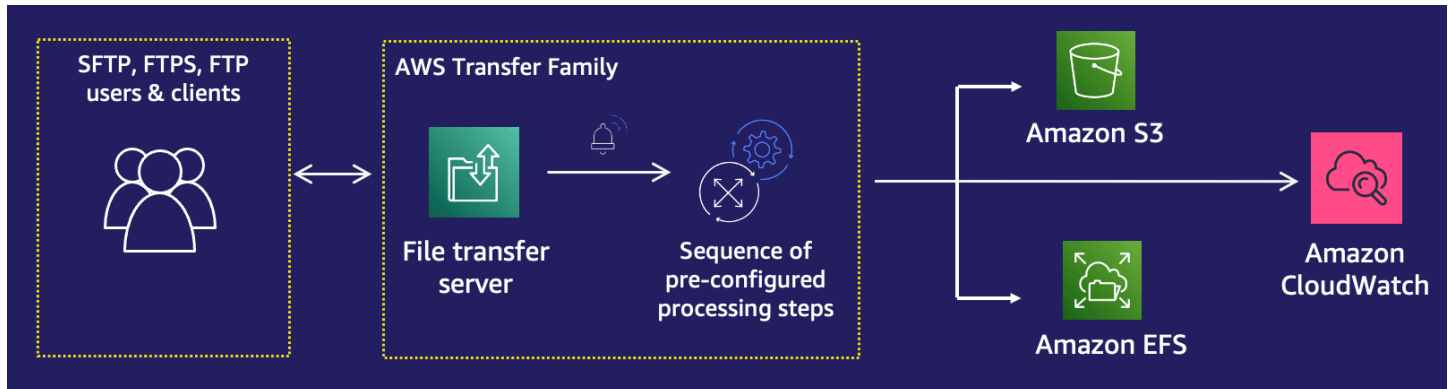
Advertencia crítica de caducidad de 7 días

Cree una alarma crítica que se active cuando un certificado tenga 7 días o menos hasta que caduque:

- Métrica: DaysUntilExpiry
- Estadística: Maximum
- Periodo: 1 día
- Umbral: 7
- Comparación: inferior o igual al umbral
- Tratamiento de datos faltantes: trate los datos faltantes como buenos (sin infringirlos)

AWS Transfer Family flujos de trabajo gestionados

AWS Transfer Family admite flujos de trabajo gestionados para el procesamiento de archivos. Con los flujos de trabajo administrados, puede iniciar un flujo de trabajo después de transferir un archivo a través de SFTP, FTPS, FTP. Con esta característica, puede cumplir de forma segura y rentable sus requisitos de conformidad para el intercambio de archivos business-to-business (B2B, entre empresas) coordinando todos los pasos necesarios para el procesamiento de archivos. Además, se beneficia de la auditoría integral y de la visibilidad.



Al organizar las tareas de procesamiento de archivos, los flujos de trabajo administrados lo ayudan a preprocesar los datos antes de que los consuman las aplicaciones posteriores. Estas tareas de procesamiento de archivos pueden incluir lo siguiente:

- Mover archivos a carpetas específicas del usuario.
- Descifrado de archivos como parte de un flujo de trabajo.
- Etiquetado de archivos.
- Realizar un procesamiento personalizado creando y adjuntando una AWS Lambda función a un flujo de trabajo.
- Enviar notificaciones cuando un archivo ha sido transferido correctamente. (Para ver una entrada de blog que detalle este caso de uso, consulte [Personalizar las notificaciones de entrega de archivos mediante flujos de trabajo AWS Transfer Family gestionados](#)).

Para replicar y estandarizar rápidamente las tareas comunes de procesamiento de archivos posteriores a la carga que abarcan varias unidades de negocio de su organización, puede implementar flujos de trabajo mediante la infraestructura como código (IaC). Puede especificar que se inicie un flujo de trabajo administrado en los archivos que se carguen en su totalidad. También puede especificar que se inicie un flujo de trabajo gestionado diferente en los archivos que se

carguen solo parcialmente debido a una desconexión prematura de la sesión. Built-in la gestión de excepciones le ayuda a reaccionar rápidamente ante los resultados del procesamiento de archivos y, al mismo tiempo, le ofrece el control sobre cómo gestionar los errores. Además, cada paso del flujo de trabajo produce registros detallados, que puede auditar para rastrear el linaje de datos.

Para comenzar, realice los siguientes pasos:

1. Configure su flujo de trabajo para que contenga las acciones de preprocesamiento, como copiar, etiquetar y otros pasos, en función de sus necesidades. Para obtener más información, consulte [Crear un flujo de trabajo](#).
2. Configure un rol de ejecución, que Transfer Family utilizará para ejecutar el flujo de trabajo. Para obtener más información, consulte [Políticas de IAM para flujos de trabajo](#).
3. Asigne el flujo de trabajo a un servidor para que, al llegar el archivo, las acciones especificadas en este flujo de trabajo se evalúen y se inicien en tiempo real. Para obtener más información, consulte [Configuración y ejecución de un flujo de trabajo](#).

Información relacionada

- Para supervisar las ejecuciones del flujo de trabajo, consulte [Uso de CloudWatch métricas para servidores Transfer Family](#).
- Para obtener registros de ejecución detallados e información sobre la solución de problemas, consulte [Solucionar errores relacionados con el flujo de trabajo con Amazon CloudWatch](#).
- Transfer Family ofrece una entrada de blog y un taller que lo guiarán a través de la creación de una solución de transferencia de archivos. Esta solución aprovecha los SFTP/FTPS puntos AWS Transfer Family de conexión gestionados y Amazon Cognito y DynamoDB para la gestión de usuarios.

La entrada del blog está disponible en [Uso de Amazon Cognito como proveedor de identidad con Amazon AWS Transfer Family S3](#). Puede ver los detalles del taller [aquí](#).

- Consulte [Flujos de trabajo administrados de AWS Transfer Family](#) para ver una breve introducción a los flujos de trabajo de Transfer Family.
- [El siguiente taller ofrece laboratorios prácticos para crear flujos de trabajo totalmente automatizados y basados en eventos que implican la transferencia de archivos hacia o desde servidores SFTP externos a Amazon S3, y el procesamiento previo y posterior común de esos archivos: taller de MFT. Event-driven](#)

En este vídeo se ofrece un recorrido por este taller.

Temas

- [Crear un flujo de trabajo](#)
- [Utilice pasos predefinidos](#)
- [Uso de pasos de procesamiento de archivos personalizados](#)
- [Políticas de IAM para flujos de trabajo](#)
- [Gestión de excepciones para un flujo de trabajo](#)
- [Monitoreo de la ejecución del flujo](#)
- [Creación de un flujo de trabajo a partir de una plantilla](#)
- [Eliminación de un flujo de trabajo de un servidor de Transfer Family](#)
- [Restricciones y limitaciones de los flujos de trabajo administrados](#)

Para obtener más ayuda sobre cómo empezar a utilizar los flujos de trabajo administrados, consulte los siguientes recursos:

- AWS Transfer Family vídeo de demostración [de flujos de trabajo gestionados](#)
- Entrada de blog [sobre cómo crear una plataforma de transferencia de archivos nativa de la nube mediante AWS Transfer Family flujos de trabajo](#)

Crear un flujo de trabajo

Puede crear un flujo de trabajo gestionado mediante el Consola de administración de AWS, tal y como se describe en este tema. Para simplificar al máximo el proceso de creación de flujos de trabajo, existen paneles de ayuda contextual disponibles para la mayoría de las secciones de la consola.

Un flujo de trabajo consta de dos tipos de pasos:

- Pasos nominales: los pasos nominales son pasos de procesamiento de archivos que desea aplicar a los archivos entrantes. Si selecciona más de un paso nominal, cada paso se procesa en una secuencia lineal.
- Exception-handling pasos: los controladores de excepciones son pasos de procesamiento de archivos que se AWS Transfer Family ejecutan en caso de que algún paso nominal falle o provoque errores de validación.

Crear un flujo de trabajo

1. Abra la consola en. AWS Transfer Family <https://console.aws.amazon.com/transfer/>
2. En el panel de navegación izquierdo, seleccione Flujos de trabajo.
3. En la página Flujos de trabajo, seleccione Crear flujo de trabajo.
4. En la página Crear flujo de trabajo, escriba una descripción. Esta descripción aparece en la página Flujos de trabajo.
5. En la sección Pasos nominales, seleccione Añadir paso. Añada uno o más pasos.
 - a. Elija un tipo de paso entre las opciones disponibles. Para obtener más información acerca de los diferentes tipos de paso, consulte [the section called “Utilice pasos predefinidos”](#).
 - b. Seleccione Siguiente y, a continuación, configure los parámetros del paso.
 - c. Seleccione Siguiente y, a continuación, revise los detalles del paso.
 - d. Seleccione Crear paso para añadir el paso y continuar.
 - e. Siga añadiendo los pasos que necesite. El número máximo de pasos en un flujo de trabajo es 8.
 - f. Tras añadir todos los pasos nominales necesarios, desplácese hacia abajo hasta la sección Controladores de excepciones: opcional y seleccione Añadir paso.

Note

Para estar informado de los errores en tiempo real, le recomendamos que configure los controladores de excepciones y los pasos que se ejecuten cuando se produzca un error en el flujo de trabajo.

6. Para configurar los controladores de excepciones, añada los pasos de la misma manera que se describió anteriormente. Si un archivo provoca que algún paso genere una excepción, los controladores de excepciones se invocan uno por uno.
7. (Opcional) Desplácese hacia abajo hasta la sección Etiquetas y añada etiquetas a su flujo de trabajo.
8. Revise la configuración y seleccione Crear flujo de trabajo.

 Important

Una vez que haya creado un flujo de trabajo, no podrá editarlo, así que asegúrese de revisar la configuración detenidamente.

Configuración y ejecución de un flujo de trabajo

Antes de poder ejecutar un flujo de trabajo, debe asociarlo a un servidor de Transfer Family.

Configuración de Transfer Family para ejecutar un flujo de trabajo en los archivos cargados

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Servidores.
 - Para añadir el flujo de trabajo a un servidor existente, seleccione el servidor que desee utilizar para el flujo de trabajo.
 - También puede crear un servidor nuevo y agregarle el flujo de trabajo. Para obtener más información, consulte [Configuración de un punto final de servidor SFTP, FTPS o FTP](#).
3. En la página de detalles del servidor, desplácese hacia abajo hasta la sección Detalles adicionales y, a continuación, seleccione Editar.

 Note

De forma predeterminada, los servidores no tienen ningún flujo de trabajo asociado. Utilice la sección Detalles adicionales para asociar un flujo de trabajo al servidor seleccionado.

4. En la página Editar detalles adicionales, en la sección Flujos de trabajo administrados, seleccione un flujo de trabajo para que se ejecute en todas las cargas.

 Note

Si aún no tiene un flujo de trabajo, seleccione Crear un nuevo flujo de trabajo para crear uno.

- a. Elija el ID del flujo de trabajo que desee utilizar.
- b. Seleccione un rol de ejecución. Este es el rol que asume Transfer Family al ejecutar los pasos del flujo de trabajo. Para obtener más información, consulte [Políticas de IAM para flujos de trabajo](#). Seleccione Save.

Managed workflows [Info](#)

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

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

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

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

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

[dropdown] [refresh]

Note

Si ya no desea que un flujo de trabajo esté asociado al servidor, puede eliminar la asociación. Para obtener más información, consulte [Eliminación de un flujo de trabajo de un servidor de Transfer Family](#).

Ejecución de un flujo de trabajo

Para ejecutar un flujo de trabajo, debe cargar un archivo en un servidor de Transfer Family que haya configurado con un flujo de trabajo asociado.

Note

Cada vez que elimine un flujo de trabajo de un servidor y lo reemplace por uno nuevo o actualice la configuración del servidor (lo que afecta al rol de ejecución del flujo de trabajo), debe esperar, aproximadamente, 10 minutos antes de ejecutar el nuevo flujo de trabajo.

El servidor de Transfer Family almacena en caché los detalles del flujo de trabajo y tarda 10 minutos en actualizar su caché.

Además, debe cerrar sesión en cualquier sesión de SFTP activa y volver a iniciarla después del período de espera de 10 minutos para ver los cambios.

Example

```
# Execute a workflow
> sftp bob@s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com

Connected to s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com.
sftp> put doc1.pdf
Uploading doc1.pdf to /amzn-s3-demo-bucket/home/users/bob/doc1.pdf
doc1.pdf                                     100% 5013KB
 601.0KB/s   00:08
sftp> exit
>
```

Una vez cargado el archivo, la acción definida se lleva a cabo en su archivo. Por ejemplo, si su flujo de trabajo contiene un paso de copiado, el archivo se copia en la ubicación que definió en ese paso. Puede usar Amazon CloudWatch Logs para realizar un seguimiento de los pasos que se ejecutaron y su estado de ejecución.

Visualización de flujos de trabajo

Puede ver los detalles de los flujos de trabajo creados anteriormente o de las ejecuciones de los flujos de trabajo. Para ver estos detalles, puede usar la consola o el AWS Command Line Interface (AWS CLI).

Console

Visualización de flujos de trabajo

1. Abre la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Flujos de trabajo.
3. En la página Flujos de trabajo, elija un flujo de trabajo.

Se abrirá la página de detalles del flujo de trabajo.

The screenshot shows the AWS Transfer Family console interface. On the left is a navigation sidebar with links to Servers, Connectors, AS2 Trading Partners, Certificates, Profiles, Workflows (selected), Feature Spotlight, What's New, and Documentation. The main content area displays details for a specific workflow. At the top, there's a breadcrumb trail: Transfer Family > Workflows > w-1234567890abcdef0. A 'Delete' button is in the top right. The 'Description' section shows the workflow name 'Test my workflow' and a description 'Test workflow A'. Below this is the 'Nominal steps (1)' section, which contains a table with one step: a TAG step named 'tag_step'. The 'Exception handlers (1)' section contains a table with one handler: a DELETE handler named 'delete_if_exception'. The 'In-flight executions (0)' section shows a search bar and a table with no data, indicating no executions are currently running. At the bottom, the 'Tags (1)' section includes a 'Manage tags' button and a note about using tags to organize workflows.

CLI

Para ver los detalles del flujo de trabajo, utilice el comando de la CLI `describe-workflow`, tal y como se muestra en el siguiente ejemplo. Reemplace el ID del flujo de trabajo `w-1234567890abcdef0` con su propio valor. Para obtener más información, consulte [describe-workflow](#) en la Referencia de comando de AWS CLI .

```
# View Workflow details
> aws transfer describe-workflow --workflow-id w-1234567890abcdef0
{
  "Workflow": {
    "Arn": "arn:aws:transfer:us-east-1:111122223333:workflow/w-1234567890abcdef0",
    "WorkflowId": "w-1234567890abcdef0",
    "Name": "Copy file to shared_files",
    "Steps": [
      {
```

```
        "Type": "COPY",
        "CopyStepDetails": {
          "Name": "Copy to shared",
          "FileLocation": {
            "S3FileLocation": {
              "Bucket": "amzn-s3-demo-bucket",
              "Key": "home/shared_files/"
            }
          }
        }
      },
      "OnException": {}
    ]
  }
}
```

Si el flujo de trabajo se creó como parte de una AWS CloudFormation pila, puede gestionarlo mediante la CloudFormation consola () <https://console.aws.amazon.com/cloudformation>.

Transfer Family > Workflows > w-

W-

Delete

This workflow belongs to the AWS CloudFormation stack **stack-transfer-notifications-blog**. [Manage this stack](#) on the CloudFormation console.

Description

Name

Stack-managed

Workflow description

Workflow for blogpost

Nominal steps (4) Info

Number	Description	Type	Configuration
1	Lambda	CUSTOM	Details
2	CopyFile	COPY	Details
3	TagFileNotified	TAG	Details
4	DeleteOriginalSourceFile	DELETE	Details

Utilice pasos predefinidos

Al crear un flujo de trabajo, puede optar por añadir uno de los siguientes pasos predefinidos que se describen en este tema. También puede optar por agregar sus propios pasos de procesamiento de archivos personalizados. Para obtener más información, consulte [the section called “Uso de pasos de procesamiento de archivos personalizados”](#).

Temas

- [Copiar archivo](#)
- [Descifrar el archivo](#)
- [Etiquetado de archivos](#)
- [Eliminar archivo](#)
- [Variables con nombre para los flujos de trabajo](#)
- [Ejemplo de flujo de trabajo de etiquetado y eliminación](#)

Copiar archivo

El paso de copiar archivo crea una copia del archivo cargado en una nueva ubicación de Amazon S3. Actualmente, solo puede utilizar el paso de copiar archivos con Amazon S3.

En el siguiente paso de copiar archivos, se copian los archivos en la test carpeta de. *amzn-s3-demo-destination-bucket*

Si el paso de copiar el archivo no es el primer paso del flujo de trabajo, puede especificar la ubicación del archivo. Al especificar la ubicación del archivo, puede copiar el archivo que se utilizó en el paso anterior o el archivo original que se cargó. Puede utilizar esta característica para realizar varias copias del archivo original y, al mismo tiempo, mantener intacto el archivo de origen para archivarlos y conservar los registros. Para ver un ejemplo, consulta [Ejemplo de flujo de trabajo de etiquetado y eliminación](#).

Configure copy parameters

Step name

File location

Select the file location to use as an input for this step

☒ Copy the file created from previous step to a new location

Input file is selected from the previous step's output

☐ Copy the original source file to a new location

Originally uploaded file

Destination bucket name

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

☐ Overwrite existing

Proporcione el bucket y los detalles de la clave

Debe proporcionar el nombre del bucket y una clave para el destino del paso de copiar el archivo. La clave puede ser un nombre de ruta o un nombre de archivo. El hecho de que la clave se trate como un nombre de ruta o como un nombre de archivo depende de si termina la clave con la barra inclinada (/).

Si el último carácter es /, el archivo se copia en la carpeta, y su nombre no cambia. Si el último carácter es alfanumérico, se cambiará el nombre del archivo cargado al valor clave. En este caso,

si ya existe un archivo con ese nombre, el comportamiento depende de la configuración del campo **Sobrescribir existente**.

- Si se selecciona **Sobrescribir existente**, el archivo existente se reemplaza por el archivo que se está procesando.
- Si no se selecciona **Sobrescribir existente**, no ocurre nada, y el procesamiento del flujo de trabajo se detiene.

Tip

Si se ejecutan escrituras simultáneas en la misma ruta de archivo, es posible que se produzca un comportamiento inesperado al sobrescribir los archivos.

Por ejemplo, si el valor de la clave es `test/`, los archivos cargados se copian en la carpeta `test`. Si el valor de la clave es `test/today` (y la opción **Sobrescribir existente** está seleccionada), todos los archivos que cargue se copiarán en un archivo llamado `today` en la carpeta `test` y cada archivo posterior sobrescribirá al anterior.

Note

Amazon S3 admite buckets y objetos y no existe jerarquía. Sin embargo, puede usar prefijos y delimitadores en los nombres de las claves de los objetos para establecer una jerarquía y organizar sus datos de forma similar a las carpetas.

Utilizar una variable con nombre en el paso de copiar un archivo

En el paso de copiar un archivo, puede utilizar una variable para copiar, dinámicamente, los archivos en carpetas específicas del usuario. Actualmente, puede usar `${transfer:UserName}` o `${transfer:UploadDate}` como una variable para copiar archivos a una ubicación de destino para el usuario en concreto que carga los archivos o según la fecha actual.

En el siguiente ejemplo, si el usuario `richard-roe` carga un archivo, se copia en la carpeta `amzn-s3-demo-destination-bucket/richard-roe/processed/`. En el siguiente ejemplo, si el usuario `mary-major` carga un archivo, queda copiado en la carpeta `amzn-s3-demo-destination-bucket/mary-major/processed/`.

Configure parameters

Configure copy parameters

Step name

dynamic-copy

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UserName}/processed`

☐ Overwrite existing

Del mismo modo, se puede utilizar `${transfer:UploadDate}` como variable para copiar los archivos a una ubicación de destino con el nombre de la fecha actual. En el siguiente ejemplo, si establece el destino `${transfer:UploadDate}/processed` en el 1 de febrero de 2022, los archivos cargados se copiarán en la carpeta `amzn-s3-demo-destination-bucket/2022-02-01/processed/`.

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UploadDate}/processed`

☐ Overwrite existing

También puede utilizar estas dos variables juntas al combinar sus funciones. Por ejemplo, puede establecer el prefijo de la clave de destino en **folder/\${transfer:UserName}/\${transfer:UploadDate}/**, lo que crearía carpetas anidadas, por ejemplo. `folder/marymajor/2023-01-05/`

Permisos de IAM para el paso de copiado

Para permitir que un paso de copiado se realice correctamente, asegúrese de que el rol de ejecución de su flujo de trabajo contenga los siguientes permisos.

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
```

```
"Effect": "Allow",
"Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
],
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

Note

El permiso `s3:ListBucket` solo es necesario si no selecciona Sobrescribir existente. Este permiso comprueba el bucket para verificar si ya existe un archivo con el mismo nombre. Si ha seleccionado Sobrescribir existente, el flujo de trabajo no necesita comprobar el archivo y puede escribirlo sin más.

Si sus archivos de Amazon S3 tienen etiquetas, debe añadir uno o dos permisos a su política de IAM.

- Añada `s3:GetObjectTagging` para un archivo de Amazon S3 que no tenga versiones.
- Añada `s3:GetObjectVersionTagging` para un archivo de Amazon S3 que tenga versiones.

Descifrar el archivo

El blog sobre AWS almacenamiento tiene una entrada que describe cómo descifrar archivos de forma sencilla sin escribir ningún código mediante los flujos de trabajo gestionados por Transfer Family, [cifrar y descifrar archivos con PGP](#) y. AWS Transfer Family

Algoritmos de cifrado simétrico compatibles

Para el descifrado PGP, Transfer Family admite algoritmos de cifrado simétrico que se utilizan para cifrar los datos reales de los archivos dentro de los archivos PGP.

- Para obtener información detallada sobre los algoritmos de cifrado simétrico compatibles, consulte. [Algoritmos de cifrado simétrico PGP](#)

- Para obtener información sobre los algoritmos de key pair de PGP que se utilizan con estos algoritmos simétricos, consulte [Algoritmos de key pair PGP](#)

Utilizar el descifrado PGP en su flujo de trabajo

Transfer Family cuenta con compatibilidad integrada para el descifrado Pretty Good Privacy (PGP). Puede utilizar el descifrado PGP en los archivos que se carguen mediante SFTP, FTPS o FTP a Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS).

Para utilizar el descifrado PGP, debe crear y almacenar las claves privadas de PGP que se utilizarán para descifrar sus archivos. Por ello, los usuarios pueden cifrar los archivos mediante las claves de cifrado PGP correspondientes antes de cargarlos en el servidor de Transfer Family. Después de recibir los archivos cifrados, puede descifrarlos en su flujo de trabajo. Para ver un tutorial detallado, consulte [Configuración de un flujo de trabajo gestionado para descifrar un archivo](#).

Para obtener información sobre los algoritmos y recomendaciones de PGP compatibles, consulte [Algoritmos de cifrado y descifrado PGP](#)

Uso del descifrado PGP en su flujo de trabajo

1. Identifique un servidor de Transfer Family para alojar su flujo de trabajo o cree uno nuevo. Debe tener el ID del servidor antes de poder almacenar sus claves PGP en AWS Secrets Manager con el nombre secreto correcto.
2. Guarde su clave PGP AWS Secrets Manager con el nombre secreto requerido. Para obtener más información, consulte [Administración de claves PGP](#). Los flujos de trabajo pueden localizar, automáticamente, la clave PGP correcta que se utilizará para el descifrado en función del nombre secreto en Secrets Manager.

Note

Cuando guardas secretos en Secrets Manager, Cuenta de AWS incurres en cargos. Para obtener más información acerca de los precios, consulte [AWS Secrets Manager Precios](#).

3. Cifre un archivo con su par de claves PGP. (Si desea obtener una lista de los clientes compatibles, consulte [Clientes PGP admitidos](#).) Si está utilizando la línea de comando, utilice el siguiente comando. Para usar este comando, reemplace *username@example.com* por

la dirección de correo electrónico que usó para crear el par de claves PGP. Reemplace *testfile.txt* por el nombre del archivo que desea cifrar.

```
gpg -e -r username@example.com testfile.txt
```

Important

Al cifrar archivos para usarlos con AWS Transfer Family flujos de trabajo, asegúrese siempre de especificar un destinatario no anónimo mediante el parámetro. `-r` El cifrado anónimo (sin especificar un destinatario) puede provocar errores de descifrado en el flujo de trabajo, ya que el sistema no podrá identificar qué clave utilizar para el descifrado. La información sobre la depuración de este problema está disponible en. [Solucione problemas de cifrado de destinatarios anónimos](#)

4. Suba el archivo cifrado a su servidor de Transfer Family.
5. Configure un paso de descifrado en su flujo de trabajo. Para obtener más información, consulte [Añada un paso de descifrado](#).

Añada un paso de descifrado

Un paso de descifrado descifra un archivo cifrado que se cargó en Amazon S3 o Amazon EFS como parte de su flujo de trabajo. Para obtener información detallada sobre la configuración del cifrado, consulte [Utilizar el descifrado PGP en su flujo de trabajo](#).

Al crear el paso de descifrado para un flujo de trabajo, debe especificar el destino de los archivos descifrados. También debe seleccionar si desea sobrescribir los archivos existentes si ya existe un archivo en la ubicación de destino. Puede supervisar los resultados del flujo de trabajo de descifrado y obtener los registros de auditoría de cada archivo en tiempo real mediante Amazon CloudWatch Logs.

Tras elegir el tipo de archivo de descifrado para el paso, aparecerá la página de configuración de parámetros. Complete los valores de la sección Configuración de parámetros de descifrado de PGP.

Las opciones disponibles son las siguientes:

- Nombre del paso: escriba un nombre descriptivo para el paso.
- Ubicación del archivo: al especificar la ubicación del archivo, puede cifrar el archivo utilizado en el paso anterior o el archivo original que se cargó.

 Note

Este parámetro no está disponible si este paso es el primero del flujo de trabajo.

- Destino de los archivos descifrados: elija un bucket de Amazon S3 o un sistema de archivos Amazon EFS como destino del archivo descifrado.
- Si elige Amazon S3, debe proporcionar un nombre de bucket de destino y un prefijo de clave. Para establecer los parámetros del prefijo de la clave de destino por nombre de usuario, introduzca **`${transfer:UserName}`** como el prefijo de la clave de destino. De igual manera, para establecer los parámetros del prefijo de la clave de destino por fecha de carga, introduzca **`${Transfer:UploadDate}`** para el prefijo de la clave de destino.
- Si elige Amazon EFS, debe proporcionar una ruta y un sistema de archivos de destino.

 Note

La opción de almacenamiento que elija aquí debe coincidir con el sistema de almacenamiento que utilice el servidor de Transfer Family al que está asociado este flujo de trabajo. De lo contrario, se producirá un error al intentar ejecutar este flujo de trabajo.

- Sobrescribir existente: si carga un archivo y ya existe un archivo con el mismo nombre de archivo en el destino, el comportamiento depende de la configuración de este parámetro:
 - Si se selecciona Sobrescribir existente, el archivo existente se reemplaza por el archivo que se está procesando.
 - Si no se selecciona Sobrescribir existente, no ocurre nada, y el procesamiento del flujo de trabajo se detiene.

 Tip

Si se ejecutan escrituras simultáneas en la misma ruta de archivo, es posible que se produzca un comportamiento inesperado al sobrescribir los archivos.

La siguiente captura de pantalla muestra un ejemplo de las opciones que puede elegir para el paso de descifrado del archivo.

Step 1

[Choose step type](#)

Step 2

Configure parameters

Step 3

Review and create

Configure parameters

Configure PGP decryption parameters

Store your PGP private key(s) and passphrase(s) in AWS Secrets Manager. [Learn more](#)

 Refer to the [AWS Transfer Family pricing page](#) for pricing details. 

Step name

File location

Select the file location to use as an input for this step

- ☒ **Apply on the file created from the previous step**
Input file is selected from the previous step's output
- ☐ **Apply on the original file**
Originally uploaded file

Destination for decrypted files

Choose an S3 bucket or an EFS file system for storing decrypted files.

☒ **Amazon S3**
Store your decrypted files as Amazon S3 objects

☐ **Amazon EFS**
Store your decrypted files in an EFS file system

Destination bucket name

Destination key prefix

If you are decrypting files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize the destination prefix by username or upload date respectively.

- ☐ **Overwrite existing**
Overwrite if a file with the same file name already exists at the destination.

Permisos de IAM para el paso de cifrado

Para permitir que un paso de descifrado se realice correctamente, asegúrese de que el rol de ejecución de su flujo de trabajo contenga los siguientes permisos.

```
{
  "Sid": "ListBucket",
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}, {
  "Sid": "Decrypt",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue",
  ],
  "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
}
```

Note

El permiso `s3:ListBucket` solo es necesario si no selecciona Sobrescribir existente. Este permiso comprueba el bucket para verificar si ya existe un archivo con el mismo nombre. Si ha seleccionado Sobrescribir existente, el flujo de trabajo no necesita comprobar el archivo y puede escribirlo sin más.

Si sus archivos de Amazon S3 tienen etiquetas, debe añadir uno o dos permisos a su política de IAM.

- Añada `s3:GetObjectTagging` para un archivo de Amazon S3 que no tenga versiones.

- Añada `s3:GetObjectVersionTagging` para un archivo de Amazon S3 que tenga versiones.

Etiquetado de archivos

Para etiquetar los archivos entrantes para su posterior procesamiento, utilice un paso de etiquetado. Introduzca el valor de la etiqueta que desea asignar a los archivos entrantes. Actualmente, la operación de etiquetado solo se admite si utiliza Amazon S3 para el almacenamiento de su servidor de Transfer Family.

El siguiente ejemplo de paso de etiquetado asigna `scan_outcome` y `clean` como la clave y el valor de la etiqueta respectivamente.

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

Para permitir que un paso de etiquetado se realice correctamente, asegúrese de que el rol de ejecución de su flujo de trabajo contenga los siguientes permisos.

```
{  
    "Sid": "Tag",  
    "Effect": "Allow",
```

```

    "Action": [
      "s3:PutObjectTagging",
      "s3:PutObjectVersionTagging"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  }

```

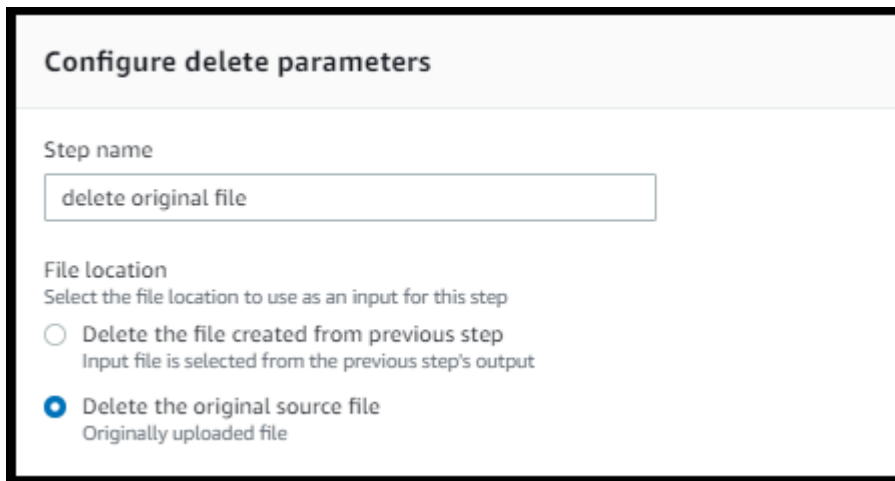
Note

Si su flujo de trabajo contiene un paso de etiquetado que se ejecuta antes de un paso de copiado o descifrado, debe añadir uno o dos permisos a su política de IAM.

- Añada `s3:GetObjectTagging` para un archivo de Amazon S3 que no tenga versiones.
- Añada `s3:GetObjectVersionTagging` para un archivo de Amazon S3 que tenga versiones.

Eliminar archivo

Para eliminar un archivo procesado de un paso anterior del flujo de trabajo o para eliminar el archivo cargado originalmente, utilice un paso de eliminación de archivo.



Configure delete parameters

Step name

File location
 Select the file location to use as an input for this step

☐ Delete the file created from previous step
 Input file is selected from the previous step's output

☒ Delete the original source file
 Originally uploaded file

Para permitir que un paso de eliminación se realice correctamente, asegúrese de que el rol de ejecución de su flujo de trabajo contenga los siguientes permisos.

```

{
  "Sid": "Delete",

```

```
"Effect": "Allow",
"Action": [
    "s3:DeleteObjectVersion",
    "s3:DeleteObject"
],
"Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
* "
}
```

Variables con nombre para los flujos de trabajo

Para los pasos de copiado y descifrado, puede utilizar una variable para realizar acciones de forma dinámica. Actualmente, AWS Transfer Family admite las siguientes variables con nombre.

- Se utiliza `${transfer:UserName}` para copiar o descifrar archivos a un destino en función del usuario que los carga.
- Se utiliza `${transfer:UploadDate}` para copiar o descifrar archivos a una ubicación de destino en función de la fecha actual.

Ejemplo de flujo de trabajo de etiquetado y eliminación

El siguiente ejemplo ilustra un flujo de trabajo que etiqueta los archivos entrantes que deben ser procesados por una aplicación secundaria, como una plataforma de análisis de datos. Tras etiquetar el archivo entrante, el flujo de trabajo elimina el archivo cargado originalmente para ahorrar costos de almacenamiento.

Console

Ejemplo de etiquetado y flujos de trabajo

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Flujos de trabajo.
3. En la página Flujos de trabajo, seleccione Crear flujo de trabajo.
4. En la página Crear flujo de trabajo, escriba una descripción. Esta descripción aparece en la página Flujos de trabajo.
5. Añada el primer paso (copiado).
 - a. En la sección Pasos nominales, seleccione Añadir paso.

- b. Seleccione Copiar archivo, y después Siguiente.
- c. Introduzca un nombre de paso y, a continuación, seleccione un bucket de destino y un prefijo de clave.

Step 1
Choose step type

Step 2
Configure parameters

Step 3
Review and create

Configure parameters

Configure copy parameters

Step name
copy-step-first-step

Destination bucket name
example-bucket ▼

Destination key prefix
If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.
test/

☐ Overwrite existing

- d. Seleccione Siguiente y, a continuación, revise los detalles del paso.
 - e. Seleccione Crear paso para añadir el paso y continuar.
6. Añada el segundo paso (etiquetado).
- a. En la sección Pasos nominales, seleccione Añadir paso.
 - b. Seleccione Etiqueta archivo, y después Siguiente.
 - c. Introduzca un nombre de paso.
 - d. En Ubicación del archivo, seleccione Etiquetar el archivo creado en el paso anterior.
 - e. Introduzca una clave y un valor.

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

- f. Seleccione Siguiente y, a continuación, revise los detalles del paso.
 - g. Seleccione Crear paso para añadir el paso y continuar.
7. Añada el tercer paso (eliminación).
- a. En la sección Pasos nominales, seleccione Añadir paso.
 - b. Seleccione Eliminar pilas y, a continuación, Siguiente.

Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

- c. Introduzca un nombre de paso.

- d. En Ubicación del archivo, seleccione Eliminar el archivo fuente original.
 - e. Seleccione Siguiente y, a continuación, revise los detalles del paso.
 - f. Seleccione Crear paso para añadir el paso y continuar.
8. Revise la configuración del flujo de trabajo y, a continuación, seleccione Crear flujo de trabajo.

CLI

Ejemplo de etiquetado y flujos de trabajo

1. Guarde el siguiente código en un archivo, por ejemplo, `tagAndMoveWorkflow.json`. Reemplace cada *user input placeholder* por su propia información.

```
[
  {
    "Type": "COPY",
    "CopyStepDetails": {
      "Name": "CopyStep",
      "DestinationFileLocation": {
        "S3FileLocation": {
          "Bucket": "amzn-s3-demo-bucket",
          "Key": "test/"
        }
      }
    }
  },
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "demo"
        }
      ],
      "SourceFileLocation": "${previous.file}"
    }
  },
  {
    "Type": "DELETE",
```



```
"DeleteStepDetails":{
  "Name":"DeleteStep",
  "SourceFileLocation": "${original.file}"
}
]
```

El primer paso copia el archivo cargado en una nueva ubicación de Amazon S3. El segundo paso agrega una etiqueta (par clave-valor) al archivo (`previous.file`) que se copió en la nueva ubicación. Y, por último, el tercer paso elimina el archivo original (`original.file`).

2. Cree un flujo de trabajo a partir del archivo guardado. Reemplace cada *user input placeholder* por su propia información.

```
aws transfer create-workflow --description "short-description" --steps
file://path-to-file --region region-ID
```

Por ejemplo:

```
aws transfer create-workflow --description "copy-tag-delete workflow" --steps
file://tagAndMoveWorkflow.json --region us-east-1
```

 Note

Para obtener más información sobre el uso de archivos para cargar parámetros, consulte [Cómo cargar parámetros desde un archivo](#).

3. Actualización de un servidor existente.

 Note

En este paso, se supone que ya tiene un servidor de Transfer Family y que desea asociarle un flujo de trabajo. Si no es así, consulte [Configuración de un punto final de servidor SFTP, FTPS o FTP](#). Reemplace cada *user input placeholder* por su propia información.

```
aws transfer update-server --server-id server-ID --region region-ID
```

```
--workflow-details '{"OnUpload":[{"WorkflowId": "workflow-ID", "ExecutionRole": "execution-role-ARN"}]}'
```

Por ejemplo:

```
aws transfer update-server --server-id s-1234567890abcdef0 --region us-east-2  
--workflow-details '{"OnUpload":[{"WorkflowId": "w-  
abcdef01234567890", "ExecutionRole": "arn:aws:iam::111111111111:role/nikki-wolf-  
execution-role"}]}'
```

Uso de pasos de procesamiento de archivos personalizados

Al utilizar un paso de procesamiento de archivos personalizado, puede utilizar su propia lógica de procesamiento de archivos con AWS Lambda. Al recibir los archivos, un servidor de Transfer Family invoca una función de Lambda que contiene una lógica de procesamiento de archivos personalizada, como el cifrado de archivos, la detección de malware o la comprobación de tipos de archivos incorrectos. En el siguiente ejemplo, el rol de AWS Lambda de destino se utiliza para procesar el archivo de salida del paso anterior.

Configure custom parameters

Step name
custom file processing step

File location
Select the file location to use as an input for this step

☒ Apply custom processing to the file created from previous step
Input file is selected from the previous step's output

☐ Apply custom processing to the original source file
Originally uploaded file

Target
am:aws:lambda:us-east-2:1234567... ▼

Timeout (seconds)
60

Note

Para ver una función de Lambda de ejemplo, consulte [Ejemplo de función de Lambda para un paso de flujo de trabajo personalizado](#). Para ver eventos de ejemplo (incluida la ubicación de los archivos que se pasan a Lambda), consulte [Ejemplos de eventos enviados AWS Lambda al subir el archivo](#).

Con un paso de flujo de trabajo personalizado, debe configurar la función Lambda para llamar a la operación de la [SendWorkflowStepState](#) API. `SendWorkflowStepState` notifica a la ejecución del flujo de trabajo que el paso se ha completado correctamente o con un estado de error. El estado de la operación de la API `SendWorkflowStepState` invoca un paso del controlador de excepciones o un paso nominal en la secuencia lineal en función del resultado de la función de Lambda.

Si se produce un error en la función Lambda o se agota el tiempo de espera, se produce un error en el paso y se muestra `StepErrored` en los registros. CloudWatch Si la función de Lambda forma parte del paso nominal y la función responde a `SendWorkflowStepState` con `Status="FAILURE"` o se agota el tiempo de espera, el flujo continúa con los pasos del controlador de excepciones. En este caso, el flujo de trabajo no continúa ejecutando los pasos nominales restantes (si los hay). Para obtener más información, consulte [Gestión de excepciones para un flujo de trabajo](#).

Al llamar a la operación de la API `SendWorkflowStepState`, debe enviar los siguientes parámetros:

```
{
  "ExecutionId": "string",
  "Status": "string",
  "Token": "string",
  "WorkflowId": "string"
}
```

Puede extraer `ExecutionId`, `Token` y `WorkflowId` del evento de entrada que se pasa cuando se ejecuta la función de Lambda (en las siguientes secciones se muestran ejemplos). El valor `Status` puede ser `SUCCESS` o `FAILURE`.

Para poder llamar a la operación de `SendWorkflowStepState` API desde su función Lambda, debe usar una versión del AWS SDK que se publicó después de la introducción de [Managed Workflows](#).

Uso de varias funciones de Lambda de forma consecutiva

Cuando se utilizan varios pasos personalizados uno tras otro, la opción de ubicación del archivo funciona de forma diferente que si se utiliza un solo paso personalizado. Transfer Family no permite volver a pasar el Lambda-processed archivo para usarlo como entrada del siguiente paso. Por lo tanto, si tiene varios pasos personalizados configurados para usar la opción `previous.file`, todos usarán la misma ubicación de archivo (la ubicación del archivo de entrada para el primer paso personalizado).

Note

La configuración `previous.file` también funciona de forma diferente si tiene un paso predefinido (etiquetado, copiado, descifrado o eliminación) después de un paso personalizado. Si el paso predefinido está configurado para usar la configuración `previous.file`, el paso predefinido usará el mismo archivo de entrada que el paso personalizado. El archivo procesado del paso personalizado no se pasa al paso predefinido.

Acceso a un archivo después de un procesamiento personalizado

Si utiliza Amazon S3 como almacenamiento y su flujo de trabajo incluye un paso personalizado que realiza acciones en el archivo cargado originalmente, los pasos siguientes no podrán acceder al archivo procesado. Es decir, ningún paso posterior al paso personalizado puede hacer referencia al archivo actualizado desde la salida del paso personalizado.

Suponga, por ejemplo, que tiene los tres pasos siguientes en su flujo de trabajo.

- Paso 1: cargue un archivo con el nombre `example-file.txt`.
- Paso 2: invoque una función de Lambda que cambie `example-file.txt` de alguna manera.
- Paso 3: intente realizar un procesamiento adicional en la versión actualizada de `example-file.txt`.

Si configura el `sourceFileLocation` para que el paso 3 sea `${original.file}`, el paso 3 utilizará la ubicación original del archivo desde el momento en que el servidor cargó el archivo para almacenarlo en el paso 1. Si utiliza `${previous.file}` para el paso 3, el paso 3 reutilizará la ubicación del archivo que el paso 2 utilizó como entrada.

Por lo tanto, el paso 3 produce un error. Por ejemplo, si el paso 3 intenta copiar el `example-file.txt` actualizado, obtendrá el siguiente error:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "NOT_FOUND",
    "errorMessage": "ETag constraint not met (Service: null; Status Code: 412; Error Code: null; Request ID: null; S3 Extended Request ID: null; Proxy: null)",
    "stepType": "COPY",
    "stepName": "CopyFile"
  },
}
```

Este error se produce porque el paso personalizado modifica toda la etiqueta de entidad (ETag) para `example-file.txt` de forma que no coincide con el archivo original.

Note

Este comportamiento no se produce si utiliza Amazon EFS porque Amazon EFS no utiliza etiquetas de entidad para identificar los archivos.

Ejemplos de eventos enviados AWS Lambda al subir el archivo

Los siguientes ejemplos muestran los eventos que se envían AWS Lambda cuando se completa la carga de un archivo. Un ejemplo utiliza un servidor de Transfer Family en el que el dominio está configurado con Amazon S3. El otro ejemplo utiliza un servidor de Transfer Family donde el dominio usa Amazon EFS.

Custom step that uses an Amazon S3 domain

```
{
  "token": "MzI0Nzc4ZDktMGRmMi00MjFhLTgxMjUtYWZmZmRmODNkYjc0",
  "serviceMetadata": {
    "executionDetails": {
      "workflowId": "w-1234567890example",
      "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
    },
    "transferDetails": {
      "sessionId": "36688ff5d2deda8c",
    }
  }
}
```

```

        "userName": "myuser",
        "serverId": "s-example1234567890"
    },
    "fileLocation": {
        "domain": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "path/to/mykey",
        "eTag": "d8e8fca2dc0f896fd7cb4cb0031ba249",
        "versionId": null
    }
}

```

Custom step that uses an Amazon EFS domain

```

{
  "token": "MTg0N2Y3N2UtNWl5Ny00ZmZlLTk5YTgtZTU3YzViYjllNmZm",
  "serviceMetadata": {
    "executionDetails": {
      "workflowId": "w-1234567890example",
      "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
    },
    "transferDetails": {
      "sessionId": "36688ff5d2deda8c",
      "userName": "myuser",
      "serverId": "s-example1234567890"
    }
  },
  "fileLocation": {
    "domain": "EFS",
    "fileSystemId": "fs-1234567",
    "path": "/path/to/myfile"
  }
}

```

Ejemplo de función de Lambda para un paso de flujo de trabajo personalizado

La siguiente función de Lambda extrae la información relativa al estado de la ejecución y, a continuación, llama a la operación de la [SendWorkflowStepState](#) API para devolver el estado al flujo de trabajo del paso SUCCESS, o bien. FAILURE Antes de que su función llame a la operación de la

API `SendWorkflowStepState`, puede configurar Lambda para que realice una acción en función de la lógica del flujo de trabajo.

```
import json
import boto3

transfer = boto3.client('transfer')

def lambda_handler(event, context):
    print(json.dumps(event))

    # call the SendWorkflowStepState API to notify the workflow about the step's
    # SUCCESS or FAILURE status
    response = transfer.send_workflow_step_state(
        WorkflowId=event['serviceMetadata']['executionDetails']['workflowId'],
        ExecutionId=event['serviceMetadata']['executionDetails']['executionId'],
        Token=event['token'],
        Status='SUCCESS|FAILURE'
    )

    print(json.dumps(response))

    return {
        'statusCode': 200,
        'body': json.dumps(response)
    }
```

Permisos de IAM para un paso personalizado

Para permitir que un paso que llame a una Lambda se realice correctamente, asegúrese de que el rol de ejecución de su flujo de trabajo contenga los siguientes permisos.

```
{
  "Sid": "Custom",
  "Effect": "Allow",
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": [
    "arn:aws:lambda:region:account-id:function:function-name"
  ]
}
```

Políticas de IAM para flujos de trabajo

Al añadir un flujo de trabajo a un servidor, debe seleccionar un rol de ejecución. El servidor utiliza este rol cuando ejecuta el flujo de trabajo. Si el rol no tiene los permisos adecuados, AWS Transfer Family no podrá ejecutar el flujo de trabajo.

En esta sección se describe un posible conjunto de permisos AWS Identity and Access Management (IAM) que puede utilizar para ejecutar un flujo de trabajo. Más adelante en este tema se describen otros ejemplos.

Note

Si sus archivos de Amazon S3 tienen etiquetas, debe añadir uno o dos permisos a su política de IAM.

- Añada `s3:GetObjectTagging` para un archivo de Amazon S3 que no tenga versiones.
- Añada `s3:GetObjectVersionTagging` para un archivo de Amazon S3 que tenga versiones.

Creación de un rol de ejecución para su flujo de trabajo

1. Cree una nueva función de IAM y añada la política AWS gestionada `AWSTransferFullAccess` a la función. Para obtener más información sobre cómo crear un nuevo rol de IAM, consulte [the section called “Creación de una política y un rol de IAM”](#).
2. Crear otra política con los siguientes permisos y asíciela al rol. Reemplace cada *user input placeholder* por su propia información.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConsoleAccess",
      "Effect": "Allow",
      "Action": "s3:GetBucketLocation",
      "Resource": "*"
    },
    {
      "Sid": "ListObjectsInBucket",
```



```

        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ]
    },
    {
        "Sid": "AllObjectActions",
        "Effect": "Allow",
        "Action": "s3:*Object",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    },
    {
        "Sid": "GetObjectVersion",
        "Effect": "Allow",
        "Action": "s3:GetObjectVersion",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    },
    {
        "Sid": "Custom",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": [
            "arn:aws:lambda:us-east-1:123456789012:function:function-name"
        ]
    },
    {
        "Sid": "Tag",
        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",
            "s3:PutObjectVersionTagging"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    }
]

```

}

3. Guarde este rol y especifíquelo como rol de ejecución cuando añada un flujo de trabajo a un servidor.

Note

Al crear funciones de IAM, le AWS recomienda que restrinja el acceso a sus recursos tanto como sea posible para su flujo de trabajo.

Relaciones de confianza del flujo de trabajo

Los roles de ejecución del flujo de trabajo también requieren una relación de confianza con `transfer.amazonaws.com`. Para establecer una relación de confianza para AWS Transfer Family, consulte [Para establecer una relación de confianza](#).

Mientras establece su relación de confianza, también puede tomar medidas para evitar el problema del suplente confuso. Para obtener una descripción de este problema, así como ejemplos de cómo evitarlo, consulte [the section called "Cross-service prevención policial confusa"](#).

Ejemplo de rol de ejecución: descifrado, copiado y etiquetado

Si tiene flujos de trabajo que incluyen pasos de etiquetado, copiado y descifrado, puede utilizar la siguiente política de IAM. Reemplace cada *user input placeholder* por su propia información.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyRead",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    },
    {
```

```

        "Sid": "CopyWrite",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:PutObjectTagging"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
        "Sid": "CopyList",
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-source-bucket",
            "arn:aws:s3:::amzn-s3-demo-destination-bucket"
        ]
    },
    {
        "Sid": "Tag",
        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",
            "s3:PutObjectVersionTagging"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "Condition": {
            "StringEquals": {
                "s3:RequestObjectTag/Archive": "yes"
            }
        }
    },
    {
        "Sid": "ListBucket",
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-destination-bucket"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",

```

```

        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
},
{
    "Sid": "Decrypt",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/transfer/*"
}
]
}

```

Ejemplo de rol de ejecución: ejecutar un rol y eliminarlo

En este ejemplo, tiene un flujo de trabajo que invoca una AWS Lambda función. Si el flujo de trabajo elimina el archivo cargado y tiene un paso de controlador de excepciones para actuar en caso de que se produzca un error en la ejecución del flujo de trabajo en el paso anterior, utilice la siguiente política de IAM. Reemplace cada *user input placeholder* por su propia información.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Delete",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        },
        {
            "Sid": "Custom",
            "Effect": "Allow",

```

```
    "Action": [
      "lambda:InvokeFunction"
    ],
    "Resource": [
      "arn:aws:lambda:us-east-1:123456789012:function:function-name"
    ]
  }
}
```

Gestión de excepciones para un flujo de trabajo

Si se produce algún error durante la ejecución de un flujo de trabajo, se ejecutan los pasos de gestión de excepciones que especificó. Los pasos de gestión de errores de un flujo de trabajo se especifican del mismo modo en que se especifican los pasos nominales del flujo de trabajo. Por ejemplo, supongamos que ha configurado el procesamiento personalizado en pasos nominales para validar los archivos entrantes. Si se produce un error en la validación del archivo, un paso de gestión de excepciones puede enviar un correo electrónico al administrador.

El siguiente ejemplo de flujo de trabajo contiene dos pasos:

- Un paso nominal que comprueba si el archivo cargado está en formato CSV
- Un paso de gestión de excepciones que envía un correo electrónico en caso de que el archivo cargado no esté en formato CSV y el paso nominal falle

Para iniciar el paso de gestión de excepciones, la AWS Lambda función del paso nominal debe responder con. `Status="FAILURE"` Para obtener más información sobre el control de errores, consulte [the section called “Uso de pasos de procesamiento de archivos personalizados”](#).

w-1234567890abcdef0

Delete

Description

Name

Delete after upload

Workflow description

test-my-workflow

Nominal steps (1) Info

Number	Description	Type	Configuration
1	is-CSV	CUSTOM	Details

Exception handlers (1) Info

Number	Description	Type	Configuration
1	send-email	CUSTOM	Details

Monitoreo de la ejecución del flujo

Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones que ejecutas Nube de AWS en tiempo real. Puedes usar Amazon CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puedes medir para tus flujos de trabajo. Puedes ver las métricas del flujo de trabajo y los registros consolidados a través de Amazon CloudWatch.

CloudWatch iniciar sesión en un flujo de trabajo

CloudWatch proporciona una auditoría y un registro consolidados del progreso y los resultados del flujo de trabajo.

Ver los CloudWatch registros de Amazon para flujos de trabajo

1. Abre la CloudWatch consola de Amazon en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación izquierdo, seleccione Registros y, a continuación, Grupos de registros.
3. En la página de grupos de registros, en la barra de navegación, elige la región correcta para tu AWS Transfer Family servidor.
4. Elija el grupo de registro que corresponda a su servidor.

Por ejemplo, si su ID del servidor es `s-1234567890abcdef0`, su grupo de registros es `/aws/transfer/s-1234567890abcdef0`.

5. En la página de detalles del grupo de registros de su servidor, se muestran los flujos de registro más recientes. Hay dos flujos de registro para el usuario que está explorando:
 - Uno para cada sesión del Protocolo de File Transfer (SFTP) de Secure Shell (SSH).
 - Uno para el flujo de trabajo que se está ejecutando en el servidor. El formato del flujo de registro del flujo de trabajo es `username.workflowID.uniqueStreamSuffix`.

Por ejemplo, si su usuario es `mary-major`, tendrá los flujos de registro siguientes:

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

Note

Los identificadores alfanuméricos de 16 dígitos que se muestran en este ejemplo son ficticios. Los valores que ves en Amazon CloudWatch son diferentes.

La página de Eventos de registro para `mary-major-usa-east.1234567890abcdef0` muestra los detalles de cada sesión de usuario y el flujo de registro `mary.w-abcdef01234567890.021345abcdef6789` contiene los detalles del flujo de trabajo.

El siguiente es un ejemplo de flujo de registro para `mary.w-abcdef01234567890.021345abcdef6789`, basado en un flujo de trabajo (`w-abcdef01234567890`) que contiene un paso de copiado.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  }
}
```

```

    }
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
},
{
  "type": "StepStarted",
  "details": {
    "input": {
      "fileLocation": {
        "backingStore": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  },
  "stepType": "COPY",
  "stepName": "copyToShared"
},
"workflowId": "w-abcdef01234567890",
"executionId": "execution-id",
"transferDetails": {
  "serverId": "s-server-id",
  "username": "mary",
  "sessionId": "session-id"
}
},
{
  "type": "StepCompleted",
  "details": {
    "output": {},
    "stepType": "COPY",
    "stepName": "copyToShared"
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "server-id",

```



```
        "username": "mary",
        "sessionId": "session-id"
    },
    {
        "type": "ExecutionCompleted",
        "details": {},
        "workflowId": "w-abcdef01234567890",
        "executionId": "execution-id",
        "transferDetails": {
            "serverId": "s-server-id",
            "username": "mary",
            "sessionId": "session-id"
        }
    }
}
```

CloudWatch métricas para flujos de trabajo

AWS Transfer Family proporciona varias métricas para los flujos de trabajo. Puede ver las métricas de la cantidad de flujos de trabajo que se iniciaron, se completaron correctamente y se produjeron errores en el minuto anterior. Todas las CloudWatch métricas de Transfer Family se describen en [Uso de CloudWatch métricas para servidores Transfer Family](#).

Creación de un flujo de trabajo a partir de una plantilla

Puede implementar una CloudFormation pila que cree un flujo de trabajo y un servidor a partir de una plantilla. Este procedimiento contiene un ejemplo que puede utilizar para implementar rápidamente un flujo de trabajo.

Para crear una CloudFormation pila que cree un AWS Transfer Family flujo de trabajo y un servidor

1. Abra la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
2. Guarde el siguiente código en un archivo.

YAML

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  SFTPServer:
    Type: 'AWS::Transfer::Server'
    Properties:
```

```

WorkflowDetails:
  OnUpload:
    - ExecutionRole: workflow-execution-role-arn
      WorkflowId: !GetAtt
        - TransferWorkflow
        - WorkflowId
  TransferWorkflow:
    Type: AWS::Transfer::Workflow
  Properties:
    Description: Transfer Family Workflows Blog
    Steps:
      - Type: COPY
        CopyStepDetails:
          Name: copyToUserKey
          DestinationFileLocation:
            S3FileLocation:
              Bucket: archived-records
              Key: ${transfer:UserName}/
            OverwriteExisting: 'TRUE'
      - Type: TAG
        TagStepDetails:
          Name: tagFileForArchive
          Tags:
            - Key: Archive
              Value: yes
      - Type: CUSTOM
        CustomStepDetails:
          Name: transferExtract
          Target: arn:aws:lambda:region:account-id:function:function-name
          TimeoutSeconds: 60
      - Type: DELETE
        DeleteStepDetails:
          Name: DeleteInputFile
          SourceFileLocation: '${original.file}'
    Tags:
      - Key: Name
        Value: TransferFamilyWorkflows

```

JSON

```

{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {

```

```

"SFTPServer": {
  "Type": "AWS::Transfer::Server",
  "Properties": {
    "WorkflowDetails": {
      "OnUpload": [
        {
          "ExecutionRole": "workflow-execution-role-arn",
          "WorkflowId": {
            "Fn::GetAtt": [
              "TransferWorkflow",
              "WorkflowId"
            ]
          }
        ]
      ]
    }
  }
},
"TransferWorkflow": {
  "Type": "AWS::Transfer::Workflow",
  "Properties": {
    "Description": "Transfer Family Workflows Blog",
    "Steps": [
      {
        "Type": "COPY",
        "CopyStepDetails": {
          "Name": "copyToUserKey",
          "DestinationFileLocation": {
            "S3FileLocation": {
              "Bucket": "archived-records",
              "Key": "${transfer:UserName}/"
            }
          },
          "OverwriteExisting": "TRUE"
        }
      },
      {
        "Type": "TAG",
        "TagStepDetails": {
          "Name": "tagFileForArchive",
          "Tags": [
            {
              "Key": "Archive",
              "Value": "yes"
            }
          ]
        }
      }
    ]
  }
}

```

```
    }  
  ]  
},  
{  
  "Type": "CUSTOM",  
  "CustomStepDetails": {  
    "Name": "transferExtract",  
    "Target": "arn:aws:lambda:region:account-id:function:function-name",  
    "TimeoutSeconds": 60  
  }  
},  
{  
  "Type": "DELETE",  
  "DeleteStepDetails": {  
    "Name": "DeleteInputFile",  
    "SourceFileLocation": "${original.file}"  
  }  
}  
],  
"Tags": [  
  {  
    "Key": "Name",  
    "Value": "TransferFamilyWorkflows"  
  }  
]  
}  
}  
}
```

3. Reemplace los elementos siguientes por sus propios valores.
 - Reemplace *workflow-execution-role-arn* por el ARN de un rol de ejecución de flujo de trabajo real. Por ejemplo, `arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`
 - Reemplace `arn:aws:lambda:region:account-id:function:function-name` por el ARN de la función de Lambda. Por ejemplo, `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`.
4. Siga las instrucciones para implementar una CloudFormation pila a partir de una plantilla existente en [Seleccionar una plantilla de pila](#) en la Guía del AWS CloudFormation usuario.

Una vez desplegada la pila, puede ver sus detalles en la pestaña Salidas de la CloudFormation consola. La plantilla crea un nuevo servidor AWS Transfer Family SFTP que utiliza usuarios gestionados por el servicio y un nuevo flujo de trabajo, y asocia el flujo de trabajo al nuevo servidor.

Eliminación de un flujo de trabajo de un servidor de Transfer Family

Si ha asociado un flujo de trabajo a un servidor de Transfer Family y ahora quiere eliminar esa asociación, puede hacerlo mediante la consola o mediante programación.

Console

Eliminación de un flujo de trabajo de un servidor de Transfer Family

1. Abra la consola en AWS Transfer Family . <https://console.aws.amazon.com/transfer/>
2. En el panel de navegación izquierdo, seleccione Servidores.
3. Elija el identificador del servidor en la columna ID del servidor.
4. En la página de detalles del servidor, desplácese hacia abajo hasta la sección Detalles adicionales y, a continuación, seleccione Editar.
5. En la página Editar detalles adicionales, en la sección Flujos de trabajo administrados, borre la información de todos los ajustes:
 - Seleccione el guion (-) en la lista de flujos de trabajo del Flujo de trabajo para cargar archivos completos.
 - De no estar ya autorizado, seleccione el guion (-) de la lista de flujos de trabajo del Flujo de trabajo para cargar archivos parciales.
 - Seleccione el guion (-) de la lista de roles para el Rol de ejecución de flujos de trabajo administrados.

Si no ve el guion, desplácese hacia arriba hasta que lo vea, ya que es el primer valor de cada menú.

El resultado debe ser similar a lo siguiente.

Managed workflows [Info](#)

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

Select a workflow ▼ [Create a new Workflow](#)

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

Select a workflow ▼ [Create a new Workflow](#)

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

- ▼

- Desplácese hacia abajo y seleccione Guardar para guardar sus cambios.

CLI

Utilice la llamada `update-server` (o `UpdateServer` para la API) y proporcione argumentos vacíos para los parámetros `OnUpload` y `OnPartialUpload`.

Desde AWS CLI, ejecute el siguiente comando:

```
aws transfer update-server --server-id your-server-id --workflow-details
'{"OnPartialUpload":[],"OnUpload":[]}'
```

Reemplace *your-server-id* por el ID de su servidor. Por ejemplo, si el ID de su servidor es `s-01234567890abcdef`, el comando es el siguiente:

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
'{"OnPartialUpload":[],"OnUpload":[]}'
```

Restricciones y limitaciones de los flujos de trabajo administrados

Restricciones

Las siguientes restricciones se aplican actualmente a los flujos de trabajo de procesamiento posteriores a la carga para AWS Transfer Family.

- Cross-account y no se admiten AWS Lambda las funciones entre regiones. Sin embargo, puede realizar copias entre cuentas, siempre que sus políticas AWS Identity and Access Management (de IAM) estén configuradas correctamente.
- Para todos los pasos del flujo de trabajo, todos los buckets de Amazon S3 a los que acceda el flujo de trabajo deben estar en la misma región que el flujo de trabajo en sí.
- Para un paso de descifrado, el destino del descifrado debe coincidir con el origen de la región y el almacenamiento de respaldo (por ejemplo, si el archivo que se va a descifrar está almacenado en Amazon S3, el destino especificado también debe estar en Amazon S3).
- Solo se admiten los pasos personalizados asíncronos.
- Los tiempos de espera de los pasos personalizados son aproximados. Es decir, es posible que el tiempo de espera tarde un poco más de lo especificado. Además, el flujo de trabajo depende de la función de Lambda. Por lo tanto, si la función se retrasa durante la ejecución, el flujo de trabajo no es consciente del retraso.
- Si supera el límite de limitación, Transfer Family no añade operaciones de flujo de trabajo a la cola.
- Los flujos de trabajo no se inician para los archivos que tienen un tamaño de 0. Los archivos con un tamaño superior a 0 inician el flujo de trabajo asociado.
- Puede adjuntar un flujo de trabajo de procesamiento de archivos a un servidor Transfer Family que utilice el protocolo AS2; sin embargo, los mensajes AS2 no ejecutan los flujos de trabajo adjuntos al servidor.

Limitaciones

Además, los siguientes límites funcionales se aplican a los flujos de trabajo de Transfer Family:

- El número máximo de flujos de trabajo por región y por cuenta está limitado a 10.
- El tiempo de espera máximo para los pasos personalizados es de 30 minutos.
- El número máximo de pasos en un flujo de trabajo es 8.
- El número máximo de etiquetas por grupo de trabajo es 50.
- El número máximo de ejecuciones simultáneas que contienen un paso de descifrado es de 250 por flujo de trabajo.
- Puede almacenar un máximo de 3 claves privadas PGP, por servidor de Transfer Family y por usuario.
- El tamaño máximo de un archivo de datos es de 10 GB.

- Limitamos la nueva tasa de ejecución mediante un sistema de [buckets de tokens](#) con una capacidad de ampliación de 100 y una tasa de recarga de 1.
- Cada vez que elimine un flujo de trabajo de un servidor y lo reemplace por uno nuevo o actualice la configuración del servidor (lo que afecta al rol de ejecución del flujo de trabajo), debe esperar, aproximadamente, 10 minutos antes de ejecutar el nuevo flujo de trabajo. El servidor de Transfer Family almacena en caché los detalles del flujo de trabajo y tarda 10 minutos en actualizar su caché.

Además, debe cerrar sesión en cualquier sesión de SFTP activa y volver a iniciarla después del período de espera de 10 minutos para ver los cambios.

Administración de servidores

En esta sección, encontrará información sobre cómo ver una lista de sus servidores, cómo ver los detalles de su servidor, cómo editar los detalles de su servidor y cómo cambiar la clave de host de su SFTP-enabled servidor.

Temas

- [Ver una lista de servidores](#)
- [Eliminar un servidor](#)
- [Vea los detalles de los servidores SFTP, FTPS y FTP](#)
- [Vea los detalles del servidor AS2](#)
- [Compatibilidad con IPv6 para servidores Transfer Family](#)
- [Editar detalles del servidor](#)
- [Editar la configuración del proveedor de identidad](#)
- [Administre las claves de host de su SFTP-enabled servidor](#)
- [Monitoreo del uso en la consola](#)

Ver una lista de servidores

En la AWS Transfer Family consola, encontrarás una lista de todos los servidores que se encuentran en la AWS región que hayas elegido.

Para buscar una lista de los servidores que existen en una AWS región

- Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.

Si tiene uno o más servidores en la AWS región actual, la consola se abre para mostrar una lista de sus servidores. Si no aparece la lista de servidores, asegúrese de que está en la región correcta. También puede seleccionar Servers (Servidores) en el panel de navegación.

Para obtener más información acerca de cómo visualizar los detalles de sus servidores, consulte [Vea los detalles de los servidores SFTP, FTPS y FTP](#).

Eliminar un servidor

Este procedimiento explica cómo eliminar un servidor Transfer Family mediante la AWS Transfer Family consola o AWS CLI.

Important

Se le facturará por cada uno de los protocolos habilitados para acceder a su punto de conexión hasta que elimine el servidor.

Warning

Al eliminar un servidor, se eliminan todos sus usuarios. Los datos del bucket al que se accedió mediante el servidor no se eliminan y permanecen accesibles para los usuarios AWS que tienen privilegios en esos buckets de Amazon S3.

Console

Para eliminar un servidor mediante la consola

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Servidores.
3. Seleccione la casilla de verificación correspondiente al servidor que desea eliminar.
4. En Actions (Acciones), seleccione Delete (Eliminar).
5. En la ventana de diálogo de confirmación que aparece, escriba la palabra **delete**, y luego seleccione Eliminar para confirmar que desea eliminar el servidor.

El servidor se elimina de la página Servidores y ya no se le facturará a usted por él.

AWS CLI

Para eliminar un servidor mediante la CLI

1. (Opcional) Ejecute el siguiente comando para ver los detalles del servidor que desea eliminar permanentemente.

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

Este `describe-server` comando devuelve todos los detalles del servidor.

2. Ejecute el siguiente comando para eliminar el servidor.

```
aws transfer delete-server --server-id your-server-id
```

Si se ejecuta correctamente, el comando elimina el servidor y no devuelve ninguna información.

Vea los detalles de los servidores SFTP, FTPS y FTP

Puede encontrar una lista de detalles y propiedades de un servidor individual AWS Transfer Family . Las propiedades del servidor incluyen los protocolos, el proveedor de identidad, el estado, el tipo de punto de conexión, el nombre de host personalizado, el punto de conexión, los usuarios, el rol de registro, la clave de host del servidor y las etiquetas.

Visualización de los detalles del servidor

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación, seleccione Servers (Servidores).
3. Elija el identificador en la columna ID de servidor para ver la página Detalles del servidor, que se muestra a continuación.

Puede cambiar las propiedades del servidor en esta página al seleccionar Editar. Para obtener más información acerca de la edición de los detalles de los servidores, consulte [Editar detalles del servidor](#). La página de detalles de los servidores AS2 es ligeramente diferente. Para los servidores AS2, consulte. [Vea los detalles del servidor AS2](#)

Protocols Protocols over which clients can connect to your server's endpoint • SFTP	Identity provider Identity provider type Service managed

Note

Los valores de Descripción y Fecha de importación de la clave del host del servidor son nuevos a partir de septiembre de 2022. Estos valores se introdujeron para admitir la característica de claves de host múltiples. Esta característica requería la migración de cualquier clave de host única que estuviera en uso antes de la introducción de varias claves de host.

El valor de Fecha de importación de una clave de host de servidor migrada se establece en la fecha de la última modificación del servidor. Es decir, la fecha que aparece en la clave de host migrada corresponde a la fecha en la que modificó el servidor de alguna forma por última vez, antes de la migración de la clave de host del servidor.

La única clave que se migró es la clave de host del servidor más antigua o la única. Todas las claves adicionales tienen su fecha real de cuando las importó. Además, la clave migrada tiene una descripción que permite identificarla fácilmente como si se hubiera migrado.

La migración se produjo entre el 2 y el 13 de septiembre. La fecha de migración real dentro de este intervalo depende de la región del servidor.

Additional details[Edit](#)**Log group**[/aws/transfer/s-](#)**Logging role** [Info](#)

-

Security Policy [Info](#)

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

Domain

Amazon S3

Login display banner[View the display message](#)**Optimized directories** [Info](#)

ENABLED

SetStat option

Ignore

TLS session resumption

-

Passive IP

-

Vea los detalles del servidor AS2

Puede encontrar una lista de detalles y propiedades de un AWS Transfer Family servidor individual. Las propiedades del servidor incluyen los protocolos, el estado y mucho más. En el caso de los servidores AS2, también puedes ver las direcciones IP de salida MDN asíncronas del AS2.

Protocols

Edit

Protocols over which clients can connect to your server's endpoint

- AS2

Identity provider

Edit

 **AS2 Auth**
Basic authentication is not supported for AS2. Access can be controlled through VPC security groups.

A cada servidor AS2 se le asignan tres direcciones IP estáticas. Utilice estas direcciones IP para enviar mDNS asíncronos a sus socios comerciales a través de AS2.

AS2 asynchronous MDN egress IP details

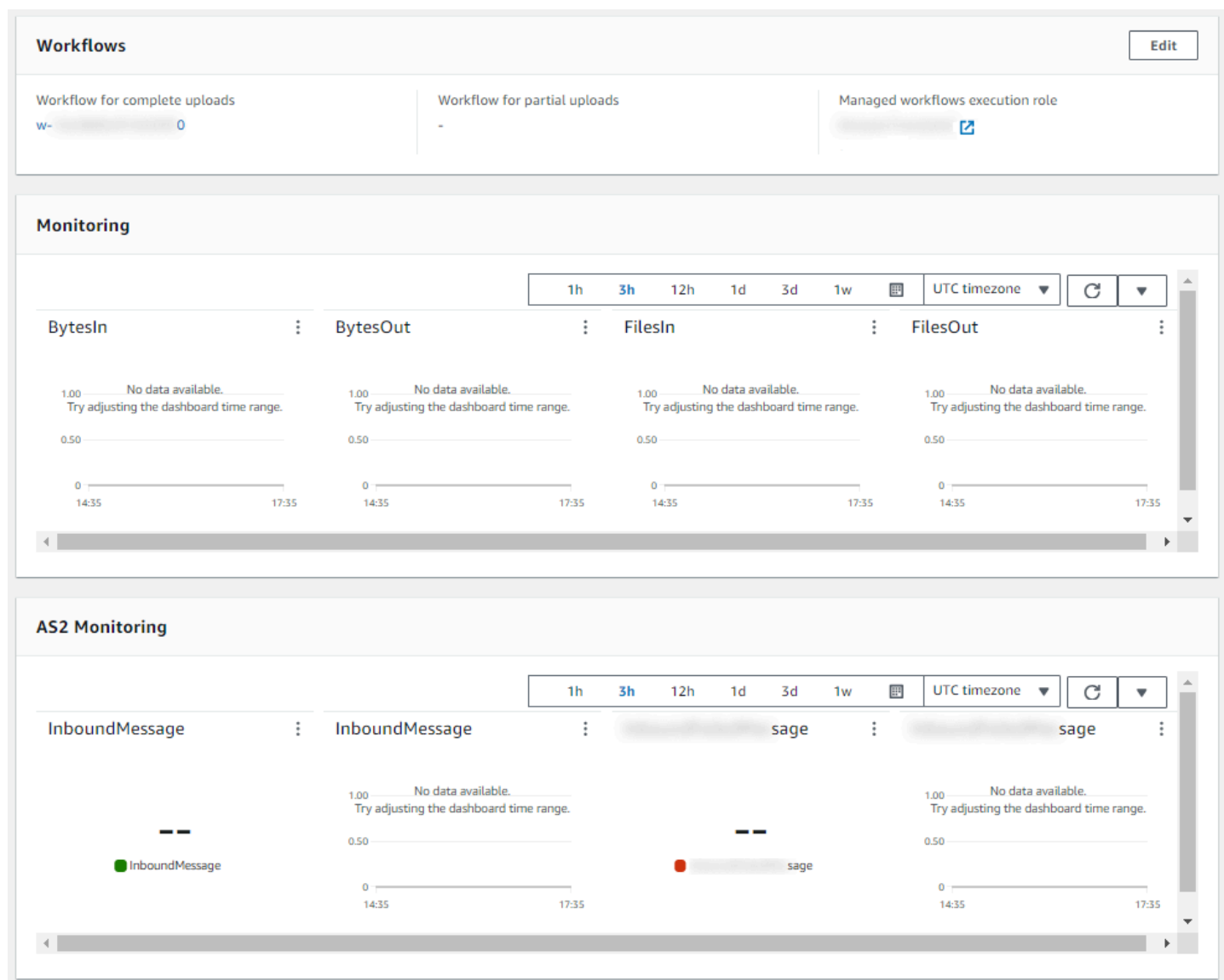
Below are the service managed static IP addresses used for sending your asynchronous MDNs to trading partners over AS2







La parte inferior de la página de detalles del servidor AS2 contiene detalles de cualquier flujo de trabajo adjunto e información de monitoreo y etiquetado.



Compatibilidad con IPv6 para servidores Transfer Family

AWS Transfer Family admite puntos finales de doble pila (IPv4 e IPv6) para los siguientes recursos:

- Terminales públicos de SFTP
- Puntos finales internos de VPC para todos los protocolos (y AS2) SFTP/FTPS/FTP
- Terminales públicos para servidores AS2-enabled Transfer Family, siguiendo los pasos que se indican en [Uso de un Application Load Balancer para la conectividad de servidores AS2 de doble pila](#)
- Puntos de conexión de API

Con el soporte de doble pila, sus puntos de conexión Transfer Family pueden comunicarse con clientes habilitados para IPv4 e IPv6. Esto le permite pasar gradualmente de sistemas basados en IPv4 a sistemas basados en IPv6 sin necesidad de cambiar todos de una vez, cumplir con los requisitos de conformidad con IPv6 y eliminar la necesidad de costosos equipos de red para gestionar la traducción de direcciones entre IPv4 e IPv6. Para obtener más información, consulte [DNS y puntos finales](#) en la referencia de la API. AWS Transfer Family Para obtener una lista completa de los puntos de enlace disponibles, consulte los puntos de [AWS Transfer Family enlace y las cuotas](#) en. Referencia general de AWS

Limitaciones de IPv6

Los siguientes recursos de Transfer Family no son compatibles actualmente con IPv6:

- VPC-Internet puntos finales
- tipo de punto final VPC_ENDPOINT (obsoleto)

El protocolo FTPS admite los comandos PASV y EPSV para solicitar un puerto de datos abierto para las operaciones de listado, obtención y colocación de archivos. Sin embargo, el PASV no funciona con IPv6 porque requiere una respuesta. IPv4-specific El EPSV sigue funcionando porque solo devuelve información sobre los puertos.

Para utilizar el FTPS, recomendamos una de las siguientes opciones:

- Configure su cliente FTPS para que utilice EPSV
- Utilice IPv4 en lugar de IPv6

SFTP admite IPv4 e IPv6. Recomendamos usar SFTP en lugar de FTPS cuando se trabaja con puntos finales de doble pila.

Configuración de IPv6 para servidores

Al crear un nuevo servidor o actualizar uno existente, puede elegir el tipo de dirección IP:

- IPv4 (predeterminado): por motivos de compatibilidad con versiones anteriores, el servidor solo aceptará conexiones IPv4.
- Dual-stack: El servidor aceptará conexiones IPv4 e IPv6.

Para actualizar el tipo de dirección IP de un servidor existente:

1. Detenga el servidor.
2. Edite los detalles del punto final.
3. Cambie el tipo de dirección IP a Dual-stack.
4. Inicie el servidor de .

 Note

En el VPC-Internet caso de los puntos finales, actualmente no se admite el modo de doble pila.

Uso de un Application Load Balancer para la conectividad de servidores AS2 de doble pila

Puede habilitar la conectividad de doble pila (IPv4 e IPv6) con su servidor AS2 mediante un Application Load Balancer que tenga un punto final orientado al público. Esto permite a los socios comerciales conectarse a su servidor AS2 mediante IPv4 o IPv6.

Para configurar un Application Load Balancer de doble pila para su servidor AS2

1. Cree una VPC con la siguiente configuración:
 - VPC solo
 - Entrada CIDR IPv4 manual
 - Amazon-provided Bloque CIDR de IPv6
2. Cree al menos dos subredes en diferentes zonas de disponibilidad:
 - Agregue los CIDR de IPv6 a las subredes
 - Al crear subredes, asigne solo un subconjunto de las direcciones de la VPC para dejar IPv4/IPv6 las direcciones disponibles para subredes adicionales
3. Cree una puerta de enlace a Internet para la VPC.
4. Edite la tabla de rutas y añada dos rutas:
 - Una ruta con destino `0.0.0.0/0`
 - Una ruta con destino `::/0`

- Establezca ambos objetivos de ruta en la puerta de enlace de Internet que creó
5. Cree un AS2-enabled servidor en la VPC que creó en el paso 1. Asegúrese de especificar el `IpAddressType` `asDUALSTACK`.

Para obtener más información sobre cómo crear un servidor Transfer Family que utilice el protocolo AS2, consulte [Crear un servidor AS2](#).

6. Cree un grupo objetivo:
 - En Especificar los detalles del grupo, configure:
 - Tipo de destino: direcciones IP
 - Nombre: introduzca un nombre
 - Protocol: HTTP
 - Puerto: 5080
 - VPC: seleccione la VPC que creó
 - Versión del protocolo: HTTP1
 - Health Checks: utilice los valores predeterminados
 - Para los objetivos de Register:
 - Introduzca la dirección IPv4 privada de su servidor AS2
 - Seleccione Incluir como pendiente a continuación
7. Cree un Application Load Balancer:
 - Introduzca un nombre
 - En Scheme, elija Internet-facing
 - Para el tipo de dirección IP, elija Dualstack
 - Para el mapeo de redes:
 - Seleccione la VPC que creó
 - Seleccione las zonas de disponibilidad en las que creó las subredes
 - Para los grupos de seguridad, seleccione un grupo de seguridad que permita el tráfico IPv4 e IPv6 entrante desde cualquier dirección IP del puerto 80
 - Para los oyentes y el enrutamiento:
 - Protocol: HTTP
 - Port: 80
 - Acción predeterminada: reenviar al grupo objetivo que ha creado

- Selecciona Crear balanceador de cargas

Tras crear el Application Load Balancer, los socios comerciales pueden usar su nombre DNS para enviar tráfico a su servidor AS2. Esta configuración permite que su servidor AS2 acepte conexiones de clientes IPv4 e IPv6 a través del Application Load Balancer de doble pila.

Editar detalles del servidor

Tras crear un AWS Transfer Family servidor, puede editar la configuración del servidor.

Temas

- [Edite los protocolos de transferencia de archivos](#)
- [Editar el punto de conexión del servidor](#)
- [Edite la configuración de registro](#)
- [Editar la política de seguridad](#)
- [Cambiar el flujo de trabajo administrado para su servidor](#)
- [Cambiar los banners de visualización de su servidor](#)
- [Puesta de un servidor de online u offline](#)

Edición de la configuración de un servidor

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Servidores.
3. Elija el identificador en la columna ID de servidor para ver la página Detalles del servidor, que se muestra a continuación.

Puede cambiar las propiedades del servidor en esta página al seleccionar Editar:

- Para cambiar los protocolos, consulte [Edite los protocolos de transferencia de archivos](#).
- Para el proveedor de identidad, ahora puede cambiar entre cualquier tipo de proveedor de identidad (gestionado por servicio, AWS Directory Service o proveedor de identidad personalizado). Para obtener más información sobre cómo cambiar los tipos de proveedores de identidad y la información necesaria para cada transición, consulte. [Editar la configuración del proveedor de identidad](#)

- Para cambiar el tipo de punto de conexión o el nombre de host personalizado, consulte [Editar el punto de conexión del servidor](#).
- Para añadir un acuerdo, primero debe añadir AS2 como protocolo a su servidor. Para obtener más información, consulte [Edite los protocolos de transferencia de archivos](#).
- Para administrar las claves de host de su servidor, consulte [Administre las claves de host de su SFTP-enabled servidor](#).
- En Detalles adicionales, puede editar la siguiente información:
 - Para cambiar el rol de registro, consulte [Edite la configuración de registro](#).
 - Para cambiar la política de seguridad, consulte [Editar la política de seguridad](#).
 - Para cambiar la clave de host del servidor, consulte [Administre las claves de host de su SFTP-enabled servidor](#).
 - Para cambiar el flujo de trabajo administrado del servidor, consulte [Cambiar el flujo de trabajo administrado para su servidor](#).
 - Para editar los banners de visualización de su servidor, consulte [Cambiar los banners de visualización de su servidor](#).
- En Additional configuration (Configuración adicional), puede editar la siguiente información:
 - SetStat opción: active esta opción para ignorar el error que se genera cuando un cliente intenta usarlo SETSTAT en un archivo que está cargando en un bucket de Amazon S3. Para obtener más información, consulte la SetStatOption documentación del [ProtocolDetails](#)tema.
 - Reanudación de la sesión TLS: proporciona un mecanismo para reanudar o compartir una clave secreta negociada entre el control y la conexión de datos para una sesión de FTPS. Para obtener más información, consulte la TlsSessionResumptionMode documentación del [ProtocolDetails](#)tema.
 - IP pasiva: indica el modo pasivo para los protocolos FTP y FTPS. Escriba una sola dirección IPv4, como la dirección IP pública de un cortafuegos, un enrutador o un equilibrador de carga. Para obtener más información, consulte la PassiveIp documentación del [ProtocolDetails](#)tema.

 Note

Evite colocar balanceadores de carga de red (NLB) o puertas de enlace NAT delante de los servidores. AWS Transfer Family Esta configuración aumenta los costes y puede provocar problemas de rendimiento. Para obtener más información,

consulte [Evite colocar los NLB y los NAT delante de AWS Transfer Family servidores](#)

- Para iniciar o detener el servidor, consulte [Puesta de un servidor de online u offline](#).
- Para eliminar un servidor, consulte [Eliminar un servidor](#).
- Para editar las propiedades de un usuario, consulte [Administrar los controles de acceso](#).

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider

[Edit](#)

Identity provider type
Service managed

Note

Los valores de Descripción y Fecha de importación de la clave del host del servidor son nuevos a partir de septiembre de 2022. Estos valores se introdujeron para admitir la característica de claves de host múltiples. Esta característica requería la migración de cualquier clave de host única que estuviera en uso antes de la introducción de varias claves de host.

El valor de Fecha de importación de una clave de host de servidor migrada se establece en la fecha de la última modificación del servidor. Es decir, la fecha que aparece en la clave de host migrada corresponde a la fecha en la que modificó el servidor de alguna forma por última vez, antes de la migración de la clave de host del servidor.

La única clave que se migró es la clave de host del servidor más antigua o la única. Todas las claves adicionales tienen su fecha real de cuando las importó. Además, la clave migrada tiene una descripción que permite identificarla fácilmente como si se hubiera migrado.

La migración se produjo entre el 2 y el 13 de septiembre. La fecha de migración real dentro de este intervalo depende de la región del servidor.

Edit

Additional details

Log group /aws/transfer/s-	Domain Amazon S3	SetStat option Ignore
Logging role Info -	Login display banner View the display message	TLS session resumption -
Security Policy Info TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	Optimized directories Info ENABLED	Passive IP -

Edite los protocolos de transferencia de archivos

En la AWS Transfer Family consola, puede editar el protocolo de transferencia de archivos. El protocolo de transferencia de archivos conecta al cliente con el punto de conexión del servidor.

Edición de los protocolos

1. En la página de Detalles del servidor, seleccione Editar junto a Protocolos.
2. En la página Editar protocolos, active o desactive la casilla o casillas del protocolo para añadir o quitar los siguientes protocolos de transferencia de archivos:

- Protocolo de File Transfer (SFTP) Secure Shell (SSH): File Transfer a través de SSH.

Para obtener más información acerca de SFTP, consulte [Crea un SFTP-enabled servidor](#).

- Protocolo seguro de File Transfer (FTPS): transferencia de archivos con cifrado TLS

Para obtener más información acerca de FTP, consulte [Cree un FTPS-enabled servidor](#).

- Protocolo de File Transfer (FTP): transferencia de archivos sin cifrado

Para obtener más información acerca de FTPS, consulte [Cree un servidor FTP-enabled](#).

Note

Si ya tiene un servidor compatible solo con SFTP y desea agregar FTPS y FTP, debe asegurarse de tener la configuración correcta de proveedor de identidad y tipo de punto de conexión que sea compatible con FTPS y FTP.

Edit protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

[Cancel](#)[Save](#)

Si selecciona FTPS, debe elegir un certificado almacenado en AWS Certificate Manager (ACM) que se utilizará para identificar el servidor cuando los clientes se conecten a él a través de FTPS.

Para solicitar un nuevo certificado público, consulte [Solicitar un certificado público](#) en la Guía del usuario de AWS Certificate Manager .

Para importar un certificado existente en ACM, consulte [Importación de certificados en ACM](#) en la Guía del usuario de AWS Certificate Manager .

Para solicitar un certificado privado para usar FTPS a través de direcciones IP privadas, consulte [Solicitar un certificado privado](#) en la Guía del usuario de AWS Certificate Manager .

Se admiten certificados con los siguientes algoritmos criptográficos y tamaños de clave:

- RSA de 2048 bits (RSA_2048)
- RSA de 4096 bits (RSA_4096)
- Curva elíptica principal de 256 bits (EC_prime256v1)
- Curva elíptica principal de 384 bits (EC_secp384r1)
- Curva elíptica principal de 521 bits (EC_secp521r1)

 Note

El certificado debe ser un certificado de SSL/TLS X.509 versión 3 válido con el FQDN o la dirección IP especificados y contener información sobre el emisor.

3. Seleccione Save. Regresará a la página de Detalles del servidor.

Editar el punto de conexión del servidor

En la AWS Transfer Family consola, puede modificar el tipo de punto final del servidor y el nombre de host personalizado. Además, en el caso de los puntos finales de la VPC, puede editar la información de la zona de disponibilidad.

Edición de los detalles del punto de conexión del servidor

1. En la página de Detalles del servidor, seleccione Editar junto a Detalles del punto de conexión.
2. Antes de poder editar el tipo de punto final, primero debe detener el servidor. A continuación, en la página Editar configuración de punto final, para el tipo de punto final, puede elegir uno de los siguientes valores:
 - Público: esta opción permite que su servidor sea accesible a través de Internet.
 - VPC : esta opción hace que su servidor sea accesible en su nube privada virtual (VPC). Para obtener información acerca de las VPC, consulte [Creación de un servidor en una nube privada virtual \(VPC\)](#).
3. Para el Nombre de host personalizado, elija una de las siguientes opciones:
 - Ninguno: si no desea utilizar un dominio personalizado, seleccione None.

Obtendrá un nombre de servidor proporcionado por AWS Transfer Family. El nombre de host del servidor tiene la forma `serverId.server.transfer.regionId.amazonaws.com`.

- Alias DNS de Amazon Route 53: para usar un alias de DNS creado automáticamente para usted en Route 53, seleccione esta opción.
- Otros DNS: para usar un nombre de host que ya posea en un servicio de DNS externo, seleccione Other DNS.

Al elegir el alias DNS de Amazon Route 53 u Otro DNS, se especifica el método de resolución de nombres que se va a asociar con el punto de conexión del servidor.

Por ejemplo, el nombre de dominio personalizado podría ser `sftp.inbox.example.com`. Un nombre de host personalizado utiliza el nombre de DNS indicado y un servicio DNS que puede resolverlo. Puede utilizar Route 53 para resolver los nombres de su DNS o utilizar su propio proveedor de servicios de DNS. Para obtener información sobre el modo en que AWS Transfer Family se utiliza Route 53 para dirigir el tráfico desde el dominio personalizado al punto de conexión, consulte [Uso de nombres de host personalizados](#).

4. En el caso de los puntos de enlace de VPC, puede cambiar la información en el panel Zonas de disponibilidad.
5. Seleccione Save. Regresará a la página de Detalles del servidor.

Edite la configuración de registro

En la AWS Transfer Family consola, puede cambiar la configuración de registro.

 Note

Si Transfer Family creó una función de IAM de CloudWatch registro para usted al crear un servidor, se llama a la función de IAM. `AWSTransferLoggingAccess` Puede usarlo para todos sus servidores de Transfer Family.

Edición de la configuración de registro

1. En la página de Detalles del servidor, seleccione Editar junto a Detalles adicionales.
2. Según su configuración, elija entre un rol de registro, un registro JSON estructurado o ambos. Para obtener más información, consulte [Actualización del registro de un servidor](#).

Editar la política de seguridad

Este procedimiento explica cómo cambiar la política de seguridad de un servidor Transfer Family mediante la AWS Transfer Family consola o AWS CLI.

 Note

Si su punto final lo es FIPS-enabled, no puede cambiar la política de seguridad FIPS por una política de seguridad que no sea FIPS.

Console

Para editar la política de seguridad mediante la consola

1. En la página de Detalles del servidor, seleccione Editar junto a Detalles adicionales.
2. En la sección Opciones de algoritmos criptográficos, elija una política de seguridad que contenga los algoritmos criptográficos habilitados para su uso en el servidor.

Para obtener más información sobre las políticas de seguridad, consulte [Políticas de seguridad para AWS Transfer Family servidores](#).

3. Seleccione Save.

Volverá a la página de detalles del servidor, donde podrá ver la política de seguridad actualizada.

AWS CLI

Para editar la política de seguridad mediante la CLI

1. Ejecute el siguiente comando para ver la política de seguridad actual que está adjunta al servidor.

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

Este `describe-server` comando devuelve todos los detalles del servidor, incluida la siguiente línea:

```
"SecurityPolicyName": "TransferSecurityPolicy-2018-11"
```

En este caso, la política de seguridad del servidor es `TransferSecurityPolicy-2018-11`.

2. Asegúrese de proporcionar el nombre exacto de la política de seguridad al comando. Por ejemplo, ejecute el siguiente comando para actualizar el servidor a `TransferSecurityPolicy-2023-05`.

```
aws transfer update-server --server-id your-server-id --security-policy-name  
"TransferSecurityPolicy-2023-05"
```

Note

Los nombres de las políticas de seguridad disponibles aparecen en [Políticas de seguridad para AWS Transfer Family servidores](#).

Si se ejecuta correctamente, el comando devuelve el siguiente código y actualiza la política de seguridad del servidor.

```
{  
  "ServerId": "your-server-id"  
}
```

Cambiar el flujo de trabajo administrado para su servidor

En la AWS Transfer Family consola, puede cambiar el flujo de trabajo gestionado asociado al servidor.

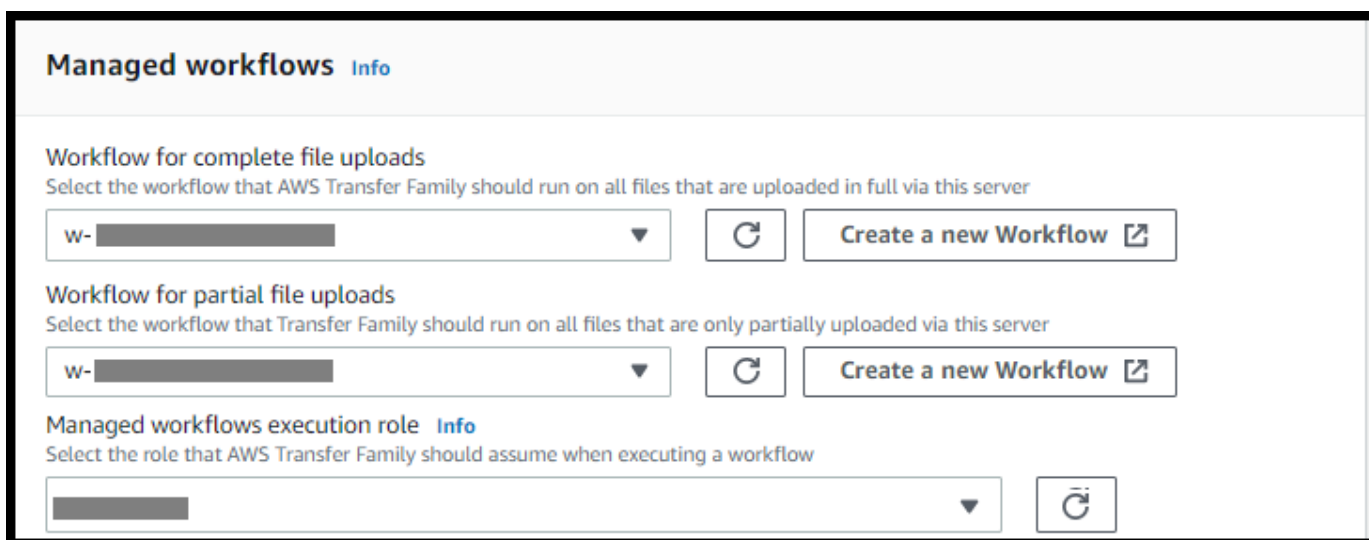
Cambio del flujo de trabajo administrado

1. En la página de Detalles del servidor, seleccione Editar junto a Detalles adicionales.
2. En la página Editar detalles adicionales, en la sección Flujos de trabajo administrados, seleccione un flujo de trabajo para que se ejecute en todas las cargas.

Note

Si aún no tiene un flujo de trabajo, seleccione Crear un nuevo flujo de trabajo para crear uno.

- a. Seleccione el ID del flujo de trabajo que desee utilizar.
- b. Seleccione un rol de ejecución. Este es el rol que asume Transfer Family al ejecutar los pasos del flujo de trabajo. Para obtener más información, consulte [Políticas de IAM para flujos de trabajo](#). Seleccione Save.



Managed workflows [Info](#)

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

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

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

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

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

[dropdown] [refresh]

3. Seleccione Save. Regresará a la página de Detalles del servidor.

Cambiar los banners de visualización de su servidor

En la AWS Transfer Family consola, puede cambiar los banners de visualización asociados al servidor.

Cómo cambiar los banners de visualización

1. En la página de Detalles del servidor, seleccione Editar junto a Detalles adicionales.
2. En la página Editar detalles adicionales, en la sección Banners de visualización, introduzca el texto de los banners de visualización disponibles.
3. Seleccione Save. Regresará a la página de Detalles del servidor.

Puesta de un servidor de online u offline

En la AWS Transfer Family consola, puede conectar o desconectar el servidor.

Activación en línea de su servidor

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación, seleccione Servers (Servidores).
3. Seleccione la casilla de verificación del servidor que está desactivado.
4. En Actions (Acciones), seleccione Start (Iniciar).

El cambio de un servidor de offline a online puede tardar algunos minutos.

Note

Aunque un servidor se detenga para ponerlo offline, se sigue incurriendo en cargos de servicio por él. Para evitar los cargos adicionales por un servidor, debe eliminar el servidor.

Desconexión del servidor

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación, seleccione Servers (Servidores).
3. Seleccione la casilla de verificación del servidor que está activado (online).
4. En Actions (Acciones), seleccione Stop (Detener).

Mientras un servidor se inicia o se detiene, no está disponible para realizar operaciones con archivos. La consola no muestra el estado de inicio o detención.

Si encuentra la condición de error `START_FAILED` o `STOP_FAILED`, póngase en contacto con nosotros AWS Support para que le ayuden a resolver los problemas.

Editar la configuración del proveedor de identidad

Puede cambiar el tipo de proveedor de identidad de su servidor de cualquier tipo a cualquier otro tipo. Los tipos de proveedores de identidad disponibles son:

- Servicio gestionado: almacene las credenciales de usuario dentro del servicio
- AWS Directory Service: utilice Microsoft AD AWS administrado o AWS Directory Service para los servicios de dominio Entra ID
- Personalizado: utilice la función Lambda o Amazon API Gateway para integrarlo con su proveedor de identidad existente

Al cambiar los tipos de proveedores de identidad, debe proporcionar información específica en función de la transición que vaya a realizar. En las siguientes secciones se describe la información necesaria para cada tipo de cambio.

Important

Consideraciones a la hora de cambiar de proveedor de identidad:

- Migración de usuarios: al cambiar los tipos de proveedores de identidad, las configuraciones de usuario existentes no se migran automáticamente. Deberá configurar los usuarios en el nuevo sistema del proveedor de identidades.
- Pruebas: pruebe minuciosamente la nueva configuración del proveedor de identidad antes de realizar el cambio en los entornos de producción.
- Permisos: asegúrese de que el nuevo proveedor de identidades tenga configurados los permisos y funciones de IAM necesarios antes de realizar el cambio.

Cambiar a un proveedor de identidades gestionado por un servicio

Al cambiar de cualquier otro tipo de proveedor de identidad a uno administrado por un servicio, debe:

- Seleccione Servicio gestionado como tipo de proveedor de identidades
- Cree nuevos usuarios directamente AWS Transfer Family después de completar el cambio, ya que las configuraciones de usuario existentes de otros proveedores de identidad no se transferirán

Ejemplo: si cambias de un proveedor de identidad personalizado a uno gestionado por el servicio, tendrás que volver a crear todas las cuentas de usuario y sus permisos asociados dentro del servicio.

AWS Transfer Family

Cambiar a AWS Directory Service

Al cambiar de cualquier otro tipo de proveedor de identidad a AWS Directory Service, debe proporcionar:

- Directorio: seleccione un Microsoft AD o AWS Directory Service AWS administrado existente para el directorio de Entra ID Domain Services
- Acceso: elija si desea restringir el acceso a un grupo específico o permitir el acceso a todos los usuarios del directorio
- Función de acceso: función de IAM que permite acceder AWS Transfer Family a su directorio

Ejemplo: si va a cambiar de un servicio gestionado a uno de AWS Directory Service, debe seleccionar el d-1234567890 directorio existente, restringir el acceso al TransferUsers grupo y especificar la función de TransferDirectoryAccessRole IAM.

Cambiar a un proveedor de identidad personalizado

Al cambiar de cualquier otro tipo de proveedor de identidad a uno personalizado, debe elegir entre la función Lambda o Amazon API Gateway y proporcionar la configuración requerida:

Uso de la función Lambda

Para la integración de funciones Lambda, proporcione:

- Función: seleccione una función Lambda existente que gestione la autenticación
- Método de autenticación (para el protocolo SFTP): elija la contraseña, la clave pública o ambas

Ejemplo: si va a cambiar de AWS Directory Service a un proveedor de identidades Lambda personalizado, debe seleccionar su `TransferCustomAuth` función y elegir Password como método de autenticación.

Transfer Family > Servers > s- > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

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

☐ Service managed
Create and manage users within the service

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

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

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

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

AWS Lambda function

▼



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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

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

Cancel

Save

Uso de Amazon API Gateway

Para la integración de Amazon API Gateway, proporcione:

- URL de API Gateway: la URL de invocación de su punto final de API Gateway
- Función de invocación: una función de IAM que permite AWS Transfer Family invocar su API Gateway
- Método de autenticación (para el protocolo SFTP): elija la contraseña, la clave pública o ambas

Ejemplo: si cambias de servidor gestionado a API Gateway, debes proporcionar la URL `https://abcdef123.execute-api.us-east-1.amazonaws.com/prod`, especificar la función de `TransferApiGatewayInvocationRole` IAM y elegir clave pública como método de autenticación.

Transfer Family > Servers > s-[redacted] > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

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

☐ Service managed
Create and manage users within the service

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

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

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

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

Provide an Amazon API Gateway URL

Invocation role
IAM role for the service to invoke your Amazon API Gateway URL

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

☒ Password OR public key
☐ Password ONLY
☐ Public Key ONLY
☐ Password AND public key

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

Cancel Save

Cambio de Amazon API Gateway a la función Lambda

Una transición común es cambiar de Amazon API Gateway a la función Lambda para la integración de proveedores de identidad personalizados. Este cambio le permite simplificar su arquitectura y, al mismo tiempo, mantener la misma lógica de autenticación.

Consideraciones clave para esta transición:

- Misma función, permisos diferentes: puedes usar la misma función de Lambda para la integración de API Gateway y Lambda directa, pero la política de recursos debe actualizarse.
- Requisitos de la política de recursos: al cambiar a una integración Lambda directa, la política de recursos de la función debe conceder `transfer.amazonaws.com` permiso para invocar la función, además de `apigateway.amazonaws.com`

Para realizar este cambio

1. Actualice la política de recursos de la función Lambda para permitir la invocación `transfer.amazonaws.com` de la función.
2. En la AWS Transfer Family consola, cambie el proveedor de identidad de API Gateway a función Lambda.
3. Seleccione la función Lambda existente.
4. Pruebe la configuración para asegurarse de que la autenticación funciona correctamente.

Ejemplo de política de recursos para la integración directa de Lambda:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "transfer.amazonaws.com",
        "apigateway.amazonaws.com"
      ]
    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:function-name"
  }]
}
```

Preservación del usuario durante las transiciones entre proveedores de identidad

Al cambiar de un tipo de proveedor de identidad a otro, las configuraciones de usuario existentes se conservan en escenarios específicos para permitir una reversión eficiente en caso de problemas:

- Service-managed al proveedor de identidades personalizado y viceversa: si cambias de un proveedor de identidades gestionado por el servicio a uno personalizado y, después, vuelves a uno gestionado por el servicio, todos los usuarios se mantienen en su última configuración conocida.
- AWS Directory Service a un proveedor de identidades personalizado y viceversa: si cambias de un proveedor de AWS Directory Service identidades personalizado y luego vuelves a AWS Directory Service, todas las definiciones de los grupos de acceso delegado se conservan en su última configuración conocida.

Este comportamiento de conservación le permite probar de forma segura las configuraciones de los proveedores de identidades personalizados y volver a la configuración anterior sin perder las configuraciones de acceso de los usuarios.

Consideraciones importantes a la hora de cambiar de proveedor de identidad

- Migración de usuarios: al cambiar los tipos de proveedores de identidad, las configuraciones de usuario existentes no se migran automáticamente. Deberá configurar los usuarios en el nuevo sistema del proveedor de identidades.
- Pruebas: pruebe minuciosamente la nueva configuración del proveedor de identidad antes de realizar el cambio en los entornos de producción.
- Permisos: asegúrese de que el nuevo proveedor de identidades tenga configurados los permisos y funciones de IAM necesarios antes de realizar el cambio.

Administre las claves de host de su SFTP-enabled servidor

Las claves de host del servidor son claves privadas que utiliza el servidor Transfer Family para proporcionar una identidad única a la persona que llama y garantizar que es el servidor correcto. Esa garantía se ve reforzada por la presencia de la clave pública correcta en el archivo de la persona que

llamado `known_hosts`. (El `known_hosts` archivo es una función estándar que utilizan la mayoría de los clientes SSH para almacenar las claves públicas de los servidores a los que te has conectado). Puedes recuperar la clave pública que corresponde a la clave de host de tu servidor ejecutándola `ssh-keyscan` para tu servidor.

 Important

El cambio accidental de la clave de host de un servidor puede ser disruptivo. Según cómo esté configurado el cliente SFTP, puede fallar inmediatamente, con el mensaje de que no existe una clave de host de confianza o presentar mensajes amenazantes. Si hay scripts para automatizar las conexiones, lo más probable es que también fallen.

De forma predeterminada, AWS Transfer Family genera claves de host para el SFTP-enabled servidor. Puede importar las claves de host del servidor para preservar la identidad del host y evitar actualizar los almacenes de confianza de los clientes. [Cuándo importar las claves de host](#) enumera algunos motivos por los que puede que desee hacerlo. Si no proporciona claves de host, se generarán nuevas claves para usted.

AWS Transfer Family admite varias claves de host de distintos tipos (RSA, ECDSA y ED25519) para ofrecer compatibilidad con una gama más amplia de algoritmos de firma del host del cliente. Los distintos tipos de claves permiten algoritmos específicos: las claves RSA activan los algoritmos `rsa-*`, las claves ECDSA activan los algoritmos `ecdsa-*` y las claves ED25519 activan los algoritmos `ed25519`. Planifique los tipos de claves al momento de crear el servidor, ya que introducir tipos de claves adicionales una vez que los clientes hayan empezado a interactuar con el servidor puede ser perjudicial para algunos clientes y puede resultar tan problemático como sustituir las claves de host existentes.

Para evitar que se pida a los usuarios que vuelvan a comprobar la autenticidad del SFTP-enabled servidor, importe la clave de host del servidor local al SFTP-enabled servidor. Hacer esto también evita que sus usuarios reciban una advertencia sobre un posible ataque man-in-the-middle.

También, puede rotar las claves del host periódicamente, como medida de seguridad adicional. Para obtener más información, consulte [Rotar las claves del host del servidor](#).

 Note

Los servidores que admiten el protocolo SFTP utilizan las claves de host del servidor.

Cuándo importar las claves de host

Si bien AWS Transfer Family puede generar claves de host automáticamente, hay varios escenarios en los que la importación de sus propias claves de host proporciona beneficios operativos:

- Migración de servidores: está migrando de un servidor existente a un servidor existente AWS Transfer Family y desea evitar actualizar los almacenes de confianza (known_hosts archivos) de los clientes existentes.
- Recuperación ante desastres y conmutación por error: tiene varios AWS Transfer Family servidores (por ejemplo, uno en EE. UU. este (Ohio) y otro en EE. UU. oeste (Oregón)) que comparten el mismo nombre de DNS público. El uso de las mismas claves de host en ambos servidores garantiza una conmutación por error sin fallos en la autenticación del cliente.
- Continuidad operativa: desea que el material clave del host esté disponible para su uso con otros servidores (AWS Transfer Family o de otro tipo) en el futuro a fin de mantener una identidad de servidor coherente en toda su infraestructura.
- Control de algoritmos: desea una mayor compatibilidad con los clientes proporcionando más algoritmos de clave de host, o quiere controlar qué algoritmos pueden usar los clientes ofreciendo únicamente claves compatibles con algoritmos específicos.

En los temas siguientes se proporcionan procedimientos detallados para administrar las claves de host del servidor:

- [Agregue una clave de host de servidor adicional](#)- Añada claves de host adicionales a su servidor
- [Eliminar una clave de host](#)- Elimine las claves de host de su servidor
- [Rotar las claves del host del servidor](#)- Gire las claves del host para mejorar la seguridad
- [Información adicional sobre la clave del host del servidor](#)- Vea y gestione los detalles clave del host

Agregue una clave de host de servidor adicional

En la AWS Transfer Family consola, puede añadir claves de host de servidor adicionales. Añadir claves de host adicionales de distintos formatos puede resultar útil para identificar un servidor cuando los clientes se conectan a él, así como para mejorar el perfil de seguridad. Por ejemplo, si la clave original es una clave RSA, puede añadir una clave ECDSA adicional.

 Note

El cliente SFTP se conectará mediante la clave más antigua de la configuración que coincida con el algoritmo de la clave. La clave más antigua de cada tipo de clave (RSA, ECDSA o ED25519) es la clave activa del servidor de ese tipo.

Nota de seguridad cuando un servidor Transfer Family tiene varios tipos de claves de host

Si un servidor tiene varios tipos de claves de host, el cliente SFTP puede asignar una preferencia por tipo. Por lo tanto, cuando existen claves de host RSA, ECDSA y ED25519 para el servidor, la elección depende de la preferencia por tipo.

Los clientes SFTP modernos prefieren las claves de host ECDSA y ED25519 cuando existen. Esto es importante si desea agregar una clave ECDSA o ED25519 cuando el servidor anteriormente solo tenía claves RSA. La adición de la nueva clave ECDSA o ED25519 podría manifestarse como una advertencia de seguridad para un cliente.

Para el cliente, la clave aparecerá como si hubiera cambiado, cuando en realidad no se ha modificado: la nueva clave se agregó además de la clave RSA existente. Tenga esto en cuenta si decide agregar nuevos tipos de claves de host de servidor.

Cómo agregar una clave de host de servidor adicional

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Servidores y, a continuación, un servidor que utilice el protocolo SFTP.
3. En la página de detalles del servidor, desplácese hacia abajo hasta la sección Claves de host del servidor.

Server host keys (2)

Actions 

Add host key

 1 

☐	Name 	Host key ID 	Fingerprint Info	Description 	Key type 	Date imported 
☐	Default host key	hostkey- 	SHA256: 	Default	ssh-rsa	2023-06-30
☐	ecdsa-521	hostkey- 	SHA256: 	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13

4. Seleccione Añadir clave de host.

Aparece la página Agregar clave de host del servidor.

5. En la sección Clave de host del servidor, introduzca una clave privada RSA, ECDSA o ED25519 que se utilice para identificar el servidor cuando los clientes se conecten a él a través del servidor. SFTP-enabled

 Note

Al crear una clave de host del servidor, asegúrese de especificarla `-N ""` (sin contraseña). Consulte [Creación de claves SSH en macOS, Linux o Unix](#) para obtener más información acerca de cómo generar pares de claves.

6. (Opcional) Añada una descripción para diferenciar entre varias claves de host del servidor. También, puede agregar etiquetas para su clave.
7. Seleccione Add key (Añadir clave). Regresará a la página de Detalles del servidor.

Para añadir una clave de host mediante AWS Command Line Interface (AWS CLI), utilice la operación [ImportHostKey](#) API y proporcione la nueva clave de host. Si crea un SFTP-enabled servidor nuevo, proporciona su clave de host como parámetro en la operación de la [CreateServer](#) API. También puedes utilizarla AWS CLI para actualizar la descripción de una clave de host existente.

El siguiente `import-host-key` AWS CLI comando de ejemplo importa una clave de host para el SFTP-enabled servidor especificado.

```
aws transfer import-host-key --description key-description --server-id your-server-id
--host-key-body file://my-host-key
```

Eliminar una clave de host

En la AWS Transfer Family consola, puede eliminar una clave de host del servidor.

Eliminación de una clave de host

1. Abra la AWS Transfer Family consola en <https://console.aws.amazon.com/transfer/>.
2. En el panel de navegación izquierdo, seleccione Servidores y, a continuación, un servidor que utilice el protocolo SFTP.
3. En la página de detalles del servidor, desplácese hacia abajo hasta la sección Claves de host del servidor.

Server host keys (2)							Actions ▾	Add host key
Find resources							< 1 >	
☐	Name	Host key ID ▾	Fingerprint Info	Description ▾	Key type ▾	Date imported ▾		
☐	Default host key	hostkey-	SHA256:	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey-	SHA256:	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

- En la sección Claves de host del servidor, seleccione una clave y, a continuación, en Acciones, seleccione Eliminar.
- En la ventana de diálogo de confirmación que aparece, ingrese la palabra **delete**, y luego seleccione Eliminar para confirmar que desea eliminar el host del servidor.

La clave de host se elimina de la página Servidores.

Para eliminar la clave de host mediante AWS CLI, utilice la operación de [DeleteHostKey](#) API y proporcione el ID del servidor y el ID de la clave de host.

El siguiente delete-host-key AWS CLI comando de ejemplo elimina una clave de host del SFTP-enabled servidor especificado.

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

Rotar las claves del host del servidor

Periódicamente, puede rotar la clave de host del servidor. En este tema se describe cómo el servidor elige qué clave aplicar y el procedimiento para rotar estas claves.

Cómo elige el cliente una clave de host del servidor

La forma en que Transfer Family elige qué clave de servidor aplicar depende de las condiciones del cliente SFTP, como se explica aquí. Se supone que hay una clave más antigua y otra más nueva.

- Un cliente SFTP no tiene una clave de host pública anterior para el servidor. La primera vez que el cliente se conecta al servidor, ocurre una de las siguientes situaciones:
 - El cliente falla en la conexión, si está configurado para hacerlo.
 - O bien, el cliente elige la primera clave que coincide con los posibles algoritmos disponibles y pregunta al usuario si se puede confiar en esa clave. Si es así, el cliente actualiza automáticamente el `known_hosts` archivo (o cualquier archivo o recurso de configuración local que el cliente utilice para registrar las decisiones de confianza) e introduce esa clave.

- Un cliente SFTP tiene una clave antigua en su `known_hosts` archivo. El cliente prefiere usar esta clave, incluso si existe una clave más nueva, ya sea para el algoritmo de esta clave o para otro algoritmo. Esto se debe a que el cliente tiene un mayor nivel de confianza en la clave que se encuentra en su `known_hosts` archivo.
- Un cliente SFTP tiene la nueva clave (en cualquiera de los algoritmos disponibles) en su archivo de `known_hosts` claves. El cliente ignora las claves antiguas porque no son de confianza y usa la nueva clave.
- Un cliente SFTP tiene ambas claves en su `known_hosts` archivo. El cliente elige la primera clave por índice que coincide con la lista de claves disponibles que ofrece el servidor.

Transfer Family prefiere que el cliente SFTP tenga todas las claves en su `known_hosts` archivo, ya que esto permite una mayor flexibilidad a la hora de conectarse a un servidor de Transfer Family. La rotación de claves se basa en el hecho de que pueden existir varias entradas en el `known_hosts` archivo para el mismo servidor Transfer Family.

Gire la clave del host del servidor (procedimiento)

Como ejemplo, supongamos que ha agregado el siguiente conjunto de claves de host de servidor a su servidor Transfer Family.

Claves de host del servidor

Tipo de clave de host	Fecha en que se añadió al servidor
RSA	1 de abril de 2020
ECDSA	1 de febrero de 2020
ED25519	1 de diciembre de 2019
RSA	1 de octubre de 2019
ECDSA	1 de junio de 2019
ED25519	1 de marzo de 2019

Rotación de las claves del host del servidor

1. Agregue una nueva clave de host del servidor. Este procedimiento se describe en [Agregue una clave de host de servidor adicional](#).
2. Elimine una o más claves de host del mismo tipo que las que había agregado anteriormente. Este procedimiento se describe en [Eliminar una clave de host](#).
3. Todas las claves están visibles y pueden estar activas, según el comportamiento descrito anteriormente en [Cómo elige el cliente una clave de host del servidor](#).

Información adicional sobre la clave del host del servidor

Puede seleccionar una clave de host para mostrar los detalles de esa clave.

Transfer Family > Servers > s-3fe215d89f074ed2a > Hostkey: hostkey-a6fed60bcb704ea9b

hostkey-a6fed60bcb704ea9b

Delete

Host key configuration

Edit

Name

ecdsa-521

Fingerprint

SHA256: [redacted]

Description

ECDSA host key

Key type

ecdsa-sha2-nistp521

Date imported

Thu, 13 Jun 2024 17:08:59 GMT

Amazon Resource Name (ARN)

 arn:aws:transfer:us-east-1:[redacted]:host-key/s-[redacted]/hostkey-a-[redacted]

Puede eliminar una clave de host o editar su descripción desde el menú Acciones de la pantalla de detalles del servidor. Seleccione la clave de host y, a continuación, la acción adecuada en el menú.

Server host keys (2)

Find resources

Actions

Edit

Delete

Add host key

< 1 >

☐	Name	Host key ID	Fingerprint	Description	Key type	Date imported
☐	Default host key	hostkey-[redacted]	SHA256:[redacted]	Default	ssh-rsa	2023-06-30
☒	ecdsa-521	hostkey-[redacted]	SHA256:[redacted]	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13

Monitoreo del uso en la consola

Puede obtener información sobre las métricas de su servidor en su página Detalles del servidor. Esto le proporciona un lugar único para supervisar sus cargas de trabajo de transferencia de archivos.

Puede realizar un seguimiento del número de archivos que ha intercambiado con sus socios y realizar un seguimiento exhaustivo de su uso mediante un panel de control centralizado. Para obtener más información, consulte [Vea los detalles de los servidores SFTP, FTPS y FTP](#). En la siguiente tabla, se describen las métricas disponibles para Transfer Family.

Namespace	Métrica	Description (Descripción)
AWS/Transfer	BytesIn	El número total de bytes transferidos al servidor. Criterios de notificación: • Para SFTP/FTP/FTPS: se emite cada 5 minutos mientras se establece una conexión con el servidor Transfer Family. Si no se transfiere ningún archivo o byte durante el período, se emite un «0». • Para AS2: cuando el cliente recibe un mensaje en su servidor AS2 y lo emite tan pronto como el mensaje entrante termina de procesarse Unidades: recuento Periodo: 5 minutos
	BytesOut	El número total de bytes transferidos desde el servidor. Criterios de información: • Para SFTP/FTP/FTPS: se emite cada 5 minutos mientras se establece una conexión con el servidor Transfer Family. Si no se transfiere ningún archivo o byte durante el período, se emite un «0». • Para AS2: cuando el cliente llama <code>StartFile Transfer</code> desde su conector AS2 y se emite tan pronto como el mensaje saliente termina de procesarse. Unidades: recuento

Namespace	Métrica	Description (Descripción)
		Periodo: 5 minutos
	FilesIn	El número total de archivos transferidos al servidor. Para los servidores que utilizan el protocolo AS2, esta métrica representa la cantidad de mensajes recibidos. Criterios de información: • Para SFTP/FTP/FTPS: se emite cada 5 minutos mientras se establece una conexión con el servidor Transfer Family. Si no se transfiere ningún archivo o byte durante el período, se emite un «0». • Para AS2: cuando el cliente recibe un mensaje en su servidor AS2 y lo emite tan pronto como el mensaje entrante termina de procesarse. Unidades: recuento Periodo: 5 minutos

Namespace	Métrica	Description (Descripción)
	FilesOut	El número total de archivos transferidos desde el servidor. Criterios de información: • Para SFTP/FTP/FTPS: se emite cada 5 minutos mientras se establece una conexión con el servidor Transfer Family. Si no se transfiere ningún archivo o byte durante el período, se emite un «0». • Para AS2: cuando el cliente llama <code>StartFile Transfer</code> desde su conector AS2 y se emite tan pronto como el mensaje saliente termina de procesarse. Unidades: recuento Periodo: 5 minutos
	InboundMessage	El número total de mensajes AS2 recibidos correctamente de un socio comercial. Criterios de notificación: cuando el cliente recibe un mensaje en su servidor AS2 y lo emite tan pronto como el mensaje entrante termina de procesarse correctamente Unidades: recuento Periodo: 5 minutos

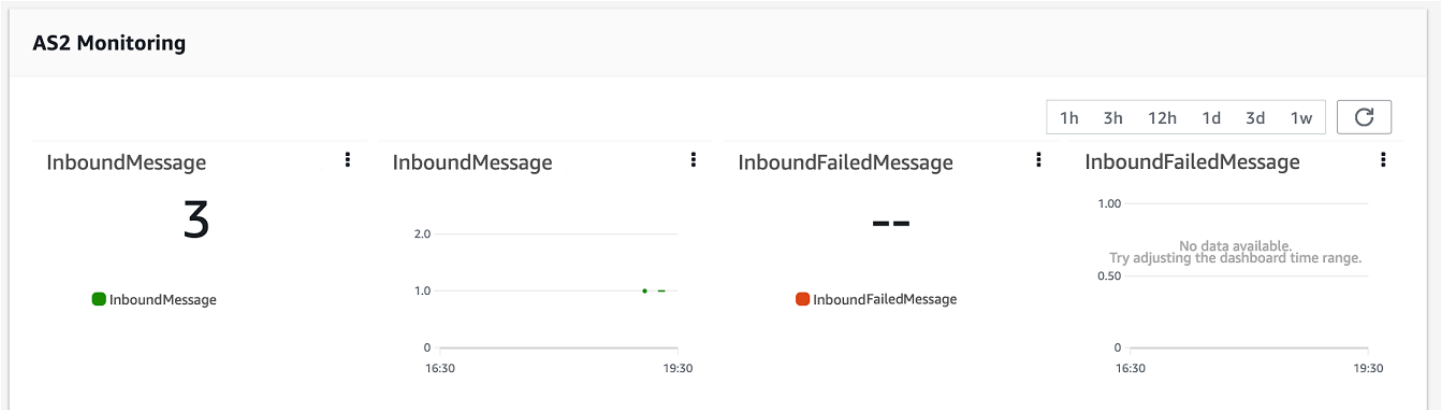
Namespace	Métrica	Description (Descripción)
	InboundFailedMessage	El número total de mensajes AS2 que se recibieron sin éxito de un socio comercial. Es decir, un socio comercial envió un mensaje, pero el servidor de Transfer Family no pudo procesarlo correctamente. Criterios de notificación: cuando el cliente recibe un mensaje en su servidor AS2 y lo emite tan pronto como el mensaje entrante termina de procesarse sin éxito Unidades: recuento Periodo: 5 minutos
	OnUploadExecutionsStarted	La cantidad total de ejecuciones de flujos de trabajo iniciadas en el servidor. Criterios de notificación: se activa cada vez que se inicia una ejecución Unidades: recuento Periodo: 1 minuto
	OnUploadExecutionsSuccess	La cantidad total de ejecuciones satisfactorias del flujo de trabajo en el servidor. Criterios de informe: se activa cada vez que una ejecución finaliza correctamente Unidades: recuento Periodo: 1 minuto

Namespace	Métrica	Description (Descripción)
	OnUploadExecutionsFailed	La cantidad total de ejecuciones de flujos de trabajo fallidas en el servidor. Criterios de informe: se activa cada vez que una ejecución no finaliza correctamente Unidades: recuento Periodo: 1 minuto
	OutboundMessage	El número total de mensajes AS2 enviados correctamente a un socio comercial. Criterios de notificación: cuando el cliente llama <code>StartFileTransfer</code> desde su conector AS2 y se emite tan pronto como el mensaje saliente termina de procesarse correctamente Unidades: recuento Periodo: 5 minutos
	OutboundFailedMessage	El número total de mensajes AS2 que se enviaron sin éxito a un socio comercial. Criterios de notificación: cuando el cliente llama <code>StartFileTransfer</code> desde su conector AS2 y se emite tan pronto como el mensaje saliente termina de procesarse sin éxito Unidades: recuento Periodo: 5 minutos

La sección Monitoreo contiene cuatro gráficos individuales. Estos gráficos muestran los bytes que entran, los bytes que salen, los archivos que entran y los archivos que salen.



Para los servidores que tienen el protocolo AS2 habilitado, hay una sección de Monitoreo de AS2 debajo de la información de Monitoreo. Esta sección contiene detalles sobre el número de mensajes entrantes, tanto correctos como fallidos.



Para abrir el gráfico seleccionado en su propia ventana, seleccione el icono de expansión ().

También puede hacer clic en el icono de puntos suspensivos verticales de un gráfico ()

para abrir un menú desplegable con los siguientes elementos:

- Ampliar: abre el gráfico seleccionado en su propia ventana.
- Actualizar: vuelve a cargar el gráfico con los datos más recientes.
- Ver en métricas: abre los detalles de las métricas correspondientes en Amazon CloudWatch.
- Ver registros: abre el grupo de registros correspondiente en CloudWatch.

Administrar los controles de acceso

Puede controlar el acceso de un usuario a AWS Transfer Family los recursos mediante una política AWS Identity and Access Management (IAM). Una política de IAM es una declaración, normalmente en formato JSON, que permite un determinado nivel de acceso a un recurso. Puede utilizar una política de IAM para definir las operaciones con archivos que desea permitir o prohibir a sus usuarios. También puede utilizar una política de IAM para definir el bucket o buckets de Amazon S3 a los que los usuarios puedan tener acceso. Para especificar estas políticas para los usuarios, debe crear un rol de IAM AWS Transfer Family que tenga asociadas la política de IAM y la relación de confianza.

A cada usuario se le asigna un rol de IAM. El tipo de función de IAM que se AWS Transfer Family utiliza se denomina función de servicio. Cuando un usuario inicia sesión en su servidor, AWS Transfer Family asume la función de IAM asignada al usuario. Para obtener información sobre cómo crear un rol de IAM que proporcione a un usuario acceso a un bucket de Amazon S3, consulte [Crear un rol para delegar permisos a un AWS servicio](#) en la Guía del usuario de IAM.

Puede conceder acceso de solo escritura a los objetos de Amazon S3 mediante determinados permisos de una política de IAM. Para obtener más información, consulte [Otorgue la capacidad de escribir y enumerar únicamente archivos](#).

El blog sobre AWS almacenamiento contiene una publicación en la que se detalla cómo configurar el acceso con privilegios mínimos. Para obtener más información, consulte [Implementación del acceso con privilegios mínimos en un AWS Transfer Family flujo de trabajo](#).

Note

Si su bucket de Amazon S3 está cifrado con AWS Key Management Service (AWS KMS), debe especificar permisos adicionales en su política. Para obtener más información, consulte [Protección y cifrado de datos](#). Además, puede consultar más información sobre [las políticas de sesión](#) en la Guía del usuario de IAM.

Temas

- [Autorización del acceso de lectura y escritura a un bucket de Amazon S3](#)
- [Creación de una política de sesión para un bucket de Amazon S3](#)

- [Enfoques de gestión dinámica de permisos](#)

Autorización del acceso de lectura y escritura a un bucket de Amazon S3

En esta sección se describe cómo crear una política de IAM que permita el acceso de escritura y lectura a un bucket de Amazon S3 específico. Al asignar un rol de IAM que tenga esta política de IAM a su usuario, este tendrá read/write acceso al bucket de Amazon S3 especificado.

La política siguiente proporciona acceso de lectura y escritura por programación a un bucket de Amazon S3. Los estados de cuenta GetObjectACL y PutObjectACL solo son obligatorios si necesitas habilitar el acceso entre cuentas. Es decir, el servidor de Transfer Family necesita acceder a un bucket de otra cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteS3",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/*"]
    }
  ]
}
```

```
]
}
```

La acción `ListBucket` requiere permiso sobre el bucket en sí. Las acciones `PUT`, `GET` y `DELETE` requieren permisos de objeto. Dado que se trata de entidades diferentes, se especifican con nombres de recurso de Amazon (ARN) distintos.

Para reducir aún más el ámbito de acceso de sus usuarios y restringirlo al directorio home del bucket de Amazon S3 especificado, consulte [Creación de una política de sesión para un bucket de Amazon S3](#).

Creación de una política de sesión para un bucket de Amazon S3

Una política de sesión es una política AWS Identity and Access Management (IAM) que restringe a los usuarios a determinadas partes de un bucket de Amazon S3. Esto se consigue evaluando el acceso en tiempo real.

Note

Las políticas de sesión solo se utilizan con Amazon S3. En el caso de Amazon EFS, se utilizan los permisos de archivos POSIX para limitar el acceso.

Puede usar una política de sesión cuando sea necesario proporcionar a un grupo de usuarios el mismo acceso a una parte determinada del bucket de Amazon S3. Por ejemplo, puede que un grupo de usuarios solo requiera acceso al directorio home. Ese grupo de usuarios comparte el mismo rol de IAM.

Note

La longitud máxima de una ruta es 2048 caracteres. Para obtener más información, consulte el [Parámetro de solicitud de política](#) correspondiente a la acción de `CreateUser` en la Referencia de la API.

Para crear una política de sesión, utilice las variables siguientes en su política de IAM:

- `${transfer:HomeBucket}`

- `${transfer:HomeDirectory}`
- `${transfer:HomeFolder}`
- `${transfer:UserName}`

Important

No puede usar las variables anteriores en Políticas administradas. Tampoco puede utilizarlas como variables de política en una definición de roles de IAM. Puede crear estas variables en una política de IAM y especificarlas directamente al configurar el usuario. Tampoco puede utilizar la variable `${aws:Username}` en esta política de sesión. Esta variable hace referencia a un nombre de usuario de IAM, no al nombre de usuario que AWS Transfer Family necesita.

Ejemplo de política de sesión

El código siguiente muestra un ejemplo de política de sesión.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::${transfer:HomeBucket}"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "${transfer:HomeFolder}/*",
            "${transfer:HomeFolder}"
          ]
        }
      }
    }
  ],
}
```

```
{
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion",
    "s3:GetObjectACL",
    "s3:PutObjectACL"
  ],
  "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
}
```

Note

En el ejemplo de política anterior se supone que los directorios principales de los usuarios están configurados para incluir una barra al final, lo que significa que se trata de un directorio. Si, por el contrario, establece el `HomeDirectory` de un usuario sin la barra final, debe incluirlo como parte de su política.

En el ejemplo anterior de política, anote el uso de los parámetros de la política `transfer:HomeFolder`, `transfer:HomeBucket` y `transfer:HomeDirectory`. Estos parámetros se establecen para el `HomeDirectory` que está configurado para el usuario, tal y como se describe en [HomeDirectory](#) y [Implementación de su método de API Gateway](#). Estos parámetros tienen las siguientes definiciones:

- El parámetro `transfer:HomeBucket` se sustituye por el primer componente de `HomeDirectory`.
- El parámetro `transfer:HomeFolder` se sustituye por las partes restantes del parámetro `HomeDirectory`.
- Se ha eliminado la barra inclinada inicial (/) del parámetro `transfer:HomeDirectory` para que pueda usarse como parte de un nombre de recurso de Amazon (ARN) de S3 en una declaración de `Resource`.

 Note

Si utiliza directorios lógicos, es decir, el `homeDirectoryType` del usuario es `LOGICAL`, estos parámetros de política (`HomeBucket`, `HomeDirectory` y `HomeFolder`) no son compatibles.

Por ejemplo, supongamos que el parámetro `HomeDirectory` que está configurado para el usuario de Transfer Family es `/home/bob/amazon/stuff/`.

- `transfer:HomeBucket` toma el valor de `/home`.
- `transfer:HomeFolder` toma el valor de `/bob/amazon/stuff/`.
- `transfer:HomeDirectory` se convierte en `home/bob/amazon/stuff/`.

El primer "Sid" permite al usuario enumerar todos los directorios a partir de `/home/bob/amazon/stuff/`.

El segundo "Sid" limita los accesos del usuario `put` y `get` a la misma ruta, `/home/bob/amazon/stuff/`.

Al aplicar la política anterior, cuando un usuario inicia sesión solo tiene acceso a los objetos de su directorio de inicio. En el momento de la conexión, AWS Transfer Family reemplaza estas variables por los valores adecuados para el usuario. Esto facilita la aplicación de los mismos documentos de política a múltiples usuarios. Este método reduce el trabajo de administración de roles y políticas de IAM para el acceso de los usuarios al bucket de Amazon S3.

También puede utilizar una política de sesión para personalizar el acceso de cada usuario en función de los requisitos de su negocio. Para obtener más información, consulte [los permisos para AssumeRole AssumeRoleWithSAML, y AssumeRoleWithWebIdentity](#) en la Guía del usuario de IAM.

 Note

AWS Transfer Family almacena el JSON de la política, en lugar del nombre de recurso de Amazon (ARN) de la política. Por lo tanto, cuando cambias la política en la consola de IAM, tienes que volver a la AWS Transfer Family consola y actualizar a tus usuarios con el contenido más reciente de la política. Puede actualizar el usuario en la pestaña Información de la política en la sección Configuración de usuario.

Si utiliza la AWS CLI, puede utilizar el siguiente comando para actualizar la política.

```
aws transfer update-user --server-id server --user-name user --policy \  
    "$ (aws iam get-policy-version --policy-arn policy --version-id version --  
    output json)"
```

Sustituciones anidadas de las políticas de sesión

Las sustituciones anidadas no se realizan en las políticas de sesión de Transfer Family. Las políticas de sesión pueden usar variables anidadas, como. `${transfer:HomeDirectory}`. Cuando se procesa la política, es posible que la variable externa (por ejemplo, `${transfer:HomeDirectory}`) se sustituya por un valor que contenga otra variable (por ejemplo, `{amzn-s3-demo-bucket:/$ (transfer:UserName)}`). Sin embargo, la variable anidada ya no se sustituye por el nombre de usuario real (por ejemplo, johndoe).

Esto significa que, al crear políticas de sesión para Transfer Family, debe tener en cuenta este comportamiento y asegurarse de que la estructura de políticas y el uso de variables estén diseñados en consecuencia. Es posible que las variables anidadas no se resuelvan como se esperaba y que la política no conceda los permisos previstos. Es importante probar y validar exhaustivamente las políticas de sesión para garantizar que funcionan según lo esperado. Este comportamiento es una consideración clave a la hora de implementar el control de acceso y los permisos para su entorno Transfer Family.

Una solución a este problema es utilizar el nombre real del bucket de Amazon S3 en la política de sesión. Así, por ejemplo, en lugar de especificarlo `${transfer:HomeDirectory}` en su política de sesión, utilice lo siguiente, donde `amzn-s3-demo-bucket` es su bucket real: `${amzn-s3-demo-bucket/transfer:UserName}`

Enfoques de gestión dinámica de permisos

Descripción de la arquitectura de permisos de Transfer Family

AWS Transfer Family admite la gestión dinámica de permisos mediante políticas de sesión, que permiten restringir los permisos efectivos de las funciones de IAM en tiempo de ejecución. Este enfoque funciona tanto para los usuarios gestionados por el servicio como para los usuarios de proveedores de identidad personalizados, pero solo se admite cuando se transfieren archivos hacia o desde Amazon S3 (no Amazon EFS).

Cada AWS Transfer Family usuario opera con un modelo de permisos que consiste en:

1. Función básica de IAM: define los permisos fundamentales del usuario
2. Política de sesión opcional: restringe (reduce el alcance) los permisos básicos en tiempo de ejecución

Los permisos efectivos son la intersección de los permisos del rol base y los permisos de la política de sesión. Las políticas de sesión solo pueden restringir los permisos; no pueden conceder permisos adicionales más allá de lo que permite el rol base.

Esta arquitectura se aplica a ambos tipos de usuarios:

- Service-managed usuarios: las políticas de sesión se pueden configurar directamente en la configuración del usuario
- Usuarios proveedores de identidad personalizados: las políticas de sesión pueden devolverse como parte de la respuesta de autenticación o almacenarse en AWS Secrets Manager

Dos enfoques para la administración de permisos

Al diseñar los permisos para los usuarios de Transfer Family que necesitan patrones de acceso únicos, puede elegir entre dos enfoques principales:

Un rol por usuario

Cree un rol de IAM independiente para cada usuario de Transfer Family con permisos específicos adaptados a las necesidades de ese usuario. Utilice este enfoque cuando:

- Cada usuario requiere permisos muy diferentes
- La administración de permisos está a cargo de diferentes personas de su organización
- Necesita un control detallado sobre el acceso de los usuarios individuales

Función compartida con políticas de sesión

Utilice un único rol de IAM con amplios permisos (como el acceso a un bucket completo de Amazon S3 que contenga varios directorios principales de usuarios) y aplique políticas de sesión para restringir a cada usuario a su área específica. Este enfoque reduce considerablemente la sobrecarga administrativa en comparación con la administración de funciones independientes para cada usuario. Utilice este enfoque cuando:

- Los usuarios necesitan tipos de acceso similares pero a recursos diferentes (por ejemplo, todos los usuarios necesitan read/write acceso, pero cada uno solo a su propia carpeta)
- Desea simplificar la administración de funciones y evitar la creación de docenas o cientos de funciones individuales
- Los usuarios solo deben acceder a sus directorios principales designados dentro de un depósito compartido
- La administración de permisos está centralizada en su organización

Por ejemplo, en lugar de crear roles separados para los usuarios «alice», «bob» y «charlie», puede crear un rol con acceso a todo el `s3://company-transfers/` grupo y, a continuación, usar las políticas de sesión para restringir a alice `s3://company-transfers/alice/s3://company-transfers/bob/`, bob to, etc.

Implementación de políticas de sesión

Las políticas de sesión funcionan restringiendo los permisos efectivos de la función de IAM básica asignada a un usuario. Los permisos finales son la intersección de los permisos del rol y los permisos de la política de sesión.

Puede implementar políticas de sesión dinámicas de dos maneras:

Substitución de variables

Utilice variables de política de Transfer Family como `${transfer:Username}`, `${transfer:HomeDirectory}`, y `${transfer:HomeBucket}` en las políticas de sesión. Estas variables se sustituyen automáticamente por los valores reales en tiempo de ejecución. Para obtener más información sobre estas variables, consulte [Creación de una política de sesión para un bucket de Amazon S3](#).

Generación dinámica

Para los proveedores de identidades personalizados, genere políticas de sesión sobre la marcha como parte de la respuesta de autenticación de su función Lambda o método API Gateway. Este enfoque le permite crear políticas altamente personalizadas basadas en los atributos de los usuarios, las pertenencias a grupos o las fuentes de datos externas en el momento de la autenticación.

También puede almacenar las políticas de sesión generadas previamente incluyendo una clave denominada Policy JSON como valor de la política de sesión. AWS Secrets Manager Esto le

permite utilizar la misma función general de IAM en varios usuarios y, al mismo tiempo, mantener los controles de acceso específicos de cada usuario.

Note

Las políticas de sesión solo se admiten para las transferencias de archivos desde y hacia Amazon S3. No se aplican a los sistemas de archivos Amazon EFS. En el caso de Amazon EFS, los permisos se rigen UID/GID y los bits de permiso se aplican dentro del propio sistema de archivos.

Implementación por tipo de usuario

Service-managed usuarios

Para los usuarios gestionados por el servicio, puede especificar las políticas de sesión directamente en la configuración del usuario a través de la AWS Transfer Family consola, la API o la CLI. Para obtener más información, consulte [Trabajar con usuarios de servicios administrados](#).

Proveedores de identidad personalizados

Para los usuarios de proveedores de identidades personalizados, puede proporcionar políticas de sesión de dos maneras:

- AWS Secrets Manager Mediante la inclusión de una clave nombrada Policy junto con la política de sesión como valor
- Directamente en la respuesta de la función Lambda o en la respuesta de API Gateway como parte del resultado de la autenticación

Para obtener más información, consulte [Solución de proveedor de identidad personalizada](#).

Ejemplo: simplificar la administración de funciones con políticas de sesión

Este ejemplo demuestra cómo la administración dinámica de permisos puede reducir significativamente la sobrecarga administrativa y, al mismo tiempo, mantener la seguridad.

Escenario

Su organización tiene 50 usuarios que necesitan acceso SFTP para transferir archivos. Cada usuario solo debe acceder a su propia carpeta dentro de un bucket compartido de Amazon S3

llamado `company-transfers`. Sin políticas de sesión, tendría que crear 50 funciones de IAM independientes.

Enfoque tradicional (sin políticas de sesión)

- Cree 50 funciones de IAM: `TransferRole-Alice`, `TransferRole-Bob`, `TransferRole-Charlie`, etc.
- Cada función tiene permisos específicos solo para la carpeta de ese usuario
- La administración de los permisos requiere actualizar los roles individuales
- Para añadir nuevos usuarios es necesario crear nuevos roles

Enfoque dinámico (con políticas de sesión)

- Cree 1 función de IAM: `TransferRole-Shared` con amplios permisos para todo el segmento
- Utilice las políticas de sesión para restringir a cada usuario a su carpeta específica durante el tiempo de ejecución
- La administración de los permisos requiere actualizar un rol o una plantilla de política de sesión
- La adición de nuevos usuarios no requiere nuevos roles, solo la configuración del usuario

Implementación

Así es como implementaría el enfoque dinámico (utilizando el `company-transfers` bucket como ejemplo para reemplazarlo por su bucket de Amazon S3 real):

Para implementar la administración dinámica de permisos

1. Cree un rol de IAM compartido con amplios permisos de Amazon S3:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/*"
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": "s3:ListBucket",
  "Resource": "arn:aws:s3:::company-transfers"
}
]
```

2. Cree una plantilla de política de sesión que restrinja el acceso a la carpeta del usuario:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/${transfer:Username}/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${transfer:Username}*"
        }
      }
    }
  ]
}
```

3. Configure cada usuario con:

- La función de IAM compartida
- La política de sesión se aplicó de la siguiente manera:
 - Service-managed usuarios: utilice la API o la CLI para aplicar el JSON mediante el parámetro Policy al crear o modificar usuarios (la consola solo ofrece opciones de políticas predefinidas)

- Usuarios de proveedores de identidad personalizados: devuélvalos como parte de la respuesta de la función Lambda durante la autenticación o guárdelos AWS Secrets Manager como una clave denominada «Política» junto con las credenciales del usuario
- Directorio principal: `/company-transfers/${transfer:Username}/`

AWS CloudTrail iniciar sesión para AWS Transfer Family

AWS Transfer Family se integra tanto con Amazon AWS CloudTrail como con Amazon CloudWatch. CloudTrail y CloudWatch sirven para propósitos diferentes pero complementarios.

- Este tema trata sobre la integración con CloudTrail un AWS servicio que crea un registro de las acciones realizadas en su interior Cuenta de AWS. Supervisa y registra continuamente las operaciones de la API para actividades como los inicios de sesión en la consola, AWS Command Line Interface los comandos y SDK/API las operaciones. Esto te permite llevar un registro de quién realizó qué acción, cuándo y desde dónde. CloudTrail contribuye a la auditoría, la gestión del acceso y el cumplimiento de las normas, ya que proporciona un historial de todas las actividades de su AWS entorno. Para obtener más información, consulte la [Guía AWS CloudTrail del usuario](#).
- [CloudWatch Registro de Amazon para AWS Transfer Family servidores](#) cubre la integración con CloudWatch un servicio de supervisión de AWS recursos y aplicaciones. Recopila métricas y registros para proporcionar visibilidad sobre la utilización de los recursos, el rendimiento de las aplicaciones y el estado general del sistema. CloudWatch ayuda con las tareas operativas, como la resolución de problemas, la configuración de alarmas y el escalado automático. Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que 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 operaciones de la API pública, por lo que no aparecen en ningún orden específico.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de tu cuenta AWS Transfer Family, crea un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera 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 los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar 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 AWS Transfer Family las acciones se registran CloudTrail y se documentan en [ActionsAPI reference](#). Por ejemplo, las llamadas a ListUsers y StopServer las acciones generan entradas en los archivos de CloudTrail registro. CreateServer

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 de AWS Identity and Access Management usuario o raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el [elemento userIdentity de CloudTrail](#).

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Transfer Family. 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 el destinatario de la solicitud AWS Transfer Family, la dirección IP desde la que 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](#).

Temas

- [Habilite el AWS CloudTrail registro](#)
- [Ejemplo de entrada de registro para crear un servidor](#)
- [Ejemplos de registros de acceso a datos](#)

Habilite el AWS CloudTrail registro

Puede supervisar las operaciones AWS Transfer Family de la API mediante AWS CloudTrail. Al supervisar las operaciones de la API, puede obtener información útil sobre seguridad y operaciones. Si tiene [activado el registro a nivel de objeto de Amazon S3](#), RoleSessionName aparecerá en el campo Requester (Solicitante) como [AWS:Role Unique Identifier]/username.sessionid@server-id. Para obtener más información sobre los identificadores únicos de rol AWS Identity and Access Management (IAM), consulte Identificadores [únicos en la Guía](#) del AWS Identity and Access Management usuario.

Important

La longitud máxima de RoleSessionName son 64 caracteres. Si el RoleSessionName es más largo, se trunca el server-id.

Habilitación de eventos de datos de Amazon S3

Para realizar un seguimiento de las operaciones de archivos realizadas AWS Transfer Family en sus buckets de Amazon S3, debe habilitar los eventos de datos para esos buckets. Los eventos de datos proporcionan actividad de API a nivel de objeto y son particularmente útiles para rastrear las cargas y descargas de archivos y otras operaciones realizadas por los usuarios. AWS Transfer Family

Para habilitar los eventos de datos de Amazon S3 en su AWS Transfer Family servidor:

1. Abra la CloudTrail consola en <https://console.aws.amazon.com/cloudtrail/>.
2. En el panel de navegación, elija Rutas y, a continuación, seleccione una ruta existente o cree una nueva.
3. En Eventos de datos, selecciona Editar.
4. Para el tipo de evento de datos, selecciona S3.
5. Elija los buckets de Amazon S3 para registrar los eventos de datos. Puede registrar los eventos de datos de todos los buckets o especificar buckets individuales.
6. Elija si desea registrar los eventos de lectura, los eventos de escritura o ambos.
7. Seleccione Save changes (Guardar cambios).

Tras habilitar los eventos de datos, puede acceder a estos registros en el bucket de Amazon S3 configurado para su CloudTrail ruta. Los registros incluyen detalles como el usuario que realizó la acción, la marca temporal de la acción, el objeto específico afectado y el `onBehalfOf` campo que ayuda a rastrear `userId` las acciones realizadas. AWS Transfer Family

Ejemplo de entrada de registro para crear un servidor

El siguiente ejemplo muestra una entrada de CloudTrail registro (en formato JSON) que muestra la `CreateServer` acción.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAA4FFF5HHHHH6NNWWW:user1",
    "arn": "arn:aws:sts::123456789102:assumed-role/Admin/user1",
    "accountId": "123456789102",
    "accessKeyId": "AAAA52C2WWWWW3BB4Z",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-12-18T20:03:57Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAAA4FFF5HHHHH6NNWWW",
        "arn": "arn:aws:iam::123456789102:role/Admin",
        "accountId": "123456789102",
        "userName": "Admin"
      }
    }
  },
  "eventTime": "2024-02-05T19:18:53Z",
  "eventSource": "transfer.amazonaws.com",
  "eventName": "CreateServer",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "11.22.1.2",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36",
  "requestParameters": {
    "domain": "S3",
    "hostKey": "HIDDEN_DUE_TO_SECURITY_REASONS",
```

```

    "protocols": [
      "SFTP"
    ],
    "protocolDetails": {
      "passiveIp": "AUTO",
      "tlsSessionResumptionMode": "ENFORCED",
      "setStatOption": "DEFAULT"
    },
    "securityPolicyName": "TransferSecurityPolicy-2020-06",
    "s3StorageOptions": {
      "directoryListingOptimization": "ENABLED"
    }
  },
  "responseElements": {
    "serverId": "s-1234abcd5678efghi"
  },
  "requestID": "6fe7e9b1-72fc-45b0-a7f9-5840268aeadf",
  "eventID": "4781364f-7c1e-464e-9598-52d06aa9e63a",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789102",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "transfer.us-east-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
}

```

Ejemplos de registros de acceso a datos

Cuando habilita los eventos de datos de Amazon S3 para su CloudTrail ruta, puede realizar un seguimiento de las operaciones de archivos realizadas a través de ellos AWS Transfer Family. Estos registros le ayudan a controlar quién accedió a qué datos, cuándo y cómo.

Ejemplo de entrada de registro para un acceso correcto a los datos

El siguiente ejemplo muestra una entrada de CloudTrail registro para una operación de descarga de archivos correcta AWS Transfer Family.

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:TransferSessionUser",
    "arn": "arn:aws:sts::123456789012:assumed-role/TransferS3AccessRole/TransferSessionUser",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/TransferS3AccessRole",
        "accountId": "123456789012",
        "userName": "TransferS3AccessRole"
      },
      "attributes": {
        "creationDate": "2025-07-15T16:12:05Z",
        "mfaAuthenticated": "true"
      }
    },
    "invokedBy": "transfer.amazonaws.com"
  },
  "eventTime": "2025-07-15T16:15:22Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "bucketName": "my-transfer-bucket",
    "key": "users/john.doe/reports/quarterly-report-2025-Q2.pdf",
    "Host": "my-transfer-bucket.s3.amazonaws.com",
    "x-amz-request-payer": "requester"
  },
  "responseElements": null,
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2458732,
  }
}

```

```

    "x-amz-id-2":
"EXAMPLE123456789+abcdefghijklmnopqrstuvxyzABCDEFGHIJKLMNOPQRSTUVWXYZ="
  },
  "requestID": "EXAMPLE123456789",
  "eventID": "example12-3456-7890-abcd-ef1234567890",
  "readOnly": true,
  "resources": [
    {
      "type": "AWS::S3::Object",
      "ARN": "arn:aws:s3:::my-transfer-bucket/users/john.doe/reports/quarterly-
report-2025-Q2.pdf"
    },
    {
      "accountId": "123456789012",
      "type": "AWS::S3::Bucket",
      "ARN": "arn:aws:s3:::my-transfer-bucket"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "123456789012",
  "eventCategory": "Data",
  "requestParameters": {
    "x-amz-onBehalfOf": "john.doe.sessionid@s-abcd1234efgh5678"
  }
}

```

En este ejemplo, anote los siguientes campos importantes:

- `eventName`: Indica la operación de API de S3 que se realizó (GetObject para la descarga de un archivo).
- `requestParameters.bucketName` y `requestParameters.key`: Muestra a qué objeto de S3 se accedió.
- `additionalEventData.bytesTransferredOut`: Muestra el tamaño del archivo descargado en bytes.
- `requestParameters.x-amz-onBehalfOf`: Contiene el AWS Transfer Family nombre de usuario y el ID de sesión, lo que le permite rastrear qué AWS Transfer Family usuario realizó la acción.

El `x-amz-onBehalfOf` campo es especialmente importante, ya que vincula la llamada a la API de S3 con el AWS Transfer Family usuario específico que inició la acción. Este campo sigue el formato `username.sessionid@server-id`, donde:

- `username` es el AWS Transfer Family nombre de usuario.
- `sessionid` es un identificador único de la sesión del usuario.
- `server-id` es el ID del AWS Transfer Family servidor.

Operaciones comunes de acceso a datos

Al supervisar el acceso a los datos AWS Transfer Family, normalmente verá las siguientes operaciones de la API de S3 en sus CloudTrail registros:

Operaciones de S3 comunes en AWS Transfer Family los registros

Funcionamiento de la API de S3	Acción de AWS Transfer Family	Description (Descripción)
GetObject	Descarga de archivos	El usuario ha descargado un archivo del servidor
PutObject	Cargar archivo	El usuario ha subido un archivo al servidor
DeleteObject	Eliminación de archivos	El usuario ha eliminado un archivo del servidor
ListObjects o ListObjects V2	Listado de directorios	Archivos listados por el usuario en un directorio
CopyObject	Copia de archivos	El usuario copió un archivo en el servidor

Al supervisar estas operaciones en sus CloudTrail registros, puede realizar un seguimiento de todas las actividades de los archivos que se realizan en el AWS Transfer Family servidor, lo que le ayuda a cumplir los requisitos de conformidad y a detectar el acceso no autorizado.

CloudWatch Registro de Amazon para AWS Transfer Family servidores

Amazon CloudWatch es un potente servicio de supervisión y observabilidad que proporciona una visibilidad completa de sus AWS recursos, incluidos AWS Transfer Family los siguientes:

- **Real-time supervisión:** CloudWatch supervisa los recursos y las aplicaciones de Transfer Family en tiempo real, lo que le permite realizar un seguimiento y analizar su rendimiento.
- **Recopilación de métricas:** CloudWatch recopila y rastrea varias métricas para sus recursos y aplicaciones, que son variables que puede medir y usar para el análisis.
- **CloudWatch página de inicio:** la página de CloudWatch inicio muestra automáticamente las métricas sobre Transfer Family y otros AWS servicios que utiliza, lo que proporciona una vista centralizada de sus datos de supervisión.
- **Paneles personalizados:** puede crear paneles personalizados CloudWatch para mostrar las métricas específicas de sus aplicaciones personalizadas y los recursos que elija monitorear.
- **Alarmas y notificaciones:** CloudWatch le permite crear alarmas que supervisen sus métricas y activar notificaciones o acciones automatizadas cuando se superen ciertos umbrales. Esto puede resultar útil para supervisar la actividad de transferencia de archivos en los servidores de Transfer Family y escalar los recursos en consecuencia.
- **Optimización de costos:** puede usar los datos recopilados por usted CloudWatch para identificar los recursos infrautilizados y tomar medidas, como detener o eliminar instancias, para optimizar sus costos.

En general, las capacidades integrales de monitoreo lo CloudWatch convierten en una herramienta valiosa para administrar y optimizar su infraestructura de Transfer Family y las aplicaciones que se ejecutan en ella.

Los detalles para CloudWatch iniciar sesión en las aplicaciones web de Transfer Family están disponibles en [CloudTrail registro para aplicaciones web Transfer Family](#).

Tipos de CloudWatch registro para Transfer Family

Transfer Family ofrece dos formas de registrar eventos en CloudWatch:

- Registro estructurado JSON

- Registro mediante una función de registro

Para los servidores Transfer Family, puede elegir el mecanismo de registro que prefiera. Para los conectores y los flujos de trabajo, solo se admiten las funciones de registro.

Registro estructurado en JSON

Para registrar los eventos del servidor, se recomienda utilizar el registro estructurado JSON. Esto proporciona un formato de registro más completo que permite la consulta de CloudWatch registros. Para este tipo de registro, la política de IAM del usuario que crea el servidor (o edita la configuración de registro del servidor) debe contener los siguientes permisos:

- `logs:CreateLogDelivery`
- `logs>DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

A continuación, se muestra una política de ejemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  }
]
}

```

Para obtener más información sobre la configuración del registro estructurado de JSON, consulte.

[Crear, actualizar y ver los registros de los servidores](#)

Función de registro

Para registrar los eventos de un flujo de trabajo gestionado que está conectado a un servidor, así como de los conectores, debe especificar un rol de registro. Para establecer el acceso, debe crear una política de IAM basada en recursos y un rol de IAM que proporcione la información de acceso. El siguiente es un ejemplo de política para una Cuenta de AWS que puede registrar eventos del servidor.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}

```

Para obtener más información sobre la configuración de una función de registro para registrar los eventos del flujo de trabajo, consulte [Administrar el registro de los flujos de trabajo](#).

Crear, actualizar y ver los registros de los servidores

Para todos los AWS Transfer Family servidores, ofrecemos un registro estructurado. Le recomendamos que utilice un registro estructurado para todos los servidores Transfer Family nuevos y existentes. Entre las ventajas del uso del registro estructurado se incluyen las siguientes:

- Recibir los registros en un formato JSON estructurado.
- Consulte sus registros con Amazon CloudWatch Logs Insights, que descubre automáticamente los campos con formato JSON.
- Compartir grupos de registros entre AWS Transfer Family recursos le permite combinar flujos de registros de varios servidores en un solo grupo de registros, lo que facilita la administración de las configuraciones de monitoreo y los ajustes de retención de registros.
- Cree métricas y visualizaciones agregadas que se puedan añadir a los CloudWatch paneles.
- Realizar un seguimiento de los datos de uso y rendimiento mediante grupos de registros para crear métricas de registro, visualizaciones y paneles consolidados.

Para habilitar el registro de los flujos de trabajo que están conectados a los servidores, debe usar una función de registro.

Note

Al agregar una función de registro, el grupo de registro siempre está `/aws/transfer/your-serverID` activo y no se puede cambiar. Esto significa que, a menos que envíe los registros estructurados del servidor al mismo grupo, iniciará sesión en dos grupos de registro distintos.

Si sabe que va a asociar un flujo de trabajo a su servidor y, por lo tanto, necesita añadir una función de registro, puede configurar el registro estructurado para que se registre en el grupo de registros predeterminado `/aws/transfer/your-serverID`.

Para modificar el grupo de registro, consulte [StructuredLogDestinations](#) la referencia de la AWS Transfer Family API.

Si crea un servidor mediante la consola de Transfer Family, el registro se habilita de forma predeterminada. Tras crear el servidor, puede utilizar la operación de `UpdateServer` API para cambiar la configuración de registro. Para obtener más información, consulte [StructuredLogDestinations](#).

Actualmente, para los flujos de trabajo, si desea habilitar el registro, debe especificar un rol de registro:

- Si asocia un flujo de trabajo a un servidor mediante la operación `CreateServer` o la `UpdateServer` API, el sistema no crea automáticamente una función de registro. Si desea registrar los eventos de su flujo de trabajo, debe adjuntar explícitamente un rol de registro al servidor.
- Si crea un servidor mediante la consola Transfer Family y adjunta un flujo de trabajo, los registros se envían a un grupo de registros que contiene el ID del servidor en el nombre. El formato es `/aws/transfer/server-id`, por ejemplo, `/aws/transfer/s-1111aaaa2222bbbb3`. Los registros del servidor se pueden enviar a este mismo grupo de registros o a uno diferente.

Consideraciones sobre el registro para crear y editar los servidores en la consola

- Los nuevos servidores creados a través de la consola solo admiten el registro JSON estructurado, a menos que haya un flujo de trabajo adjunto al servidor.
- Ningún registro no es una opción para los servidores nuevos que usted cree en la consola.
- Los servidores existentes pueden habilitar el registro JSON estructurado a través de la consola en cualquier momento.
- Al habilitar el registro JSON estructurado a través de la consola, se deshabilita el método de registro existente para que no se cobre dos veces a los clientes. La excepción es si existe un flujo de trabajo asociado con el servidor.
- Si habilita el registro JSON estructurado, no podrá deshabilitarlo posteriormente a través de la consola.
- Si habilita el registro JSON estructurado, puede cambiar el destino del grupo de registros a través de la consola en cualquier momento.
- Si habilita el registro JSON estructurado, no podrá editar el rol de registro a través de la consola si ha habilitado ambos tipos de registro a través de la API. La excepción es si existe su servidor tiene un flujo de trabajo adjunto. Sin embargo, el rol de registro sigue apareciendo en Detalles adicionales.

Consideraciones sobre el registro para crear y editar los servidores mediante API o SDK

- Si crea un servidor nuevo a través de la API, puede configurar uno o ambos tipos de registro, o elegir no realizar ningún registro.

- Para los servidores existentes, habilita o deshabilita el registro JSON estructurado en cualquier momento.
- Puede cambiar el grupo de registros mediante la API en cualquier momento.
- Puede cambiar el rol del registro mediante la API en cualquier momento.

Para habilitar el registro estructurado, debe iniciar sesión en una cuenta con los siguientes permisos

- logs:CreateLogDelivery
- logs>DeleteLogDelivery
- logs:DescribeLogGroups
- logs:DescribeResourcePolicies
- logs:GetLogDelivery
- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

En la sección encontrará un ejemplo de política [Configura el rol de CloudWatch registro](#).

Temas

- [Crear registros para servidores](#)
- [Actualización del registro de un servidor](#)
- [Vista de la configuración del servidor](#)

Crear registros para servidores

Al crear un servidor nuevo, en la página Configurar detalles adicionales, puede especificar un grupo de registros existente o crear uno nuevo.

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

Note Logging role is only required when selecting a workflow in the Managed workflows section below.

Si elige Crear grupo de registros, la CloudWatch consola (<https://console.aws.amazon.com/cloudwatch/>) se abre en la página Crear grupo de registros. Para obtener más información, consulte [Crear un grupo de CloudWatch registros en Logs](#).

Actualización del registro de un servidor

Los detalles del registro dependen del escenario de la actualización.

Note

Si opta por el registro JSON estructurado, es posible que, en raras ocasiones, se produzca un retraso donde Transfer Family deje de registrar en el formato anterior, pero demore cierto tiempo en empezar a registrar en el nuevo formato JSON. Esto puede provocar que los eventos no se registren. No se producirán interrupciones en el servicio, pero debe tener cuidado al transferir los archivos durante la primera hora después de cambiar el método de registro, ya que los registros podrían perderse.

Si está editando un servidor existente, las opciones dependerán del estado del servidor.

- El servidor ya tiene habilitado un rol de registro, pero no tiene activado el registro JSON estructurado.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/scooter ▼



Create log group [↗](#)

Enabling the structured JSON log format will override your existing logging configuration. Potential changes include new log format and log group.

Logging Role [Info](#)

Select an existing role from your account

AWSTransferLoggingAccess ▼



Workflows events will be delivered to a log group labelled with the server ID.

- El servidor no tiene activado ningún registro.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☐ Enable structured JSON logging

Choose an existing log group ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- El servidor ya tiene habilitado el registro JSON estructurado, pero no tiene un rol de registro especificado.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/ ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- El servidor ya tiene habilitado el registro JSON estructurado y tiene un rol de registro especificado.

Edit additional details

Logging [Info](#)

Log group [Info](#)
Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

▼

Logging Role [Info](#)
Select an existing role from your account

▼

 Workflows events will be delivered to a log group labelled with the server ID.

Vista de la configuración del servidor

Los detalles de la página de configuración del servidor dependen del escenario:

Según el escenario, la página de configuración del servidor puede tener un aspecto similar a uno de los siguientes ejemplos:

- No se ha habilitado ningún registro.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role -	Passive IP -

- El registro JSON estructurado está habilitado.

Additional details
Edit

Log group /aws/transfer/s[redacted]	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role -	Passive IP -

- El rol de registros está activado, pero el registro JSON estructurado no está activado.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-[redacted]	SetStat option Ignore
Server host key Info SHA256:lx39/[redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role [redacted]execution-role[redacted]	Passive IP -

- Ambos tipos de registro (rol de registro y registro JSON estructurado) están habilitados.

Additional details

Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows	Passive IP -

Administrar el registro de los flujos de trabajo

CloudWatch proporciona auditorías y registros consolidados del progreso y los resultados del flujo de trabajo. Además, AWS Transfer Family proporciona varias métricas para los flujos de trabajo. Puede ver las métricas de la cantidad de flujos de trabajo que se iniciaron, se completaron correctamente y se produjeron errores en el minuto anterior. Todas las CloudWatch métricas de Transfer Family se describen en [Uso de CloudWatch métricas para servidores Transfer Family](#).

Ver los CloudWatch registros de Amazon para flujos de trabajo

1. Abre la CloudWatch consola de Amazon en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación izquierdo, seleccione Registros y, a continuación, Grupos de registros.
3. En la página de grupos de registros, en la barra de navegación, elige la región correcta para tu AWS Transfer Family servidor.
4. Elija el grupo de registro que corresponda a su servidor.

Por ejemplo, si su ID del servidor es s-1234567890abcdef0, su grupo de registros es /aws/transfer/s-1234567890abcdef0.

5. En la página de detalles del grupo de registros de su servidor, se muestran los flujos de registro más recientes. Hay dos flujos de registro para el usuario que está explorando:
 - Uno para cada sesión del Protocolo de File Transfer (SFTP) de Secure Shell (SSH).

- Uno para el flujo de trabajo que se está ejecutando en el servidor. El formato del flujo de registro del flujo de trabajo es `username.workflowID.uniqueStreamSuffix`.

Por ejemplo, si su usuario es mary-major, tendrá los flujos de registro siguientes:

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

 Note

Los identificadores alfanuméricos de 16 dígitos que se muestran en este ejemplo son ficticios. Los valores que ves en Amazon CloudWatch son diferentes.

La página de Eventos de registro para mary-major-usa-east.1234567890abcdef0 muestra los detalles de cada sesión de usuario y el flujo de registro mary.w-abcdef01234567890.021345abcdef6789 contiene los detalles del flujo de trabajo.

El siguiente es un ejemplo de flujo de registro para mary.w-abcdef01234567890.021345abcdef6789, basado en un flujo de trabajo (w-abcdef01234567890) que contiene un paso de copiado.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
}
```

```

    }
  },
  {
    "type": "StepStarted",
    "details": {
      "input": {
        "fileLocation": {
          "backingStore": "S3",
          "bucket": "amzn-s3-demo-bucket",
          "key": "mary/workflowSteps2.json",
          "versionId": "version-id",
          "etag": "etag-id"
        }
      },
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "StepCompleted",
    "details": {
      "output": {},
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "ExecutionCompleted",
    "details": {},
    "workflowId": "w-abcdef01234567890",

```

```
{
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
}
```

Configura el rol de CloudWatch registro

Para establecer el acceso, debe crear una política de IAM basada en recursos y un rol de IAM que proporcione la información de acceso.

Para habilitar el CloudWatch registro de Amazon, comience por crear una política de IAM que permita el CloudWatch registro. A continuación, cree un rol de IAM y asócielo la política. Puede hacerlo cuando [crea un servidor](#) o [edita un servidor existente](#). Para obtener más información CloudWatch, consulta [¿Qué es Amazon CloudWatch?](#) y [¿Qué es Amazon CloudWatch Logs?](#) en la Guía del CloudWatch usuario de Amazon.

Utilice el siguiente ejemplo de políticas de IAM para permitir el CloudWatch registro.

Use a logging role

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

Use structured logging

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

En la política del ejemplo anterior **Resource**, sustituya *region-id* y por *Cuenta de AWS* sus valores. Por ejemplo, **"Resource": "arn:aws::logs:us-east-1:111122223333:log-group:/aws/transfer/*"**

A continuación, crea un rol y adjunta la política de CloudWatch registros que creó.

Para crear un rol de IAM y asociar una política

1. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.

En la página Crear rol, asegúrese de que servicio de AWS está seleccionado.

2. Elija Transfer (Transferencia) en la lista de servicios y, a continuación, elija Next: Permissions (Siguiendo: Permisos). Esto establece una relación de confianza entre el rol de IAM AWS Transfer Family y el mismo. Además, añada las claves de condición `aws:SourceAccount` y `aws:SourceArn` para protegerse del problema del suplente confuso. Para obtener más información, consulte la documentación siguiente:

- Procedimiento para establecer una relación de confianza con AWS Transfer Family: [Para establecer una relación de confianza](#)
 - Descripción del problema del suplente confuso: [el problema del suplente confuso](#)
3. En la sección Adjuntar políticas de permisos, busque y elija la política de CloudWatch registros que acaba de crear y elija Siguiente: etiquetas.
 4. (Opcional) Introduzca una clave y un valor de etiqueta y seleccione Siguiente: Revisión.
 5. En la página Review (Revisión), escriba un nombre y una descripción para el nuevo rol y, a continuación, elija Create role (Crear rol).
 6. Para ver los registros, seleccione la ID de servidor para abrir la página de configuración del servidor y seleccione Ver registros. Se le redirigirá a la CloudWatch consola, donde podrá ver sus flujos de registro.

En la CloudWatch página de su servidor, puede ver los registros de la autenticación de los usuarios (correcta y fallida), las cargas de datos (PUToperaciones) y las descargas de datos (GEToperaciones).

Visualización de las transmisiones de registros de Transfer Family

Visualización de los registros del servidor de Transfer Family

1. Navegue a la página de detalles de un servidor.
2. Seleccione Ver registros . Esto abre Amazon CloudWatch.
3. Se muestra el grupo de registros del servidor seleccionado.

CloudWatch ×

CloudWatch > Log groups > /aws/transfer/s-

/aws/transfer/s- Actions View in Logs Insights Search log group

Log group details

ARN arn:aws:logs:us-east-2:5:log-group:/aws/transfer/s-:*	Metric filters 0 Subscription filters 0 Contributor Insights rules -	Data protection - new Inactive Sensitive data found - new - KMS key ID -

Creation time
2 years ago

Retention
Never expire

Stored bytes
39.39 MB

Log streams Metric filters Subscription filters Contributor Insights Tags Data protection - new

Log streams (10) [Refresh] [Delete] [Create log stream] [Search all log streams]

Filter log streams or try prefix search ☐ Exact match ☐ Show expired [Info](#) < 1 > [Settings]

☐	Log stream	Last event
☐	ERRORS	2023-
☐	scooterstack4-	2023-
☐	scooterstack4-	2023-
☐	scooterstack4-	2023-
☐	scooterstack4-	2023-

4. Puede seleccionar un flujo de registro para mostrar los detalles y las entradas individuales del flujo.
 - Si hay una lista de ERRORES, puede seleccionarla para ver los detalles de los errores más recientes del servidor.

CloudWatch > Log groups > /aws/transfer/s- > ERRORS

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

↻

Actions ▾

Create metric filter

🔍 Filter events

Clear1m30m1h12hCustom

Display ▾

⚙️

▶	Timestamp	Message	
There are older events to load. Load more.			
▶	2023-03-23T16:08:29.281-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:30.979-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:32.647-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:34.306-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:36.010-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:08:37.659-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
▶	2023-03-23T16:12:33.307-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
▼	2023-03-23T16:12:34.943-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
		ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" SourceIP=	Copy
▼	2023-03-23T16:12:56.857-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
▼	2023-03-23T16:12:58.430-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
▶	2023-03-23T16:13:00.106-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	

- Seleccione cualquier otra entrada para ver un ejemplo de flujo de registro.

CloudWatch > Log groups > /aws/transfer/s- > scooterstack4.

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

↻

Actions ▾

Create metric filter

🔍 Filter events

Clear1m30m1h12hCustom

Display ▾

⚙️

▶	Timestamp	Message	
No older events at this moment. Retry			
▼	2023-03-23T16:19:43.747-04:00	scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- Client=SSH-2.0- OpenSSH_7.4 Role=arn:aws:iam:: :role/ Kex=	Copy
▼	2023-03-23T16:19:47.030-04:00	scooterstack4. DISCONNECTED scooterstack4. DISCONNECTED	Copy
No newer events at this moment. Auto retry paused. Resume			

Visualización de las transmisiones de registros de Transfer Family

604

- Si el servidor tiene asociado un flujo de trabajo administrado, puede ver los registros de las ejecuciones del flujo de trabajo.

Note

El formato del flujo de registro del flujo de trabajo es

username.workflowId.uniqueStreamSuffix. Por ejemplo, `decrypt-user.w-a1111222233334444.aaaa1111bbbb2222` podría ser el nombre de un flujo de registro para el usuario **decrypt-user** y el flujo de trabajo **w-a1111222233334444**.

CloudWatch > Log groups > /aws/transfer/s- > decrypt-user.w-

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions Create metric filter

Filter events Clear 1m 30m 1h 12h Custom Display

Timestamp	Message
	There are older events to load. Load more .
2023-03-21T13:37:57.795-04:00	<code>{"type": "StepStarted", "details": {"input": {"fileLocation": {"backingStore": "S3", "bucket": "", "key": "decrypt-...</code>
2023-03-21T14:12:02.850-04:00	<code>{"type": "StepStarted", "details": {"input": {"fileLocation": {"backingStore": "S3", "bucket": "", "key": "decrypt-... <pre> { "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "", "key": "decrypt-user/test.json.gpg", "versionId": "", "etag": "" } } }, "stepType": "DECRYPT", "stepName": "decrypt-step" }, "workflowId": "w-", "executionId": "", "transferDetails": { "serverId": "s-", "username": "decrypt-user", "sessionId": "" } } </pre> </code>
2023-03-21T14:12:03.464-04:00	<code>{"type": "StepCompleted", "details": {"output": {}}, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-</code>

Note

Para cualquier entrada de registro expandida, puede copiarla en el portapapeles seleccionando Copiar. Para obtener más información sobre CloudWatch los registros, consulte [Visualización de los datos de registro](#).

Creación de CloudWatch alarmas de Amazon

El siguiente ejemplo muestra cómo crear CloudWatch alarmas de Amazon con la AWS Transfer Family métrica,FilesIn.

CDK

```
new cloudwatch.Metric({
  namespace: "AWS/Transfer",
  metricName: "FilesIn",
  dimensionsMap: { ServerId: "s-000000000000000000" },
  statistic: "Average",
  period: cdk.Duration.minutes(1),
}).createAlarm(this, "AWS/Transfer FilesIn", {
  threshold: 1000,
  evaluationPeriods: 10,
  datapointsToAlarm: 5,
  comparisonOperator:
    cloudwatch.ComparisonOperator.GREATER_THAN_OR_EQUAL_TO_THRESHOLD,
});
```

CloudFormation

```
Type: AWS::CloudWatch::Alarm
Properties:
  Namespace: AWS/Transfer
  MetricName: FilesIn
  Dimensions:
    - Name: ServerId
      Value: s-000000000000000000
  Statistic: Average
  Period: 60
  Threshold: 1000
  EvaluationPeriods: 10
  DatapointsToAlarm: 5
  ComparisonOperator: GreaterThanOrEqualToThreshold
```

Registrar las operaciones de la API de Amazon S3 en los registros de acceso de S3

Note

Esta sección no se aplica a las aplicaciones web Transfer Family.

Si [utiliza los registros de acceso de Amazon S3 para identificar las solicitudes de S3](#) realizadas en nombre de sus usuarios de transferencia de archivos, RoleSessionName se utiliza para mostrar qué rol de IAM se asumió para atender las transferencias de archivos. También muestra información adicional, como el nombre de usuario, la identificación de sesión y la identificación del servidor utilizados para las transferencias. El formato es [AWS:Role Unique Identifier]/username.sessionid@server-id y está contenido en el campo Requester (Solicitante). Por ejemplo, el siguiente es el contenido de un ejemplo de campo Requester (Solicitante) de un registro de acceso de S3 para un archivo que se copió en el bucket de S3.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/  
username.sessionid@server-id
```

En el campo Requester (Solicitante) de arriba, se muestra el rol de IAM al que se llamó IamRoleName. Para obtener más información acerca del rol de los identificadores únicos de IAM, consulte [Identificadores únicos](#) en la Guía del usuario de AWS Identity and Access Management .

Ejemplos para limitar el problema del suplente confuso

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. Para obtener más información, consulte [Cross-service confusa prevención de diputados](#).

Note

En los siguientes ejemplos, sustituya cada uno por su *user input placeholder* propia información.

En estos ejemplos, puede eliminar los detalles del ARN de un flujo de trabajo si el servidor no tiene ningún flujo de trabajo adjunto.

El siguiente ejemplo logging/invoke de política permite que cualquier servidor (y flujo de trabajo) de la cuenta asuma la función.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

El siguiente ejemplo logging/invoke de política permite que un servidor (y un flujo de trabajo) específicos asuma la función.

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

```

```

    "Sid": "AllowSpecificServerWithWorkflowAttached",
    "Effect": "Allow",
    "Principal": {
      "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:transfer:us-west-2:111122223333:server/server-id",
          "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-
id"
        ]
      }
    }
  }
}

```

CloudWatch estructura de registro para Transfer Family

En este tema se describen los campos que se rellenan en los registros de Transfer Family: tanto para las entradas de registro estructuradas de JSON como para las entradas de registro heredadas.

Temas

- [Registros estructurados en JSON para Transfer Family](#)
- [Registros heredados de Transfer Family](#)

Registros estructurados en JSON para Transfer Family

La siguiente tabla contiene detalles de los campos de entrada de registro para SFTP/FTP/FTPS las acciones de Transfer Family, en el nuevo formato de registro estructurado JSON.

Campo	Description (Descripción)	Ejemplo de entrada
tipo de actividad	La acción del usuario	Los tipos de actividad disponibles son los siguientes: AUTH_FAILURE, CONNECTED, DISCONNECTED, ERROR, EXIT_REASON, CLOSE, CREATE_SYMLINK, DELETE, MKDIR, OPEN, PARTIAL,LOSE, RENAME, RMDIR, SETSTAT, TLS_FAILURE.
bytes de entrada	Número de bytes subidos por el usuario	29238420042
bytes de salida	Número de bytes descargados por el usuario	23094032490328
ciphers	Especifica el cifrado SSH negociado para la conexión (los cifrados disponibles aparecen en) Algoritmos criptográficos	aes256-gcm@openssh.com
cliente	El software cliente del usuario	SSH-2.0-OpenSSH_7.4
home-dir	El directorio en el que aterriza el usuario final cuando se conecta al punto final si su tipo de directorio principal es PATH: si tiene un directorio principal lógico, este valor siempre es /	/user-home- bucket/test
kex	Especifica el intercambio de claves SSH (KEX) negociado para la conexión (los KEX	diffie-hellman-group14-sha256

Campo	Description (Descripción)	Ejemplo de entrada
	disponibles aparecen en) Algoritmos criptográficos	
message	Proporciona más información relacionada con el error	<i><string></i>
method	El método de autenticación	publickey
mode	Especifica cómo un cliente abre un archivo	CREAR TRUNCAR ESCRIBIR
operación	La operación del cliente en un archivo	ABRIR CERRAR
path	Ruta real del archivo afectada	/amzn-s3-demo- -file-1.pdf bucket/test
ssh-public-key	El cuerpo de la clave pública del usuario que se está conectando	AAAAC3NzaC1lZDI1NT E5AAAAIA9OY0qV6XYV HaaOiWAcj2spDJVbgj rqDPY4pxd6GnHl

Campo	Description (Descripción)	Ejemplo de entrada
ssh-public-key-fingerprint	La huella digital de la clave pública, tal como se muestra en la consola para los usuarios gestionados por el servicio al enumerar sus claves de usuario.	SHA256:BY3gNMHwTfj d4n2VuT4pTyLOk82zW Zj4KEYEu7y4r/0
 Note En la consola, la huella digital se muestra con los caracteres de relleno (si los hay): de 0 a 3 signos iguales (=) al final. En la entrada del registro, este relleno se elimina de la salida.		
ssh-public-key-type	Tipo de clave pública: Transfer Family admite claves RSA, ECDSA y ED25519-formatted	ssh-ed25519
resource-arn	Un identificador único asignado por el sistema para un recurso específico (por ejemplo, un servidor)	arn:aws:transfer:ap-northeast-1:12346789012: -1234567890akeu2js2 server/s
rol	La función de IAM del usuario	arn:aws:iam: :0293883675: -role role/testuser
id-de-sesión	Un identificador único asignado por el sistema para una sola sesión	9ca9a0e1cec6ad9d

Campo	Description (Descripción)	Ejemplo de entrada
fuelle-ip	Direcciones IP de clientes	18.323.0.129
usuario	El nombre de usuario del usuario final	mi nombre 192
política de usuario	Los permisos especificados para el usuario final: este campo se rellena si la política del usuario es una política de sesión.	El código JSON de la política de sesión que se está utilizando

Registros heredados de Transfer Family

La siguiente tabla contiene detalles de las entradas de registro de varias acciones de Transfer Family.

Note

Estas entradas no están en el nuevo formato de registro estructurado JSON.

La siguiente tabla contiene detalles de las entradas de registro de varias acciones de Transfer Family, en el nuevo formato de registro estructurado JSON.

Action	Registros correspondientes en Amazon CloudWatch Logs
Errores de autenticación	ERRORES AUTH_FAILURE METHOD=PublicKey User=LHR message="RSA +b7 +a +HXG0C7L1JIZ0" sourceIP=3.8.172.211 SHA256:Lfz3R2nmLY4raK Rb1rSvUIbAE
COPY/TAG/DELETE/DECRYPT flujo de trabajo	{"type": "StepStarted", "details": {"fileLocation": {"BackingStore": "EFS", "fileSystemID": "fs-12345678", "path": "/lhr/regex.py"}}

Action	Registros correspondientes en Amazon CloudWatch Logs
	<pre> { "stepType": "TAG", "stepName": "successful_tag_step", "WorkflowID": "w-1111aaa-a2222bbbb3", "ExecutionID": "81234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverID": "s-1234abcd5678efghi", "username": "lhr", "ID de sesión": "1234567890abcdef0" } } </pre>
Flujo de trabajo con pasos personalizados	<pre> { "type": "CustomStepInvoked", "stepType": "CUSTOM", "stepName": "efs-s3_copy_2", "WorkflowID": "w-9283e49d33297c3f7", "MzM4Mjg5YWU0YjZjQyMzE5", "ExecutionID": "1234abcd-1234-efgh-5678-ijklm7nopqr90", "TransferDetails": { "ServerID": "s-zzzz1111aaaa22223", "username": "lhr", "sessionID": "1234567890abcdef0" } } </pre>
Eliminaciones	<pre> lhr.33a8fb495ffb383b ELIMINAR RUTA=/ bucket/user /123.jpg </pre>
Descargas	<pre> lhr.33a8fb495ffb383b OPEN Path=/ /123.jpg MODE=Leer bucket/user lhr.33a8fb495ffb383b CERRAR RUTA=/ /123.jpg =3618546 bucket/user BytesOut </pre>

Action	Registros correspondientes en Amazon CloudWatch Logs
Logins/Logouts	user.914984e553bcd6b6 FUENTE CONECTADA IP = 1.22.111.222 USUARIO=L HR =CLIENTE LÓGICO = _7.4 ROLE=ARN: aws: :iam: :123456789012: -s3-access HomeDir SSH-2.0-OpenSSH role/sftp user.914984e553bcd6b6 DISCONNECTED
Cambio de nombre	lhr.33a8fb495ffb383b CAMBIAR EL NOMBRE DE LA RUTA=/ /lambo.png =/ bucket/user / ferrari.png NewPath bucket/user
Ejemplo de registro de errores de flujo de trabajo	<pre>{ "type": "StepErrored", "details": { "ErrorType": "BAD_REQUEST", "ErrorMessage": "No se puede etiquetar el archivo Efs", "stepType": "TAG", "stepName": "successful_tag_step", "WorkflowID": "w-1234abcd5678efghi", "ExecutionID": "81234abcdcd5678efghi", "ExecutionID": "81234abcdcd-1234-efgh-5678-ijklmnopqr90", "TransferDetails": { "ServerID": "s-1234abcd5678efghi", "username": "lhr", "ID de sesión": "1234567890abcdef0" } } }</pre>
Symlinks	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK LinkPath =/fs- 12345678/lhr /pqr.jpg TargetPath =abc.jpg
Subidas	lhr.33a8fb495ffb383b OPEN Path=/ /123.jpg mode=Crear Truncar Escribir bucket/user lhr.33a8fb495ffb383b CERRAR RUTA=/ /123.jpg =3618546 bucket/user BytesIn

Action	Registros correspondientes en Amazon CloudWatch Logs
Flujos de trabajo	<pre>{ "type": "ExecutionStarted", "details": { "input": { "initial": { "backingStore": "EFS", "fileSystemId": "fs-12345678", "fileLocation": { "path": "/lhr/regex.py" }, "WorkflowID": "w-1111aa2222bbbb3", "ExecutionID": "1234abcd-1234-efgh-gh-5678-ijklmno", "TransferDetails": { "ServerID": "s-1111aaaa22223", "username": "lhr", "ID de sesión": "1234567890abcdef0" } } } } }</pre> <pre>{ "type": "StepStarted", "details": { "fileLocation": { "BackingStore": "EFS", "fileSystemId": "fs-12345678", "path": "/lhr/regex.py" }, "stepType": "CUSTOM", "stepName": "efs-s3_copy_2", "WorkflowID": "w-9283e49d33297c3f7", "ExecutionID": "1234abcd-1234-efgh-5678-ijklmnopqr90", "TransferDetails": { "ServerID": "s-18ca49dce5d842e0b", "username": "lhr", "ID de sesión": "12345678ab9090b cdef0" } } }</pre>

Ejemplo de entradas de CloudWatch registro

En este tema se presentan ejemplos de entradas de registro.

Temas

- [Ejemplos de entradas de registro de sesiones de transferencia](#)
- [Ejemplos de entradas de registro para conectores SFTP](#)
- [Ejemplos de entradas de registro para conectores de celosía de VPC](#)
- [Ejemplos de entradas de registro para errores en el algoritmo de intercambio de claves](#)

Ejemplos de entradas de registro de sesiones de transferencia

En este ejemplo, un usuario de SFTP se conecta a un servidor Transfer Family, carga un archivo y, a continuación, se desconecta de la sesión.

La siguiente entrada de registro refleja a un usuario de SFTP que se conecta a un servidor Transfer Family.

```
{
  "role": "arn:aws:iam::500655546075:role/transfer-s3",
  "activity-type": "CONNECTED",
  "ciphers": "chacha20-poly1305@openssh.com,chacha20-poly1305@openssh.com",
  "client": "SSH-2.0-OpenSSH_7.4",
  "source-ip": "52.94.133.133",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "home-dir": "/test/log-me",
  "ssh-public-key":
"AAAAC3NzaC1lZDI1NTE5AAAAIA90Y0qV6XYVHaa0iWAcj2spDJVbgjrQDPY4pxd6GnH1",
  "ssh-public-key-fingerprint": "SHA256:BY3gNMHwTfjd4n2VuT4pTyL0k82zWZj4KEYEu7y4r/0",
  "ssh-public-key-type": "ssh-ed25519",
  "user": "log-me",
  "kex": "ecdh-sha2-nistp256",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

La siguiente entrada de registro refleja al usuario de SFTP que carga un archivo en su bucket de Amazon S3.

```
{
  "mode": "CREATE|TRUNCATE|WRITE",
  "path": "/test/log-me/config-file",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

Las siguientes entradas de registro reflejan la desconexión del usuario de SFTP de su sesión de SFTP. En primer lugar, el cliente cierra la conexión al bucket y, a continuación, desconecta la sesión de SFTP.

```
{
  "path": "/test/log-me/config-file",
  "activity-type": "CLOSE",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "bytes-in": "121",
  "session-id": "9ca9a0e1cec6ad9d"
}

{
  "activity-type": "DISCONNECTED",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

 Note

Los tipos de actividad disponibles son los siguientes: AUTH_FAILURE, CONNECTED,, DISCONNECTED, ERROR, EXIT_REASON, CLOSE, CREATE_SYML, RENAMERMDIR, SETSTAT. TLS_RESUME_FAILURE

Ejemplos de entradas de registro para conectores SFTP

Esta sección contiene registros de ejemplo de una transferencia correcta y otra fallida. Los registros se generan en un grupo de registros denominado `/aws/transfer/connector-id`, donde *connector-id* se encuentra el identificador del conector SFTP. Las entradas de registro para los conectores SFTP se generan al ejecutar un comando `StartFileTransfer` o `StartDirectoryListing`.

Esta entrada de registro corresponde a una transferencia que se completó correctamente.

```
{
  "operation": "RETRIEVE",
  "timestamp": "2023-10-25T16:33:27.373720Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://192.0.2.0",
  "file-path": "/remotebucket/remotefilepath",
}
```

```

    "status-code": "COMPLETED",
    "start-time": "2023-10-25T16:33:26.945481Z",
    "end-time": "2023-10-25T16:33:27.159823Z",
    "account-id": "480351544584",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "local-directory-path": "/connectors-localbucket",
    "bytes": 514,
    "egress-type": "SERVICE_MANAGED"
  }

```

Esta entrada de registro corresponde a una transferencia cuyo tiempo de espera se agotó y, por lo tanto, no se completó correctamente.

```

{
  "operation": "RETRIEVE",
  "timestamp": "2023-10-25T22:33:47.625703Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://192.0.2.0",
  "file-path": "/remotebucket/remotefilepath",
  "status-code": "FAILED",
  "failure-code": "TIMEOUT_ERROR",
  "failure-message": "Transfer request timeout.",
  "account-id": "480351544584",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
  "local-directory-path": "/connectors-localbucket",
  "egress-type": "SERVICE_MANAGED"
}

```

Esta entrada de registro corresponde a una operación de ENVÍO que se realiza correctamente.

```

{
  "operation": "SEND",
  "timestamp": "2024-04-24T18:16:12.513207284Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/amzn-s3-demo-bucket/my-test-folder/connector-metrics-us-east-1-2024-01-02.csv",
  "status-code": "COMPLETED",
  "start-time": "2024-04-24T18:16:12.295235884Z",

```

```

    "end-time": "2024-04-24T18:16:12.461840732Z",
    "account-id": "255443218509",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "bytes": 275,
    "egress-type": "SERVICE_MANAGED"
  }

```

Descripciones de algunos campos clave de los ejemplos de registro anteriores.

- `timestamp` representa cuándo se agrega el registro CloudWatch. `start-time` y `end-time` corresponden al momento en que el conector realmente inicia y finaliza una transferencia.
- `transfer-id` es un identificador único que se asigna a cada `start-file-transfer` solicitud. Si el usuario pasa varias rutas de archivo en una sola operación de `start-file-transfer` API, todos los archivos comparten la misma ruta `transfer-id`.
- `file-transfer-id` es un valor único generado para cada archivo transferido. Tenga en cuenta que la parte inicial de `file-transfer-id` es la misma que `transfer-id`.

Ejemplos de entradas de registro para conectores de celosía de VPC

Esta sección contiene registros de ejemplo para conectores de celosía de VPC. En el caso de los conectores VPC Lattice, los registros incluyen campos adicionales que proporcionan información sobre la configuración del conector y la configuración de la red.

Esta entrada de registro corresponde a una operación SEND del conector de celosía de VPC que se completó correctamente.

```

{
  "operation": "SEND",
  "timestamp": "2025-09-05T14:20:19.577192454Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "file-path": ""/amzn-s3-demo-bucket/my-test-folder/connector-vpc-lattice-us-east-1-2025-03-22.csv"",
  "status-code": "COMPLETED",
  "start-time": "2025-09-05T14:20:19.434072509Z",
  "end-time": "2025-09-05T14:20:19.481453346Z",
  "account-id": "account-id",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
  "remote-directory-path": "/test-bucket/test-folder/",

```



```

"bytes": 262,
"egress-type": "VPC_LATTICE",
"vpc-lattice-resource-configuration-arn": "arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/resource-configuration-arn-id,
"vpc-lattice-port-number": 22
}

```

Los registros de conectores VPC Lattice incluyen los siguientes campos adicionales:

- `egress-type`- Tipo de configuración de salida del conector
- `vpc-lattice-resource-configuration-arn`- ARN de la configuración de recursos de celosía de la VPC que define la ubicación del servidor SFTP de destino
- `vpc-lattice-port-number`- Número de puerto para conectarse al servidor SFTP a través de VPC Lattice

Ejemplos de entradas de registro para errores en el algoritmo de intercambio de claves

Esta sección contiene registros de ejemplo en los que se produjo un error en el algoritmo de intercambio de claves (KEX). Estos son ejemplos del flujo de registros ERRORS para registros estructurados.

Esta entrada de registro es un ejemplo de error en el tipo de clave de host.

```

{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-999999999999999999",
  "message": "no matching host key type found",
  "kex": "ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519,ssh-rsa,ssh-dss"
}

```

Esta entrada de registro es un ejemplo en el que hay una discrepancia de KEX.

```

{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",

```

```

    "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-999999999999999999",
    "message": "no matching key exchange method found",
    "kex": "diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group14-sha256"
}

```

Uso de CloudWatch métricas para servidores Transfer Family

Note

También puede obtener las métricas de Transfer Family desde la propia consola de Transfer Family. Para obtener más información, consulte [Monitoreo del uso en la consola](#)

Puede obtener información sobre su servidor mediante CloudWatch métricas. Una métrica representa un conjunto de puntos de datos ordenados por tiempo que se publican en CloudWatch. Al utilizar métricas, debe especificar el espacio de nombres, el nombre de la métrica y la [dimensión](#) de Transfer Family. Para obtener más información sobre las métricas, consulta [Métricas](#) en la Guía del CloudWatch usuario de Amazon.

En la siguiente tabla se describen las CloudWatch métricas de Transfer Family.

Namespace	Métrica	Description (Descripción)
AWS/Transfer	BytesIn	El número total de bytes transferidos al servidor. Criterios de informes: • Para SFTP/FTP/FTPS: se emite cada 5 minutos mientras se establece una conexión con el servidor Transfer Family. Si no se transfiere ningún archivo o byte durante el período, se emite un «0». • Para AS2: cuando el cliente recibe un mensaje en su servidor AS2 y lo emite tan pronto como el mensaje entrante termina de procesarse Unidades: recuento

Namespace	Métrica	Description (Descripción)
		Periodo: 5 minutos
	BytesOut	El número total de bytes transferidos desde el servidor. Criterios de información: • Para SFTP/FTP/FTPS: se emite cada 5 minutos mientras se establece una conexión con el servidor Transfer Family. Si no se transfiere ningún archivo o byte durante el período, se emite un «0». • Para AS2: cuando el cliente llama <code>StartFile Transfer</code> desde su conector AS2 y se emite tan pronto como el mensaje saliente termina de procesarse. Unidades: recuento Periodo: 5 minutos

Namespace	Métrica	Description (Descripción)
	FilesIn	El número total de archivos transferidos al servidor. Para los servidores que utilizan el protocolo AS2, esta métrica representa la cantidad de mensajes recibidos. Criterios de información: • Para SFTP/FTP/FTPS: se emite cada 5 minutos mientras se establece una conexión con el servidor Transfer Family. Si no se transfiere ningún archivo o byte durante el período, se emite un «0». • Para AS2: cuando el cliente recibe un mensaje en su servidor AS2 y lo emite tan pronto como el mensaje entrante termina de procesarse. Unidades: recuento Periodo: 5 minutos
	FilesOut	El número total de archivos transferidos desde el servidor. Criterios de información: • Para SFTP/FTP/FTPS: se emite cada 5 minutos mientras se establece una conexión con el servidor Transfer Family. Si no se transfiere ningún archivo o byte durante el período, se emite un «0». • Para AS2: cuando el cliente llama <code>StartFile Transfer</code> desde su conector AS2 y se emite tan pronto como el mensaje saliente termina de procesarse. Unidades: recuento Periodo: 5 minutos

Namespace	Métrica	Description (Descripción)
	InboundMessage	El número total de mensajes AS2 recibidos correctamente de un socio comercial. Criterios de notificación: cuando el cliente recibe un mensaje en su servidor AS2 y lo emite tan pronto como el mensaje entrante termina de procesarse correctamente Unidades: recuento Periodo: 5 minutos
	InboundFailedMessage	El número total de mensajes AS2 que se recibieron sin éxito de un socio comercial. Es decir, un socio comercial envió un mensaje, pero el servidor de Transfer Family no pudo procesarlo correctamente. Criterios de notificación: cuando el cliente recibe un mensaje en su servidor AS2 y lo emite tan pronto como el mensaje entrante termina de procesarse sin éxito Unidades: recuento Periodo: 5 minutos
	OnUploadExecutionsStarted	La cantidad total de ejecuciones de flujos de trabajo iniciadas en el servidor. Criterios de notificación: se activa cada vez que se inicia una ejecución Unidades: recuento Periodo: 1 minuto

Namespace	Métrica	Description (Descripción)
	OnUploadExecutionsSuccess	La cantidad total de ejecuciones satisfactorias del flujo de trabajo en el servidor. Criterios de informe: se activa cada vez que una ejecución finaliza correctamente Unidades: recuento Periodo: 1 minuto
	OnUploadExecutionsFailed	La cantidad total de ejecuciones de flujos de trabajo fallidas en el servidor. Criterios de informe: se activa cada vez que una ejecución no finaliza correctamente Unidades: recuento Periodo: 1 minuto
	OutboundMessage	El número total de mensajes AS2 enviados correctamente a un socio comercial. Criterios de notificación: cuando el cliente llama <code>StartFileTransfer</code> desde su conector AS2 y se emite tan pronto como el mensaje saliente termina de procesarse correctamente Unidades: recuento Periodo: 5 minutos

Namespace	Métrica	Description (Descripción)
	OutboundFailedMessage	El número total de mensajes AS2 que se enviaron sin éxito a un socio comercial. Criterios de notificación: cuando el cliente llama <code>StartFileTransfer</code> desde su conector AS2 y se emite tan pronto como el mensaje saliente termina de procesarse sin éxito Unidades: recuento Periodo: 5 minutos

Dimensiones de Transfer Family

Una dimensión es un name/value par que forma parte de la identidad de una métrica. Para obtener más información sobre las dimensiones, consulta [Dimensiones](#) en la Guía del CloudWatch usuario de Amazon.

En la siguiente tabla se describen las CloudWatch dimensiones de Transfer Family.

Dimensión	Description (Descripción)
ServerId	El ID exclusivo del usuario.
ConnectorId	El identificador único del conector. Se utiliza para AS2, para y OutboundMessage OutboundFailedMessage

Utilizándolo con AWS User Notifications AWS Transfer Family

Para recibir notificaciones sobre AWS Transfer Family eventos, puedes [AWS User Notifications](#) configurar varios canales de entrega. Recibirá una notificación cuando un evento coincida con una regla que especifique.

Puede recibir notificaciones de eventos a través de varios canales, como correo electrónico, notificaciones por chat de [Amazon Q Developer en aplicaciones de chat](#) o notificaciones push

de [AWS Console Mobile Application](#). También puedes ver las notificaciones en el [Centro de notificaciones de la consola](#). Notificaciones de usuario admite la agregación, lo que puede reducir la cantidad de notificaciones que recibe durante eventos específicos.

Para obtener más información, consulta la entrada de blog sobre cómo [personalizar las notificaciones de entrega de archivos mediante flujos de trabajo AWS Transfer Family gestionados](#) y [¿Qué es AWS User Notifications?](#) en la Guía AWS User Notifications del usuario.

Uso de consultas para filtrar las entradas de registro

Puede usar CloudWatch consultas para filtrar e identificar las entradas de registro de Transfer Family. En esta sección se incluyen algunos ejemplos.

1. Inicie sesión en Consola de administración de AWS y abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. Puede crear consultas o reglas.
 - Para crear una consulta de Logs Insights, selecciona Logs Insights en el panel de navegación izquierdo y, a continuación, introduce los detalles de la consulta.
 - Para crear una regla de Contributor Insights, selecciona Insights > Contributor Insights en el panel de navegación izquierdo y, a continuación, introduce los detalles de la regla.
3. Ejecuta la consulta o la regla que creaste.

Vea los principales factores que contribuyen a los errores de autenticación

En sus registros estructurados, una entrada del registro de errores de autenticación tiene un aspecto similar al siguiente:

```
{
  "method": "password",
  "activity-type": "AUTH_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "message": "Invalid user name or password",
  "user": "exampleUser"
}
```

Ejecuta la siguiente consulta para ver los principales factores que contribuyen a los errores de autenticación.


```
filter @logStream = 'ERRORS'
| filter `activity-type` = 'AUTH_FAILURE'
| stats count() as AuthFailures by user, method
| sort by AuthFailures desc
| limit 10
```

En lugar de utilizar CloudWatch Logs Insights, puede crear una regla de CloudWatch Contributors Insights para ver los errores de autenticación. Cree una regla similar a la siguiente.

```
{
  "AggregateOn": "Count",
  "Contribution": {
    "Filters": [
      {
        "Match": "$.activity-type",
        "In": [
          "AUTH_FAILURE"
        ]
      }
    ],
    "Keys": [
      "$.user"
    ]
  },
  "LogFormat": "JSON",
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "LogGroupARNs": [
    "arn:aws:logs:us-east-1:999999999999:log-group:/customer/structured_logs"
  ]
}
```

Vea las entradas de registro en las que se abrió un archivo

En los registros estructurados, una entrada del registro de lectura de archivos tiene un aspecto similar al siguiente:

```
{
  "mode": "READ",
  "path": "/fs-0df669c89d9bf7f45/avtester/example",
```

```
"activity-type":"OPEN",  
"resource-arn":"arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",  
"session-id":"0049cd844c7536c06a89"  
}
```

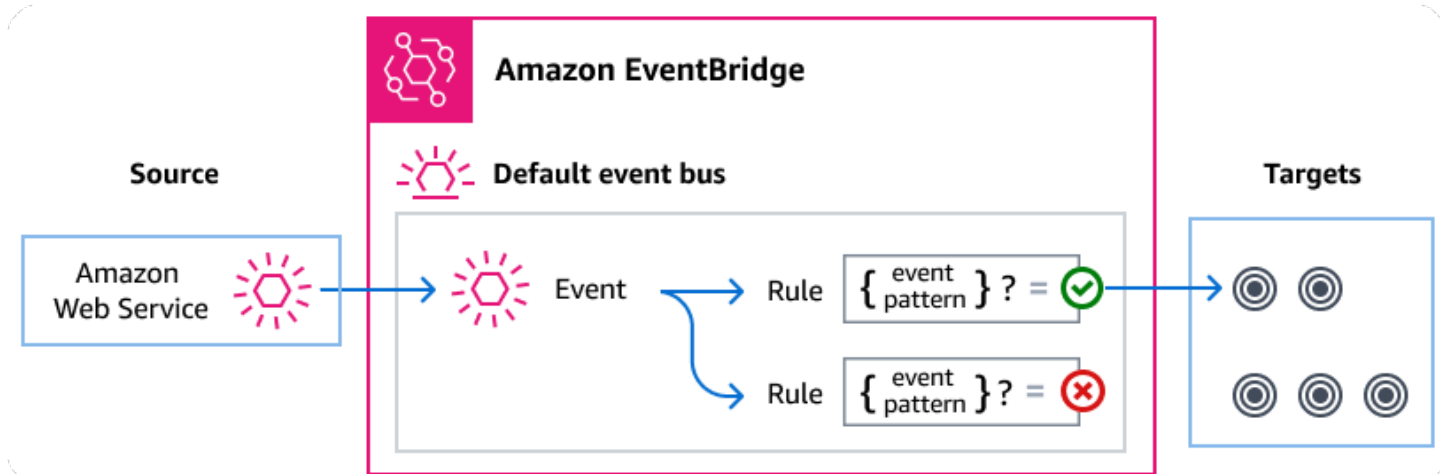
Ejecuta la siguiente consulta para ver las entradas de registro que indican que se ha abierto un archivo.

```
filter `activity-type` = 'OPEN'  
| display @timestamp, @logStream, `session-id`, mode, path
```

Administración Transfer Family eventos que utilizan Amazon EventBridge

Amazon EventBridge es un servicio sin servidor que utiliza eventos para conectar los componentes de la aplicación, lo que puede facilitar la creación de aplicaciones escalables basadas en eventos. Event-driven la arquitectura es un estilo de creación de sistemas de software poco acoplados que funcionan juntos emitiendo eventos y respondiendo a ellos. Los eventos representan un cambio en un recurso o entorno.

Como ocurre con muchos AWS servicios, Transfer Family genera y envía eventos al bus de eventos EventBridge predeterminado. Tenga en cuenta que el bus de eventos predeterminado se aprovisiona automáticamente en todas las AWS cuentas. Un bus de eventos es un enrutador que recibe eventos y los envía a cero o más destinos u objetivos. Usted especifica reglas para el bus de eventos que evalúa los eventos a medida que llegan. Cada regla comprueba si un evento coincide con el patrón de evento de la regla. Si el evento coincide, el bus de eventos envía el evento a uno o más destinos específicos.



Temas

- [Transfer Family eventos](#)
- [Enviando Transfer Family eventos mediante el uso EventBridge reglas](#)
- [Amazon EventBridge permisos](#)
- [Adicional EventBridge recursos](#)
- [Transfer Family referencia detallada de los eventos](#)

Transfer Family eventos

Transfer Family envía automáticamente los eventos al bus de EventBridge eventos predeterminado. Puede crear reglas en el bus de eventos, donde cada regla incluya un patrón de eventos y uno o más objetivos.

Los eventos que coinciden con el patrón de eventos de una regla se envían a los objetivos especificados, ya sea haciendo el mejor esfuerzo posible o de forma duradera (tenga en cuenta que algunos eventos pueden entregarse fuera de orden). Estos niveles de entrega se describen en el apartado [Nivel de entrega para eventos de AWS servicio](#) de la Amazon EventBridge Events Reference.

- Server-level los eventos para servidores SFTP, FTPS y FTP se entregan de la mejor manera posible.
- Los eventos del conector SFTP se entregan de forma duradera.
- Los eventos AS2 se entregan de forma duradera.

Los siguientes eventos son generados por Transfer Family. Para obtener más información, consulte [Eventos de EventBridge](#) en la Guía del usuario de Amazon EventBridge .

Eventos de servidor SFTP, FTPS y FTP

En las tablas siguientes se enumeran los eventos de los servidores SFTP, FTPS y FTP, organizados por tipo de evento.

Eventos de carga y descarga de archivos

Tipo de detalle del evento	Description (Descripción)
Se completó la descarga del archivo del servidor FTP	Se ha descargado correctamente un archivo para el protocolo FTP.
Falló la descarga del archivo del servidor FTP	Se produjo un error al intentar descargar un archivo para el protocolo FTP.
Se completó la carga del archivo del servidor FTP	Se ha cargado correctamente un archivo para el protocolo FTP.

Tipo de detalle del evento	Description (Descripción)
<u>No se pudo cargar el archivo del servidor FTP</u>	Se produjo un error al intentar cargar un archivo para el protocolo FTP.
<u>Se completó la descarga del archivo del servidor FTPS</u>	Se ha descargado correctamente un archivo para el protocolo FTPS.
<u>No se pudo descargar el archivo del servidor FTPS</u>	Se produjo un error al intentar descargar un archivo para el protocolo FTPS.
<u>Se completó la carga del archivo del servidor FTPS</u>	Se ha cargado correctamente un archivo para el protocolo FTPS.
<u>No se pudo cargar el archivo del servidor FTPS</u>	Se produjo un error al intentar cargar un archivo para el protocolo FTPS.
<u>Se completó la descarga del archivo del servidor SFTP</u>	Se ha descargado correctamente un archivo para el protocolo SFTP.
<u>Falló la descarga del archivo del servidor SFTP</u>	Se produjo un error al intentar descargar un archivo para el protocolo SFTP.
<u>Se completó la carga del archivo del servidor SFTP</u>	Se ha cargado correctamente un archivo para el protocolo SFTP.
<u>No se pudo cargar el archivo del servidor SFTP</u>	Se produjo un error al intentar cargar un archivo para el protocolo SFTP.

Otros eventos de operaciones de archivos

Tipo de detalle del evento	Description (Descripción)
<u>Se completó la creación del directorio del servidor FTP</u>	Se ha creado correctamente un directorio para el protocolo FTP.
<u>No se pudo crear el directorio del servidor FTP</u>	No se pudo crear un directorio para el protocolo FTP.

Tipo de detalle del evento	Description (Descripción)
Se completó la eliminación del directorio del servidor FTP	Se ha eliminado correctamente un directorio del protocolo FTP.
No se pudo eliminar el directorio del servidor FTP	No se pudo eliminar un directorio para el protocolo FTP.
Se completó la eliminación del archivo del servidor FTP	Se ha eliminado correctamente un archivo del protocolo FTP.
No se pudo eliminar el archivo del servidor FTP	Se produjo un error al intentar eliminar un archivo para el protocolo FTP.
Se ha completado el cambio de nombre del archivo del servidor FTP	Se ha cambiado correctamente el nombre de un archivo para el protocolo FTP.
Error al cambiar el nombre del archivo del servidor FTP	No se pudo cambiar el nombre de un archivo para el protocolo FTP.
Se completó la creación del directorio del servidor FTPS	Se ha creado correctamente un directorio para el protocolo FTPS.
No se pudo crear el directorio del servidor FTPS	No se pudo crear un directorio para el protocolo FTPS.
Se completó la eliminación del directorio del servidor FTPS	Se ha eliminado correctamente un directorio del protocolo FTPS.
No se pudo eliminar el directorio del servidor FTPS	No se pudo eliminar un directorio para el protocolo FTPS.
Se completó la eliminación del archivo del servidor FTPS	Se ha eliminado correctamente un archivo del protocolo FTPS.
No se pudo eliminar el archivo del servidor FTPS	Se produjo un error al intentar eliminar un archivo para el protocolo FTPS.

Tipo de detalle del evento	Description (Descripción)
<u>Se ha completado el cambio de nombre del archivo del servidor FTPS</u>	Se ha cambiado correctamente el nombre de un archivo para el protocolo FTPS.
<u>Error al cambiar el nombre del archivo del servidor FTPS</u>	No se pudo cambiar el nombre de un archivo para el protocolo FTPS.
<u>Se completó la creación del directorio del servidor SFTP</u>	Se ha creado correctamente un directorio para el protocolo SFTP.
<u>No se pudo crear el directorio del servidor SFTP</u>	No se pudo crear un directorio para el protocolo SFTP.
<u>Se completó la eliminación del directorio del servidor SFTP</u>	Se ha eliminado correctamente un directorio del protocolo SFTP.
<u>Falló la eliminación del directorio del servidor SFTP</u>	No se pudo eliminar un directorio para el protocolo SFTP.
<u>Se completó la eliminación del archivo del servidor SFTP</u>	Se ha eliminado correctamente un archivo del protocolo SFTP.
<u>No se pudo eliminar el archivo del servidor SFTP</u>	Se produjo un error al intentar eliminar un archivo para el protocolo SFTP.
<u>Se ha completado el cambio de nombre del archivo del servidor SFTP</u>	Se ha cambiado correctamente el nombre de un archivo para el protocolo SFTP.
<u>Error al cambiar el nombre del archivo del servidor SFTP</u>	No se pudo cambiar el nombre de un archivo para el protocolo SFTP.

Eventos del conector SFTP

Note

Estos eventos se entregan a un EventBridge nivel duradero, como se describe en [Nivel de entrega para eventos de AWS servicio](#) en la Referencia de EventBridge eventos de Amazon.

Tipo de detalle del evento	Description (Descripción)
Se ha completado el envío del archivo del conector SFTP	La transferencia de archivos desde un conector a un servidor SFTP remoto se ha completado correctamente.
Falló el envío del archivo del conector SFTP	Falló la transferencia de un archivo desde un conector a un servidor SFTP remoto.
Se completó la recuperación del archivo del conector SFTP	La transferencia de archivos desde un servidor SFTP remoto a un conector se ha completado correctamente.
Falló la recuperación del archivo del conector SFTP	Falló la transferencia de un archivo desde un servidor SFTP remoto a un conector.
Se completó la lista del directorio de conectores SFTP	Una llamada a la lista del directorio de archivos de inicio que se completó correctamente.
Error en la lista del directorio de conectores SFTP	Error en la lista del directorio de archivos de inicio.
Se completó el traslado remoto del conector SFTP	Los archivos o directorios se movieron o se les cambió el nombre correctamente en el servidor remoto.
Falló el movimiento remoto del conector SFTP	No se pudo mover o cambiar el nombre de los archivos o directorios en el servidor remoto.
Se completó la eliminación remota del conector SFTP	Los archivos o directorios se eliminaron correctamente en el servidor remoto.
Falló la eliminación remota del conector SFTP	No se pudieron eliminar los archivos o directorios del servidor remoto.

Eventos AS2

Note

Estos eventos se entregan a un EventBridge nivel duradero, como se describe en [Nivel de entrega para eventos de AWS servicio](#) en la Referencia de EventBridge eventos de Amazon.

Tipo de detalle del evento	Description (Descripción)
Se completó la recepción de carga útil de AS2	Se ha recibido la carga útil de un mensaje AS2.
Falló la recepción de la carga útil del AS2	No se ha recibido la carga útil de un mensaje AS2.
Se ha completado el envío de la carga útil AS2	La carga útil de un mensaje AS2 se envió correctamente.
Falló el envío de la carga útil AS2	No se pudo enviar la carga útil de un mensaje AS2.
Se completó la recepción de AS2 MDN	Se ha recibido la notificación de disposición de un mensaje AS2.
Falló la recepción de MDN de AS2	No se ha recibido la notificación de disposición de un mensaje AS2.
Se ha completado el envío de AS2 MDN	La notificación de disposición de un mensaje AS2 se envió correctamente.
Falló el envío de MDN de AS2	No se pudo enviar la notificación de disposición de un mensaje AS2.

Enviando Transfer Family eventos mediante el uso EventBridge reglas

Si desea que el bus de eventos EventBridge predeterminado envíe Transfer Family eventos a un destino, debe crear una regla que contenga un patrón de eventos que coincida con los datos de los Transfer Family eventos que desee.

Para capturar AWS Transfer Family eventos en Amazon EventBridge

1. Inicia sesión en la EventBridge consola de Amazon Consola de administración de AWS y ábrela en <https://console.aws.amazon.com/events/>.
2. En el panel de navegación, selecciona Reglas y, a continuación, selecciona Crear regla.
3. Introduzca un nombre descriptivo para la regla y, si lo desea, introduzca una descripción.
4. En Tipo de regla, seleccione Regla con un patrón de eventos y, a continuación, elija Siguiente.
5. En la sección Origen del evento, selecciona AWS eventos o eventos EventBridge asociados.
6. En la sección Método de creación, selecciona Usar formulario de patrón.
7. En la sección Patrón de eventos, proporciona la siguiente información.
 - a. En Origen de evento, seleccione Servicios de AWS .
 - b. Para el AWS servicio, selecciona Transferir.
 - c. En Tipo de evento, elige el tipo de evento de Transfer Family que quieres que active tu regla.

Según el tipo de evento que selecciones, es posible que se te presente una sección con la Especificación del tipo de evento 1.
 - d. Si ve la sección Especificación del tipo de evento 1, seleccione los eventos específicos que desee capturar (o seleccione Cualquier evento para capturar todos los eventos del tipo de evento que haya seleccionado).
 - e. (Opcional) Usa el editor de patrones de eventos para especificar filtros para los detalles del evento.
 - f. Elija Siguiente.
8. Elija un objetivo de las opciones disponibles en Seleccionar objetivos. Elige entre los siguientes objetivos disponibles.

- AWS servicio. Las opciones más populares son las funciones de Lambda para la computación sin servidor, las colas de Amazon SQS para el procesamiento de mensajes, los temas de Amazon SNS para las notificaciones y para organizar los flujos de trabajo. AWS Step Functions
- EventBridge Destino de la API. Si quieres enviar eventos a un punto final HTTP externo AWS, puedes usar un destino de API como objetivo.
- EventBridge bus de eventos. Puede enviar eventos a otro bus de eventos, ya sea en la misma cuenta y región o en una cuenta o región diferente.

Para obtener instrucciones detalladas sobre cómo crear reglas de bus de eventos, consulta [Cómo crear reglas que reaccionen a los eventos](#) en la Guía del EventBridge usuario de Amazon.

Si necesitas ayuda para seleccionar un objetivo, consulta la sección [Seleccionar objetivos](#) en la Guía del EventBridge usuario de Amazon.

9. Configura cualquier opción adicional para tu objetivo y, a continuación, selecciona Siguiente.
10. (Opcional) Añade etiquetas a la regla y selecciona Siguiente.
11. En la pantalla Revisar y crear, si todo va bien, selecciona Crear regla.

Crear patrones de eventos para Transfer Family eventos

Cuando Transfer Family entrega un evento al bus de eventos predeterminado, EventBridge utiliza el patrón de eventos definido para cada regla para determinar si el evento debe enviarse a los destinos de la regla. Un patrón de eventos coincide con los datos de los eventos de Transfer Family deseados. Cada patrón de eventos es un objeto JSON que contiene lo siguiente:

- Un atributo `source` que identifica el servicio que envía el evento. En el Transfer Family caso de los eventos, la fuente es `aws.transfer`.
- (Opcional) Un `detail-type` atributo que contiene una matriz de los tipos de eventos que deben coincidir.
- (Opcional) Un `detail` atributo que contiene cualquier otro dato de evento que pueda compararse.

Por ejemplo, el siguiente patrón de eventos coincide con todos los eventos de Transfer Family:

```
{
  "source": ["aws.transfer"]
}
```

El siguiente ejemplo de patrón de eventos coincide con todos los eventos del conector SFTP:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Connector File Send Completed", "SFTP Connector File Retrieve Completed",
                  "SFTP Connector File Retrieve Failed", "SFTP Connector File Send Failed"]
}
```

El siguiente ejemplo de patrón de eventos coincide con todos los eventos fallidos de Transfer Family:

```
{
  "source": ["aws.transfer"],
  "detail-type": [{"wildcard", "*Failed"}]
}
```

El siguiente ejemplo de patrón de eventos coincide con las descargas de SFTP realizadas correctamente por el usuario *username*:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Server File Download Completed"],
  "detail": {
    "username": [username]
  }
}
```

Para obtener más información sobre la escritura de los patrones de eventos, consulte [Patrones de eventos](#) en la Guía del usuario de EventBridge .

Probando patrones de eventos para Transfer Family eventos en EventBridge

Puede usar el EventBridge Sandbox para definir y probar rápidamente un patrón de eventos, sin tener que completar el proceso más amplio de crear o editar una regla. Con el Sandbox, puede

definir un patrón de eventos y usar un evento de muestra para confirmar que el patrón coincide con los eventos deseados. EventBridge le da la opción de crear una nueva regla mediante el uso de ese patrón de eventos directamente desde el entorno limitado.

Para obtener más información, consulte [Probar un patrón de eventos mediante el EventBridge entorno aislado](#) en la Guía del EventBridge usuario.

Amazon EventBridge permisos

Transfer Family no requiere ningún permiso adicional para enviar eventos a Amazon EventBridge.

Es posible que los destinos que especifique requieran permisos o una configuración específicos. Para obtener más información sobre el uso de servicios específicos para los destinos, consulte [Destinos de Amazon EventBridge](#) en la Guía del usuario de Amazon EventBridge .

Adicional EventBridge recursos

Consulte los siguientes temas de la [Guía del Amazon EventBridge usuario](#) para obtener más información sobre EventBridge cómo procesar y administrar eventos.

- Para obtener información detallada sobre cómo funcionan los buses de eventos, consulte [bus de eventos de Amazon EventBridge](#).
- Para obtener información sobre la estructura de los eventos, consulte [Eventos](#).
- Para obtener información sobre cómo crear patrones de eventos EventBridge para usarlos cuando se comparan eventos con reglas, consulte [Patrones de eventos](#).
- Para obtener información sobre la creación de reglas para especificar qué eventos procesa EventBridge , consulte [Reglas](#).
- Para obtener información sobre cómo especificar los servicios u otros destinos a los que se EventBridge envían los eventos coincidentes, consulte [Targets](#).

Transfer Family referencia detallada de los eventos

Todos los eventos de AWS los servicios tienen un conjunto común de campos que contienen metadatos sobre el evento. Estos metadatos pueden incluir el AWS servicio que es el origen del evento, la hora en que se generó el evento, la cuenta y la región en las que tuvo lugar el evento, entre otros. Para ver las definiciones de estos campos generales, consulte [Referencia de estructura de eventos](#) en la Guía del usuario de Amazon EventBridge .

Además, cada evento tiene un campo `detail` que contiene datos específicos de ese evento en particular. La siguiente referencia define los campos de detalle de los distintos Transfer Family eventos.

Cuando utilice EventBridge para seleccionar y gestionar Transfer Family eventos, tenga en cuenta lo siguiente:

- El `source` campo para todos los eventos de Transfer Family está establecido en `aws.transfer`.
- El campo `detail-type` especifica el tipo de evento.

Por ejemplo, `FTP Server File Download Completed`.

- El campo `detail` contiene los datos específicos de ese evento en particular.

Para obtener más información sobre cómo construir patrones de eventos que permitan que las reglas coincidan con los eventos de Transfer Family, consulte [Patrones de eventos](#) en la Guía del usuario de Amazon EventBridge.

Para obtener más información sobre los eventos y cómo EventBridge los procesa, consulte [Amazon EventBridge los eventos](#) en la Guía del Amazon EventBridge usuario.

Temas

- [Eventos de servidores SFTP, FTPS y FTP](#)
- [Eventos del conector SFTP](#)
- [Eventos AS2](#)

Eventos de servidores SFTP, FTPS y FTP

Los siguientes son los campos detallados de los eventos de los servidores SFTP, FTPS y FTP:

- Se completó la creación del directorio del servidor FTP
- No se pudo crear el directorio del servidor FTP
- Se completó la eliminación del directorio del servidor FTP
- Falló la eliminación del directorio del servidor FTP
- Se completó la eliminación del archivo del servidor FTP
- No se pudo eliminar el archivo del servidor FTP
- Se completó la descarga del archivo del servidor FTP

- Falló la descarga del archivo del servidor FTP
- Se ha completado el cambio de nombre del archivo del servidor FTP
- Falló el cambio de nombre del archivo del servidor FTP
- Se completó la carga del archivo del servidor FTP
- Falló la carga del archivo del servidor FTP
- Se completó la creación del directorio del servidor FTPS
- No se pudo crear el directorio del servidor FTPS
- Se completó la eliminación del directorio del servidor FTPS
- Falló la eliminación del directorio del servidor FTPS
- Se completó la eliminación del archivo del servidor FTPS
- No se pudo eliminar el archivo del servidor FTPS
- Se completó la descarga del archivo del servidor FTPS
- Falló la descarga del archivo del servidor FTPS
- Se ha completado el cambio de nombre del archivo del servidor FTPS
- Error al cambiar el nombre del archivo del servidor FTPS
- Se completó la carga del archivo del servidor FTPS
- Error al cargar el archivo del servidor FTPS
- Se completó la creación del directorio del servidor SFTP
- No se pudo crear el directorio del servidor SFTP
- Se completó la eliminación del directorio del servidor SFTP
- Falló la eliminación del directorio del servidor SFTP
- Se completó la eliminación del archivo del servidor SFTP
- Falló la eliminación del archivo del servidor SFTP
- Se completó la descarga del archivo del servidor SFTP
- Falló la descarga del archivo del servidor SFTP
- Se completó el cambio de nombre del archivo del servidor SFTP
- Error al cambiar el nombre del archivo del servidor SFTP
- Se completó la carga del archivo del servidor SFTP
- Falló la carga del archivo del servidor SFTP

Los detail-type campos source y se incluyen a continuación porque contienen valores específicos para los Transfer Family eventos. Para ver las definiciones de los demás campos de metadatos que se incluyen en todos los eventos, consulte la [referencia a la estructura de eventos](#) en la Guía del Amazon EventBridge usuario.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "failure-code" : "string",
    "status-code" : "string",
    "protocol" : "string",
    "bytes" : "number",
    "client-ip" : "string",
    "failure-message" : "string",
    "end-timestamp" : "string",
    "etag" : "string",
    "file-path" : "string",
    "original-file-path" : "string",
    "renamed-file-path" : "string",
    "directory-path" : "string",
    "server-id" : "string",
    "username" : "string",
    "session-id" : "string",
    "start-timestamp" : "string"
  }
}
```

detail-type

Identifica el tipo de evento.

Para este evento, el valor es uno de los nombres de eventos del servidor SFTP, FTPS o FTP enumerados anteriormente.

source

Identifica el servicio que generó el evento. Para los eventos de Transfer Family, este valor es `aws.transfer`.

detail

Un objeto JSON que contiene información sobre el evento. El servicio que genera el evento determina el contenido de este campo.

Para este evento, los datos incluyen lo siguiente:

failure-code

Categoría por la que se produjo un error en la transferencia. Valores: PARTIAL_UPLOAD | PARTIAL_DOWNLOAD | UNKNOWN_ERROR

status-code

Si la transferencia se ha realizado correctamente. Valores: COMPLETED | FAILED.

protocol

El protocolo utilizado para la transferencia. Valores: SFTP | FTPS | FTP

bytes

Número de bytes transferidos.

client-ip

La dirección IP del cliente implicado en la transferencia

failure-message

En el caso de las transferencias fallidas, los detalles del motivo del error en la transferencia.

end-timestamp

Para que las transferencias se realicen correctamente, la marca de tiempo en la que se termina de procesar el archivo.

etag

La etiqueta de entidad (solo se usa para los archivos de Amazon S3).

file-path

La ruta al archivo que se está transfiriendo, eliminando o utilizando de alguna otra forma.

original-file-path

En el caso de eventos de cambio de nombre de archivos, la ruta original del archivo antes de cambiarle el nombre.

renamed-file-path

En el caso de los eventos de cambio de nombre de archivos, la nueva ruta del archivo tras el cambio de nombre.

directory-path

En el caso de los eventos de creación y eliminación de directorios, la ruta del directorio.

server-id

El identificador único del servidor Transfer Family.

username

El usuario que realiza la transferencia.

session-id

El identificador único de la sesión de transferencia.

start-timestamp

Para que las transferencias se realicen correctamente, la marca de tiempo en la que comienza el procesamiento de los archivos.

Example Ejemplo de evento fallido al descargar un archivo del servidor SFTP

El siguiente ejemplo muestra un evento en el que se produjo un error de descarga en un servidor SFTP (si Amazon EFS se está utilizando el almacenamiento).

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Download Failed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2024-01-29T17:20:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "failure-code": "PARTIAL_DOWNLOAD",
    "status-code": "FAILED",
```

```

    "protocol": "SFTP",
    "bytes": 4100,
    "client-ip": "IP-address",
    "failure-message": "File was partially downloaded.",
    "end-timestamp": "2024-01-29T17:20:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2024-01-29T17:20:16.706282454Z"
  }
}

```

Example Ejemplo de evento: se completó la carga de un archivo en un servidor FTP

El siguiente ejemplo muestra un evento en el que una carga se completó correctamente en un servidor FTP (Amazon S3 si se está utilizando el almacenamiento).

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "FTP Server File Upload Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2024-01-29T16:31:43Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1111aaaa2222bbbb3"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "FTP",
    "bytes": 1048576,
    "client-ip": "10.0.0.141",
    "end-timestamp": "2024-01-29T16:31:43.311866408Z",
    "etag": "b6d81b360a5672d80c27430f39153e2c",
    "file-path": "/amzn-s3-demo-bucket/test/1mb_file",
    "server-id": "s-1111aaaa2222bbbb3",
    "username": "test",
    "session-id": "event-ID",
    "start-timestamp": "2024-01-29T16:31:42.462088327Z"
  }
}

```

Example Ejemplo de evento: se completó la eliminación de archivos del servidor SFTP

El siguiente ejemplo muestra un evento en el que un archivo se eliminó correctamente en un servidor SFTP.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Delete Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T14:30:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T14:30:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file-to-delete.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T14:30:26.706282454Z"
  }
}
```

Example Ejemplo de cambio de nombre de archivo del servidor SFTP completado

El siguiente ejemplo muestra un evento en el que se cambió correctamente el nombre de un archivo en un servidor SFTP.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Rename Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T15:45:12Z",
  "region": "us-east-1",
  "resources": [
```

```

    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T15:45:12.749749117Z",
    "original-file-path": "/fs-1234abcd5678efghi/user0/old-filename.txt",
    "renamed-file-path": "/fs-1234abcd5678efghi/user0/new-filename.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T15:45:11.706282454Z"
  }
}

```

Example Ejemplo de evento de creación completa del directorio del servidor SFTP

El siguiente ejemplo muestra un evento en el que se creó correctamente un directorio en un servidor SFTP.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server Directory Create Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T16:20:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T16:20:05.749749117Z",
    "directory-path": "/fs-1234abcd5678efghi/user0/new-directory",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T16:20:04.706282454Z"
  }
}

```

```
}
```

Eventos del conector SFTP

Note

Estos eventos se entregan a un EventBridge nivel duradero, como se describe en [Nivel de entrega para eventos de AWS servicio](#) en la Referencia de EventBridge eventos de Amazon.

Los siguientes son los campos detallados de los eventos del conector SFTP:

- Se ha completado el envío del archivo del conector SFTP
- Falló el envío del archivo del conector SFTP
- Se completó la recuperación del archivo del conector SFTP
- Falló la recuperación del archivo del conector SFTP
- Se completó el listado del directorio de conectores SFTP
- Falló la lista del directorio de conectores SFTP
- Se completó el movimiento remoto del conector SFTP
- Falló el movimiento remoto del conector SFTP
- Se completó la eliminación remota del conector SFTP
- Falló la eliminación remota del conector SFTP

Los detail-type campos source y se incluyen a continuación porque contienen valores específicos para los Transfer Family eventos. Para ver las definiciones de los demás campos de metadatos que se incluyen en todos los eventos, consulte la [referencia a la estructura de eventos](#) en la Guía del Amazon EventBridge usuario.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "operation" : "string",
    "max-items" : "number",
```

```

    "connector-id" : "string",
    "output-directory-path" : "string",
    "listing-id" : "string",
    "transfer-id" : "string",
    "file-transfer-id" : "string",
    "url" : "string",
    "file-path" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "local-directory-path" : "string",
    "remote-directory-path" : "string",
    "item-count" : "number",
    "truncated" : "boolean",
    "bytes" : "number",
    "egress-type" : "string",
    "vpc-lattice-resource-configuration-arn" : "string",
    "vpc-lattice-port-number" : "number",
    "local-file-location" : {
        "domain" : "string",
        "bucket" : "string",
        "key" : "string"
    },
    "output-file-location" : {
        "domain" : "string",
        "bucket" : "string",
        "key" : "string"
    }
}

```

detail-type

Identifica el tipo de evento.

Para este evento, el valor es uno de los nombres de eventos del conector SFTP enumerados anteriormente.

source

Identifica el servicio que generó el evento. Para Transfer Family los eventos, este valor es `aws.transfer`.

detail

Un objeto JSON que contiene información sobre el evento. El servicio que genera el evento determina el contenido de este campo.

Para este evento, los datos incluyen lo siguiente:

`max-items`

El número máximo de directory/file nombres que se van a devolver.

`operation`

Si la `StartFileTransfer` solicitud envía o recupera un archivo. Valores: `SEND` | `RETRIEVE`.

`connector-id`

El identificador único del conector SFTP que se está utilizando.

`output-directory-path`

La ruta (bucket y prefijo) en Amazon S3 para almacenar los resultados del file/directory listado.

`listing-id`

Un identificador único para la operación de la `StartDirectoryListing` API. Este identificador se puede utilizar para comprobar CloudWatch los registros y ver el estado de la solicitud de listado.

`transfer-id`

El identificador único del evento de transferencia (una `StartFileTransfer` solicitud).

`file-transfer-id`

El identificador único del archivo que se está transfiriendo.

`url`

La URL del punto de conexión de AS2 o SFTP del socio.

`file-path`

La ubicación y el archivo que se están enviando o recuperando.

`status-code`

Si la transferencia se ha realizado correctamente. Valores: `FAILED` | `COMPLETED`.

failure-code

En el caso de transferencias fallidas, el código del motivo por el que se produjo el error en la transferencia. Valores:ASSUME_ROLE_ERROR | UNSUPPORTED_OPERATION_ERROR | CONNECTION_ERROR | READ_FILE_ERROR | WRITE_FILE_ERROR | TIMEOUT_ERROR | LIST_DIRECTORY_ERROR | SEND_FILE_NOT_FOUND | RETRIEVE_FILE_NOT_FOUND | DIRECTORY_NOT_FOUND | FILE_NOT_FOUND | PATH_NOT_FOUND | RENAME_ERROR | DELETE_ERROR | INTERNAL_ERROR | UNKNOWN_ERROR.

failure-message

En el caso de transferencias fallidas, los detalles del motivo por el que se produjo el error en la transferencia.

start-timestamp

Para que las transferencias se realicen correctamente, la marca de tiempo en la que se inicia el procesamiento del archivo.

end-timestamp

Para que las transferencias se realicen correctamente, la marca de tiempo en la que se completa el procesamiento del archivo.

local-directory-path

En el caso de RETRIEVE las solicitudes, la ubicación en la que se debe colocar el archivo recuperado.

remote-directory-path

En el caso de SEND las solicitudes, el directorio de archivos en el que se va a colocar el archivo en el servidor SFTP del socio. Es el valor RemoteDirectoryPath que el usuario ha transferido a la StartFileTransfer solicitud. Puede especificar un directorio predeterminado en el servidor SFTP del socio. Si es así, este campo está vacío.

item-count

El número de elementos (directorios y archivos) devueltos para la solicitud de listado.

truncated

Si el resultado de la lista contiene todos los elementos contenidos en el directorio remoto o no.

bytes

El número de bytes que se están transfiriendo. El valor es 0 para las transferencias fallidas.

`egress-type`

Tipo de configuración de salida del conector. Valores: `SERVICE_MANAGED` o `VPC_LATTICE`

`vpc-lattice-resource-configuration-arn`

ARN de la configuración de recursos `VPC_LATTICE` que define la ubicación del servidor SFTP de destino. Este campo es nulo para los conectores gestionados por el servicio.

`vpc-lattice-port-number`

Número de puerto para conectarse al servidor SFTP a través de `VPC_LATTICE`.

`local-file-location`

Este parámetro contiene los detalles de la ubicación del archivo de almacenamiento. `AWS domain`

El almacenamiento que se está utilizando. Actualmente, el único valor es `S3`.

`bucket`

El contenedor del objeto en Amazon S3.

`key`

El nombre asignado al objeto en Amazon S3.

`output-file-location`

Este parámetro contiene los detalles de la ubicación en la que se almacenarán los resultados de la lista de AWS directorios.

`domain`

El almacenamiento que se está utilizando. Actualmente, el único valor es `S3`.

`bucket`

El contenedor del objeto en Amazon S3.

`key`

El nombre asignado al objeto en Amazon S3.

Example Ejemplo de evento fallido al enviar el archivo del conector SFTP

El siguiente ejemplo muestra un evento en el que un conector SFTP falló al intentar enviar un archivo a un servidor SFTP remoto.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector File Send Failed",
  "source": "aws.transfer",
  "account": "123456789012",
  "time": "2024-01-24T19:30:45Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
  ],
  "detail": {
    "operation": "SEND",
    "connector-id": "c-f1111aaaa2222bbbb3",
    "transfer-id": "transfer-ID",
    "file-transfer-id": "file-transfer-ID",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/amzn-s3-demo-bucket/testfile.txt",
    "status-code": "FAILED",
    "failure-code": "CONNECTION_ERROR",
    "failure-message": "Unknown Host",
    "remote-directory-path": "",
    "bytes": 0,
    "start-timestamp": "2024-01-24T18:29:33.658729Z",
    "end-timestamp": "2024-01-24T18:29:33.993196Z",
    "local-file-location": {
      "domain": "S3",
      "bucket": "amzn-s3-demo-bucket",
      "key": "testfile.txt"
    }
  }
}
```

Example Ejemplo de evento SFTP Connector File Retrieve Completed

El siguiente ejemplo muestra un evento en el que un conector SFTP recuperó correctamente un archivo enviado desde un servidor SFTP remoto.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector File Retrieve Completed",
  "source": "aws.transfer",
```

```

"account": "123456789012",
"time": "2024-01-24T18:28:08Z",
"region": "us-east-1",
"resources": [
    "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
],
"detail": {
    "operation": "RETRIEVE",
    "connector-id": "c-fc68000012345aa18",
    "transfer-id": "file-transfer-ID",
    "file-transfer-id": "file-transfer-ID",
    "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
    "file-path": "testfile.txt",
    "status-code": "COMPLETED",
    "local-directory-path": "/amzn-s3-demo-bucket",
    "bytes": 63533,
    "start-timestamp": "2024-01-24T18:28:07.632388Z",
    "end-timestamp": "2024-01-24T18:28:07.774898Z",
    "local-file-location": {
        "domain": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "testfile.txt"
    }
}
}

```

Example Ejemplo de listado de directorios de conectores SFTP completado

El siguiente ejemplo muestra un evento en el que una llamada a iniciar un listado del directorio recuperó un archivo de listado de un servidor SFTP remoto.

```

{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Connector Directory Listing Completed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T18:28:08Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {

```

```
"max-items": 10000,
"connector-id": "c-fc68000012345aa18",
"output-directory-path": "/amzn-s3-demo-bucket/example/file-listing-output",
"listing-id": "123456-23aa-7980-abc1-1a2b3c4d5e",
"url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",

"status-code": "COMPLETED",
"remote-directory-path": "/home",
"item-count": 10000,
"truncated": true,
"start-timestamp": "2024-01-24T18:28:07.632388Z",
"end-timestamp": "2024-01-24T18:28:07.774898Z",
"output-file-location": {
  "domain": "S3",
  "bucket": "amzn-s3-demo-bucket",
  "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
}
}
```

Eventos AS2

Note

Estos eventos se entregan a un EventBridge nivel duradero, como se describe en [Nivel de entrega para eventos de AWS servicio](#) en la Referencia de EventBridge eventos de Amazon.

Los siguientes son los campos de detalle de los eventos de AS2:

- Se completó la recepción de carga útil del AS2
- Falló la recepción de la carga útil del AS2
- Se completó el envío de la carga útil AS2
- Falló el envío de la carga útil del AS2
- Se completó la recepción de AS2 MDN
- Falló la recepción de AS2 MDN
- Se completó el envío de AS2 MDN
- Falló el envío de AS2 MDN

Los detail-type campos source y se incluyen a continuación porque contienen valores específicos para Transfer Family los eventos. Para ver las definiciones de los demás campos de metadatos que se incluyen en todos los eventos, consulte la [referencia a la estructura de eventos](#) en la Guía del Amazon EventBridge usuario.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "s3-attributes" : {
      "file-bucket" : "string",
      "file-key" : "string",
      "json-bucket" : "string",
      "json-key" : "string",
      "mdn-bucket" : "string",
      "mdn-key" : "string"
    }
    "mdn-subject" : "string",
    "mdn-message-id" : "string",
    "disposition" : "string",
    "bytes" : "number",
    "as2-from" : "string",
    "as2-message-id" : "string",
    "as2-to" : "string",
    "connector-id" : "string",
    "client-ip" : "string",
    "agreement-id" : "string",
    "server-id" : "string",
    "requester-file-name" : "string",
    "message-subject" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "transfer-id" : "string"
  }
}
```

detail-type

Identifica el tipo de evento.

Para este evento, el valor es uno de los eventos AS2 enumerados anteriormente.

source

Identifica el servicio que generó el evento. Para Transfer Family los eventos, este valor es `aws.transfer`.

detail

Un objeto JSON que contiene información sobre el evento. El servicio que genera el evento determina el contenido de este campo.

s3-attributes

Identifica el depósito y la clave de Amazon S3 del archivo que se está transfiriendo. En el caso de los eventos de MDN, también identifica el depósito y la clave del archivo MDN.

file-bucket

El contenedor del objeto en Amazon S3.

file-key

El nombre asignado al objeto en Amazon S3.

json-bucket

En el caso de las transferencias FINALIZADAS o FALLIDAS, el contenedor del archivo JSON.

json-key

En el caso de transferencias COMPLETADAS o FALLIDAS, el nombre asignado al archivo JSON en Amazon S3.

mdn-bucket

En el caso de los eventos de MDN, el contenedor del archivo MDN.

mdn-key

Para los eventos de MDN, el nombre asignado al archivo MDN en Amazon S3.

`mdn-subject`

En el caso de los eventos de MDN, una descripción textual de la disposición del mensaje.

`mdn-message-id`

Para los eventos de MDN, un identificador único para el mensaje de MDN.

`disposition`

En el caso de los eventos de MDN, la categoría de la disposición.

`bytes`

El número de bytes del mensaje.

`as2-from`

El socio comercial de AS2 que envía el mensaje.

`as2-message-id`

Un identificador único para el mensaje AS2 que se está transfiriendo.

`as2-to`

El socio comercial de AS2 que recibe el mensaje.

`connector-id`

Para los mensajes AS2 que se envían desde un servidor de Transfer Family a un socio comercial, se utiliza el identificador único del conector AS2.

`client-ip`

Para los eventos del servidor (transferencias de un socio comercial a un servidor de Transfer Family), la dirección IP del cliente implicado en la transferencia.

`agreement-id`

En el caso de los eventos del servidor, el identificador único del acuerdo AS2.

`server-id`

Para los eventos del servidor, un identificador único solo para el servidor Transfer Family.

`requester-file-name`

En el caso de los eventos de carga útil, el nombre original del archivo recibido durante la transferencia.

message-subject

Una descripción textual del asunto del mensaje.

start-timestamp

Para que las transferencias se realicen correctamente, la marca de tiempo en la que comienza el procesamiento del archivo.

end-timestamp

Para que las transferencias se realicen correctamente, la marca de tiempo en la que se completa el procesamiento del archivo.

status-code

El código que corresponde al estado del proceso de transferencia de mensajes AS2. Valores válidos: COMPLETED | FAILED | PROCESSING.

failure-code

En el caso de las transferencias fallidas, la categoría por la que se produjo el error en la transferencia.

failure-message

En el caso de las transferencias fallidas, los detalles del motivo por el que se produjo el error en la transferencia.

transfer-id

El identificador único del evento de transferencia.

Example Ejemplo de evento AS2 Payload Receive Completed

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 Payload Receive Completed",
  "source": "aws.transfer",
  "account": "076722215406",
  "time": "2024-02-07T06:47:05Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:connector/c-1111aaaa2222bbbb3"],
}
```

```

    "detail": {
      "s3-attributes": {
        "file-key": "/inbound/processed/testAs2Message.dat",
        "file-bucket": "amzn-s3-demo-bucket"
      },
      "client-ip": "client-IP-address",
      "requester-file-name": "testAs2MessageVerifyFile.dat",
      "end-timestamp": "2024-02-07T06:47:06.040031Z",
      "as2-from": "as2-from-ID",
      "as2-message-id": "as2-message-ID",
      "message-subject": "Message from AS2 tests",
      "start-timestamp": "2024-02-07T06:47:05.410Z",
      "status-code": "PROCESSING",
      "bytes": 63,
      "as2-to": "as2-to-ID",
      "agreement-id": "a-1111aaaa2222bbbb3",
      "server-id": "s-1234abcd5678efghi"
    }
  }
}

```

Example Ejemplo de evento AS2 MDN Receive Failed

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 MDN Receive Failed",
  "source": "aws.transfer",
  "account": "889901007463",
  "time": "2024-02-06T22:05:09Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:server/s-1111aaaa2222bbbb3"],
  "detail": {
    "mdn-subject": "Your Requested MDN Response re: Test run from Id 123456789abcde  
to partner ijklmnop987654",
    "s3-attributes": {
      "json-bucket": "amzn-s3-demo-bucket1",
      "file-key": "/as2Integ/TestOutboundWrongCert.dat",
      "file-bucket": "amzn-s3-demo-bucket2",
      "json-key": "/as2Integ/failed/TestOutboundWrongCert.dat.json"
    },
    "mdn-message-id": "MDN-message-ID",
    "end-timestamp": "2024-02-06T22:05:09.479878Z",
    "as2-from": "PartnerA",

```

```
"as2-message-id": "as2-message-ID",
"connector-id": "c-1234abcd5678efghj",
"message-subject": "Test run from Id 123456789abcde to partner ijklmnop987654",
"start-timestamp": "2024-02-06T22:05:03Z",
"failure-code": "VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND",
"status-code": "FAILED",
"as2-to": "MyCompany",
"failure-message": "No public certificate matching message signature could be
found in profile: p-1234abcd5678efghj",
"transfer-id": "transfer-ID"
}
}
```

Seguridad en AWS Transfer Family

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:

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. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte [AWS la documentación de seguridad](#).

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Transfer Family. Los siguientes temas muestran cómo configurarlo AWS Transfer Family para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS Transfer Family recursos.

Ofrecemos un taller que proporciona orientación prescriptiva y un laboratorio práctico sobre cómo crear una arquitectura de transferencia de archivos segura y escalable AWS sin necesidad de modificar las aplicaciones existentes ni administrar la infraestructura de servidores. Puede ver los detalles de este taller [aquí](#).

Temas

- [Ventajas de la seguridad de la conectividad de VPC](#)
- [Políticas de seguridad para AWS Transfer Family servidores](#)
- [Políticas de seguridad para AWS Transfer Family Conectores SFTP](#)
- [Uso del intercambio híbrido de claves poscuánticas con AWS Transfer Family](#)

- [Protección y cifrado de datos](#)
- [Administración de claves SSH y PGP en Transfer Family](#)
- [Administración de identidad y acceso para AWS Transfer Family](#)
- [Validación de conformidad para AWS Transfer Family](#)
- [Resiliencia en AWS Transfer Family](#)
- [Cree una conexión privada entre una VPC y AWS Transfer Family API](#)
- [Seguridad de la infraestructura en AWS Transfer Family](#)
- [Agregue un cortafuegos de aplicaciones web](#)
- [Cross-service confusa prevención de diputados](#)
- [AWS políticas administradas para AWS Transfer Family](#)

Ventajas de la seguridad de la conectividad de VPC

Los conectores SFTP con salida de VPC proporcionan beneficios Cross-VPC de seguridad mejorados a través del acceso a los recursos:

- Aislamiento de la red: todo el tráfico permanece dentro del entorno de VPC, lo que proporciona un aislamiento total de la red de Internet pública para las conexiones de puntos finales privados.
- Control de IP de origen: los servidores SFTP remotos solo ven las direcciones IP del rango CIDR de su VPC, lo que le da un control total sobre las direcciones IP de origen utilizadas para las conexiones.
- Acceso a terminales privados: Conéctese directamente a los servidores SFTP de su VPC mediante direcciones IP privadas, lo que elimina la exposición a la Internet pública.
- Conectividad híbrida: acceda de forma segura a los servidores SFTP locales a través de conexiones VPN o Direct Connect establecidas sin exposición adicional a Internet.
- Controles de seguridad de VPC: aproveche los grupos de seguridad de VPC, las NACL y las políticas de enrutamiento existentes para controlar y monitorear el tráfico de los conectores SFTP.

Modelo de seguridad VPC Lattice

La conectividad de VPC para los conectores SFTP utiliza AWS VPC Lattice con redes de servicio para proporcionar un acceso seguro a múltiples inquilinos:

- **Prevención de problemas de subcontratación:** las comprobaciones de autenticación y autorización garantizan que los conectores solo puedan acceder a los recursos específicos para los que están configurados, lo que evita el acceso no autorizado entre inquilinos.
- **IPv6-only red de servicio:** utiliza el direccionamiento IPv6 para evitar posibles conflictos de direcciones IP y mejorar el aislamiento de seguridad.
- **Sesión de acceso directo (FAS):** la gestión temporal de credenciales elimina la necesidad de almacenar las credenciales a largo plazo o de compartir recursos manualmente.
- **Resource-level control de acceso:** cada conector está asociado a una configuración de recursos específica, lo que garantiza un control de acceso detallado a los servidores SFTP individuales.

Mejores prácticas de seguridad para la conectividad de VPC

Cuando utilice conectores de tipo salida de VPC, siga estas prácticas recomendadas de seguridad:

- **Grupos de seguridad:** configure los grupos de seguridad para permitir el tráfico SFTP (puerto 22) solo entre los recursos necesarios. Restrinja los rangos de IP de origen y destino al mínimo requerido.
- **Ubicación de las puertas de enlace de recursos:** implemente las puertas de enlace de recursos en subredes privadas siempre que sea posible y asegúrese de que abarquen al menos dos zonas de disponibilidad para una alta disponibilidad.
- **Supervisión de la red:** utilice los registros de flujo de VPC y Amazon CloudWatch para supervisar los patrones de tráfico de la red y detectar actividades anómalas.
- **Registro de acceso:** habilite el registro de conectores para realizar un seguimiento de las actividades de transferencia de archivos y mantener registros de auditoría para cumplir con los requisitos de conformidad.
- **Administración de la configuración de los recursos:** revise y actualice periódicamente las configuraciones de los recursos para asegurarse de que apuntan a los servidores SFTP correctos y utilizan la configuración de red adecuada.

Políticas de seguridad para AWS Transfer Family servidores

Las políticas de seguridad del servidor AWS Transfer Family le permiten limitar el conjunto de algoritmos criptográficos (códigos de autenticación de mensajes (MAC), intercambios de claves (KEX), conjuntos de cifrado, cifrados de contenido y algoritmos hash) asociados a su servidor.

AWS Transfer Family admite políticas de seguridad poscuántica que utilizan algoritmos híbridos de intercambio de claves, combinando métodos criptográficos tradicionales con algoritmos poscuánticos para proporcionar una mayor seguridad contra las futuras amenazas de la computación cuántica. Para obtener más información, consulte [Uso del intercambio híbrido de claves poscuánticas con AWS Transfer Family](#).

Para consultar una lista de los algoritmos criptográficos admitidos, consulte [Algoritmos criptográficos](#). Para obtener una lista de los algoritmos clave admitidos para su uso con las claves del host del servidor y las claves de usuario administradas por el servicio, consulte [Administración de claves SSH y PGP en Transfer Family](#).

 Note

A partir de 2025, todas las nuevas políticas de AWS Transfer Family seguridad incluyen el soporte criptográfico poscuántico mediante algoritmos híbridos de intercambio de claves. Para obtener más información sobre la seguridad poscuántica, consulte [Uso del intercambio híbrido de claves poscuánticas con AWS Transfer Family](#)

 Note

Recomendamos encarecidamente actualizar sus servidores a nuestra política de seguridad más reciente.

- `TransferSecurityPolicy-2024-01` es la política de seguridad predeterminada que se adjunta al servidor al crear un servidor mediante la consola, la API o la CLI.
- Si crea un servidor Transfer Family utilizando CloudFormation y acepta la política de seguridad predeterminada, se asigna el `servidorTransferSecurityPolicy-2018-11`.

Si le preocupa la compatibilidad de los clientes, indique afirmativamente qué política de seguridad desea utilizar al crear o actualizar un servidor en lugar de utilizar la política predeterminada, que está sujeta a cambios. Para cambiar la política de seguridad de un servidor, consulte [Editar la política de seguridad](#).

 Note

Las políticas anteriores a las cuánticas (TransferSecurityPolicy-PQ-SSH-Experimental-2023-04y TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04) están en desuso. Le recomendamos que utilice las nuevas políticas en su lugar.

Para obtener más información sobre la seguridad de Transfer Family, consulta las siguientes entradas del blog:

- [Seis consejos para mejorar la seguridad de su AWS Transfer Family servidor](#)
- [Cómo Transfer Family puede ayudarlo a crear una solución de transferencia de archivos gestionada segura y compatible](#)

Temas

- [Algoritmos criptográficos](#)
- [Detalles de la política de seguridad](#)

Algoritmos criptográficos

Para las claves de host, admitimos los siguientes algoritmos:

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`
- `ssh-ed25519`

Además, las siguientes políticas de seguridad permiten `ssh-rsa`:

- `TransferSecurityPolicy-2018-11`
- `TransferSecurityPolicy-2020-06`
- `TransferSecurityPolicy-FIPS-2020-06`

- TransferSecurityPolicy-FIPS-2023-05
- TransferSecurityPolicy-FIPS-2024-01

 Note

Es importante entender la diferencia entre el tipo de clave RSA (que siempre es así) `ssh-rsa` y el algoritmo de clave de host de RSA, que puede ser cualquiera de los algoritmos compatibles.

La siguiente es una lista de los algoritmos criptográficos admitidos con cada política de seguridad.

 Note

En la tabla y las políticas siguientes, observe el siguiente uso de los tipos de algoritmos.

- Los servidores SFTP solo utilizan algoritmos en las `SshMac`secciones `SshCiphers` y `SshKex`s, y.
- Los servidores FTPS solo utilizan los algoritmos de la `TlsCiphers`sección.
- Los servidores FTP, dado que no utilizan cifrado, no utilizan ninguno de estos algoritmos.
- Los servidores AS2 solo utilizan algoritmos en las `HashAlgorithms`secciones `ContentEncryptionCiphers`y. Estas secciones definen los algoritmos que se utilizan para cifrar y firmar el contenido de los archivos.
- Las políticas FIPS-2024-01 de seguridad FIPS-2024-05 y las de seguridad son idénticas, excepto que FIPS-2024-05 no admiten el `ssh-rsa` algoritmo.
- Transfer Family ha introducido nuevas políticas restringidas que son muy paralelas a las políticas existentes:
 - Las políticas `TransferSecurityPolicy-2018-11` de seguridad `TransferSecurityPolicy-Restricted-2018-11` y las de seguridad son idénticas, excepto que la política restringida no admite el `chacha20-poly1305@openssh.com` cifrado.
 - Las políticas `TransferSecurityPolicy-2020-06` de seguridad `TransferSecurityPolicy-Restricted-2020-06` y las políticas son idénticas, excepto que la política restringida no admite el `chacha20-poly1305@openssh.com` cifrado.

* En la siguiente tabla, el `chacha20-poly1305@openssh.com` cifrado solo se incluye en la política no restringida,

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2023-06	TransferSecurityPolicy-2020-09	TransferSecurityPolicy-2020-11
			Compressed	Restricted		TransferSecurityPolicy-2024-05				TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
SshCiphers											
aes128-ctr	◆	◆	◆	◆	◆					◆	◆
aes128-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes192-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Compliant-2025-07			TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06		TransferSecurityPolicy-2018-11
chacha20-poly1305@openssh.com									*		*	
SshKexs												
mlkem768x25519-sha256	◆		◆									
mlkem768nistp256-sha256	◆		◆									
mlkem1024nistp384-sha384	◆		◆									
curva25519-sha256	◆	◆	◆	◆		◆		◆				◆

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01/FIPS	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-11	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Compliant-2025-07	Restricted		TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-11	TransferSecurityPolicy-2018-11
curve25519-sha256@libssh.org		◆	◆	◆		◆		◆				◆
diffie-hellman-group14-sha1												◆
diffie-hellman-group14-sha256									◆	◆	◆	

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01/FIPS	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Restricted-2025-07			TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11	
diffie-he	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
llman-gro											
up16-sha512											
diffie-he	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
llman-gru											
po18-sha512											
diffie-he	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
llman-gro											
up-exchan											
ge-sha256											

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-2025-07	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2024-05	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-11	TransferSecurityPolicy-2018-11
ecdh-sha2-nistp256	◆	◆		◆	◆	◆			◆	◆	◆
ecdh-sha2-nistp384	◆	◆		◆	◆	◆			◆	◆	◆
ecdh-sha2-nistp521	◆	◆		◆	◆	◆			◆	◆	◆
SshMacs											
hmac-sha1											◆
hmac-sha1											◆
etm@openssh.com											

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2025-07	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2025-05	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-11
hmac-sha2-256										◆	◆	◆	◆
hmac-sha2-256-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
hmac-sha2-512										◆	◆	◆	◆
hmac-sha2-512-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
umac-128-etm@openssh.com											◆		◆

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-09	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Compliant-2025-07			TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
umac-128@openssh.com									◆		◆
umac-64-etm@openssh.com											◆
umac-64@openssh.com											◆
ContentEncryptionCiphers											
aes256-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes192-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes128-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
3des-cbc	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01/FIPS	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-FIPS	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Compliant-2025-07	Restricted		TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06			TransferSecurityPolicy-2018-11

HashAlgorithms

sha256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha512	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha1	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆

TlsCiphers

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-09	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Compliant-2025-07			TransferSecurityPolicy-2024-05			TransferSecurityPolicy-Restricted-2020-06		TransferSecurityPolicy-Restricted-2018-11
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Política de seguridad	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2025-05	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
			Compliant-2025-02	Restricted-2025-07		TransferSecurityPolicy-2024-05				TransferSecurityPolicy-2020-06		TransferSecurityPolicy-2018-11
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_RSA_WITH_AES_128_CBC_SHA256												◆
TLS_RSA_WITH_AES_256_CBC_SHA256												◆

Detalles de la política de seguridad

Las siguientes secciones contienen la representación en JSON de cada política de seguridad.

TransferSecurityPolicy-2025-03

A continuación se muestra la política TransferSecurityPolicy-2025-03 de seguridad.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2025-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ]
  },
}
```

```

    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
      "SFTP",
      "FTPS"
    ]
  }
}

```

TransferSecurityPolicy-FIPS-2025-03

A continuación se muestra la política TransferSecurityPolicy-FIPS-2025-03 de seguridad.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2025-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr",
      "aes128-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512"
    ]
  }
}

```

```

    ],
    "SshMac": [
        "hmac-sha2-512-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}

```

TransferSecurityPolicy-AS2Restricted-2025-07

Esta política de seguridad está diseñada para las transferencias de archivos AS2 que requieren una seguridad mejorada al excluir los algoritmos criptográficos heredados. Es compatible con los algoritmos modernos de cifrado AES y SHA-2 hash, al tiempo que elimina la compatibilidad con algoritmos más débiles, como 3DES y SHA-1.

Note

Esta política de seguridad es idéntica a TransferSecurityPolicy-2025-03, excepto que no es compatible con 3DES (entrada ContentEncryptionCiphers) ni con SHA1 (entrada). HashAlgorithms Incluye todos los algoritmos de 2025 a 2003, incluidos los algoritmos criptográficos poscuánticos (mlkem* KEXs).

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-AS2Restricted-2025-07",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
    ],
    "HashAlgorithms": [
```

```

        "sha256",
        "sha384",
        "sha512"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}

```

TransferSecurityPolicy-SshAuditCompliant-2025-02

A continuación se muestra la política TransferSecurityPolicy-SshAuditCompliant-2025-02 de seguridad.

Note

Esta política de seguridad está diseñada en función de las recomendaciones de la `ssh-audit` herramienta y es 100% compatible con esa herramienta.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "Protocols": [
      "SFTP",
      "FTPS"
    ],
    "SecurityPolicyName": "TransferSecurityPolicy-SshAuditCompliant-2025-02",
    "SshCiphers": [

```



```
    "aes128-gcm@openssh.com",
    "aes256-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
  ],
  "SshKexs": [
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group-exchange-sha256"
  ],
  "SshMacs": [
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ],
  "Type": "SERVER"
}
```

TransferSecurityPolicy-2024-01

A continuación se muestra la política TransferSecurityPolicy-2024-01 de seguridad.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
```

```

        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}

```

TransferSecurityPolicy-FIPS-2024-01/TransferSecurityPolicy-FIPS-2024-05

A continuación se muestran las políticas TransferSecurityPolicy-FIPS-2024-05 de seguridad TransferSecurityPolicy-FIPS-2024-01 y.

Note

Las políticas de TransferSecurityPolicy-FIPS-2024-05 seguridad TransferSecurityPolicy-FIPS-2024-01 y punto final del servicio FIPS solo están disponibles en algunas AWS regiones. Para obtener más información, consulte [Puntos de conexión y cuotas de AWS Transfer Family](#) en la Referencia general de AWS.

La única diferencia entre estas dos políticas de seguridad es que son TransferSecurityPolicy-FIPS-2024-01 compatibles con el `ssh-rsa` algoritmo y TransferSecurityPolicy-FIPS-2024-05 no lo son.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",

```

```

        "diffie-hellman-group18-sha512",
        "diffie-hellman-group16-sha512",
        "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
        "hmac-sha2-256-etm@openssh.com",
        "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-2023-05

A continuación se muestra la política TransferSecurityPolicy-2023-05 de seguridad.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2023-05",
    "SshCiphers": [
      "aes256-gcm@openssh.com",

```

```

        "aes128-gcm@openssh.com",
        "aes256-ctr",
        "aes192-ctr"
    ],
    "SshKexs": [
        "curve25519-sha256",
        "curve25519-sha256@libssh.org",
        "diffie-hellman-group16-sha512",
        "diffie-hellman-group18-sha512",
        "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
        "hmac-sha2-512-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-FIPS-2023-05

Los detalles de la certificación FIPS se AWS Transfer Family pueden encontrar en <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

A continuación se muestra la política TransferSecurityPolicy-FIPS-2023-05 de seguridad.

Note

La política de TransferSecurityPolicy-FIPS-2023-05 seguridad y punto final del servicio FIPS solo está disponible en algunas AWS regiones. Para obtener más información, consulte [Puntos de conexión y cuotas de AWS Transfer Family](#) en la Referencia general de AWS.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2023-05",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
```

```

        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}

```

TransferSecurityPolicy-2022-03

A continuación se muestra la política TransferSecurityPolicy-2022-03 de seguridad.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2022-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ],
  },
}

```

```

    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}

```

TransferSecurityPolicy-2020-06 y TransferSecurityPolicy-Restricted-2020-06

A continuación se muestra la política TransferSecurityPolicy-2020-06 de seguridad.

Note

Las políticas TransferSecurityPolicy-2020-06 de seguridad TransferSecurityPolicy-Restricted-2020-06 y las políticas son idénticas, excepto que la política restringida no admite el `chacha20-poly1305@openssh.com` cifrado.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [

```



```

    "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2020-06
    "aes128-ctr",
    "aes192-ctr",
    "aes256-ctr",
    "aes128-gcm@openssh.com",
    "aes256-gcm@openssh.com"
  ],
  "SshKexs": [
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "diffie-hellman-group-exchange-sha256",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group14-sha256"
  ],
  "SshMacs": [
    "umac-128-etm@openssh.com",
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com",
    "umac-128@openssh.com",
    "hmac-sha2-256",
    "hmac-sha2-512"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",

```

```

    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-FIPS-2020-06

Los detalles de la certificación FIPS se AWS Transfer Family pueden encontrar en <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

A continuación se muestra la política TransferSecurityPolicy-FIPS-2020-06 de seguridad.

Note

La política de TransferSecurityPolicy-FIPS-2020-06 seguridad y punto final del servicio FIPS solo están disponibles en algunas AWS regiones. Para obtener más información, consulte [Puntos de conexión y cuotas de AWS Transfer Family](#) en la Referencia general de AWS.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2020-06",
    "SshCiphers": [
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",

```

```

    "hmac-sha2-512-etm@openssh.com",
    "hmac-sha2-256",
    "hmac-sha2-512"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-2018-11 y TransferSecurityPolicy-Restricted-2018-11

A continuación se muestra la política TransferSecurityPolicy-2018-11 de seguridad.

Note

Las políticas TransferSecurityPolicy-2018-11 de seguridad TransferSecurityPolicy-Restricted-2018-11 y las políticas son idénticas, excepto que la política restringida no admite el `chacha20-poly1305@openssh.com` cifrado.

```

{
  "SecurityPolicy": {

```

```

    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2018-11
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256",
      "diffie-hellman-group14-sha1"
    ],
    "SshMacs": [
      "umac-64-etm@openssh.com",
      "umac-128-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha1-etm@openssh.com",
      "umac-64@openssh.com",
      "umac-128@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512",
      "hmac-sha1"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",

```

```
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
    "TLS_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_RSA_WITH_AES_256_CBC_SHA256"
  ]
}
```

Políticas de seguridad para AWS Transfer Family Conectores SFTP

Las políticas de seguridad del conector SFTP AWS Transfer Family permiten limitar el conjunto de algoritmos criptográficos (códigos de autenticación de mensajes (MAC), intercambios de claves (KEX) y conjuntos de cifrado) asociados al conector SFTP. La siguiente es una lista de los algoritmos criptográficos compatibles para cada política de seguridad del conector SFTP.

Note

`TransferSFTPConnectorSecurityPolicy-2024-03` es la política de seguridad predeterminada que se aplica a los conectores SFTP.

Puede cambiar la política de seguridad del conector. Seleccione **Connectors** en el panel de navegación izquierdo de Transfer Family y seleccione su conector. A continuación, seleccione **Editar** en la sección de configuración de Sftp. En la sección de opciones de algoritmos criptográficos, elija cualquier política de seguridad disponible en la lista desplegable del campo **Política de seguridad**.

Algoritmos criptográficos

En cuanto a las claves de host, los conectores SFTP admiten todos los algoritmos compatibles con los servidores Transfer Family, excepto ed25519:

- rsa-sha2-256
- rsa-sha2-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521

Además, para las claves de host, admitimosssh-rsa, pero solo para. TransferSFTPConnectorSecurityPolicy-2023-07

Para la autenticación, los conectores SFTP admiten los siguientes tipos de claves:

- ssh-rsa
- ecdsa

Detalles de la política de seguridad del conector SFTP

La siguiente tabla muestra los algoritmos criptográficos específicos compatibles con cada política de seguridad del conector SFTP.

Política de seguridad	TransferSFTPConnec torSecurityPolicy- FIPS-2024-10	TransferSFTPConnec torSecurityPolicy- 2024-03	TransferSFTPConnec torSecurityPolicy- 2023-07
Ciphers			
aes128-ctr			◆
aes128-gc m@openssh.com	◆	◆	◆
aes192-ctr		◆	◆

Política de seguridad	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
aes256-ctr		◆	◆
aes256-gcm@openssh.com	◆	◆	◆
Kexs			
curve25519-sha256		◆	◆
curve25519-sha256@libssh.org		◆	◆
diffie-hellman-group14-sha1			◆
diffie-hellman-group16-sha512		◆	◆
diffie-hellman-group18-sha512		◆	◆
diffie-hellman-group-exchange-sha256		◆	◆
ecdh-sha2-nistp256	◆		
ecdh-sha2-nistp384	◆		
ecdh-sha2-nistp521	◆		
Macs			
hmac-sha2-512-etm@openssh.com		◆	◆
hmac-sha2-256-etm@openssh.com		◆	◆

Política de seguridad	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
hmac-sha2-512	◆	◆	◆
hmac-sha2-256	◆	◆	◆
hmac-sha1			◆
hmac-sha1-96			◆
Host Key Algorithms			
rsa-sha2-256	◆	◆	◆
rsa-sha2-512	◆	◆	◆
ecdsa-sha2-nistp256	◆	◆	◆
ecdsa-sha2-nistp384		◆	◆
ecdsa-sha2-nistp521		◆	◆
ssh-rsa			◆

Uso del intercambio híbrido de claves poscuánticas con AWS Transfer Family

Transfer Family admite una opción híbrida de establecimiento de claves poscuánticas para el protocolo Secure Shell (SSH). Post-quantum el establecimiento de claves es necesario porque ya es posible registrar el tráfico de la red y guardarlo para su descifrado en el futuro mediante un ordenador cuántico, lo que se denomina ataque de almacenamiento ahora, cosecha después.

Puede utilizar esta opción cuando se conecte a Transfer Family para realizar transferencias seguras de archivos desde y hacia el almacenamiento de Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS). Post-quantum El establecimiento de claves híbridas en SSH introduce mecanismos de establecimiento de claves poscuánticos, que utiliza junto con los algoritmos de intercambio de claves clásicos. Con la tecnología actual, las claves SSH creadas

con los conjuntos de cifrado clásicos están a salvo de los ataques de fuerza bruta con tecnología actual. Sin embargo, no se espera que el cifrado clásico siga siendo seguro tras la aparición de la computación cuántica a gran escala en el futuro.

Si su organización depende de la confidencialidad a largo plazo de los datos que se transmiten a través de una conexión de Transfer Family, debería considerar un plan para migrar a la criptografía poscuántica antes de que las computadoras cuánticas a gran escala estén disponibles para su uso.

Para proteger los datos cifrados hoy contra posibles ataques futuros, AWS participa con la comunidad criptográfica en el desarrollo de algoritmos cuánticos resistentes o poscuánticos. Hemos implementado conjuntos de cifrado de intercambio de claves híbrido poscuántico en Transfer Family que combinan elementos clásicos y poscuánticos.

Estos conjuntos de cifrado híbridos están disponibles para su uso en las cargas de trabajo de producción en la mayoría de las regiones de AWS. Sin embargo, dado que las características de rendimiento y los requisitos de ancho de banda de los conjuntos de cifrado híbridos son diferentes de los mecanismos clásicos de intercambio de claves, le recomendamos que los pruebe en sus conexiones de Transfer Family.

[Obtenga más información sobre la criptografía poscuántica en la entrada del blog sobre seguridad criptográfica. Post-Quantum](#)

Contenido

- [Acerca del intercambio de claves híbrido poscuántico en SSH](#)
- [Cómo funciona el establecimiento de claves híbrido poscuántico en Transfer Family](#)
 - [¿Por qué? ML-KEM](#)
 - [Post-quantum requisitos criptográficos y de intercambio de claves SSH híbridas \(FIPS 140\)](#)
- [Prueba del intercambio de claves híbrido poscuántico en Transfer Family](#)
 - [Habilite el intercambio de claves híbrido poscuántico en su punto de conexión SFTP](#)
 - [Configuración de un cliente SFTP que admita el intercambio de claves híbrido poscuántico](#)
 - [Confirmación del intercambio de claves híbrido poscuántico en SFTP](#)

Acerca del intercambio de claves híbrido poscuántico en SSH

Transfer Family admite conjuntos de cifrado de intercambio de claves híbridos poscuánticos, que utilizan tanto el algoritmo de intercambio de claves clásico de [curva elíptica Diffie-Hellman \(ECDH\)](#)

como. ML-KEM ML-KEM es un algoritmo poscuántico de cifrado y establecimiento de claves públicas que el [Instituto Nacional de Estándares y Tecnología \(NIST\) ha designado](#) como su primer algoritmo estándar de acuerdo de claves poscuánticas.

El cliente y el servidor siguen intercambiando claves ECDH. Además, el servidor encapsula un secreto compartido poscuántico en la clave pública KEM poscuántica del cliente, que se anuncia en el mensaje de intercambio de claves SSH del cliente. Esta estrategia combina la alta seguridad de un intercambio de claves clásico con la seguridad de los intercambios de claves poscuánticos propuestos para ayudar a garantizar que los protocolos de enlace estén protegidos mientras no se pueda descifrar el ECDH o el secreto compartido poscuántico.

Cómo funciona el establecimiento de claves híbrido poscuántico en Transfer Family

AWS anunció recientemente que admite el intercambio de claves poscuánticas en las transferencias de archivos SFTP en. AWS Transfer Family Transfer Family escala de forma segura las transferencias de archivos de empresa a empresa a servicios AWS de almacenamiento mediante SFTP y otros protocolos. SFTP es una versión más segura del Protocolo de File Transfer (FTP) que se ejecuta a través de SSH. La compatibilidad de intercambio de claves poscuántico de Transfer Family eleva el nivel de seguridad para las transferencias de datos a través de SFTP.

El soporte SFTP de intercambio de claves híbrido poscuántico de Transfer Family incluye la combinación de algoritmos poscuánticos y ML-KEM-768 ML-KEM-1024, con ECDH sobre curvas P256, P384 o Curve25519. Los siguientes métodos de intercambio de claves SSH correspondientes se especifican en [el borrador del intercambio de claves híbrido poscuántico SSH](#).

- mlkem768nistp256-sha256
- mlkem1024nistp384-sha384
- mlkem768x25519-sha256

¿Por qué? ML-KEM

AWS se compromete a admitir algoritmos estandarizados e interoperables. ML-KEM es el único algoritmo de intercambio de claves poscuántico estandarizado y aprobado por el proyecto de criptografía del [NIST. Post-Quantum](#). Los organismos de normalización ya se están integrando ML-KEM en los protocolos. AWS ya es compatible con ML-KEM TLS en algunos puntos finales de AWS la API.

Como parte de este compromiso, AWS ha presentado un borrador de propuesta al IETF para la criptografía poscuántica que se combina ML-KEM con NIST-approved curvas como la P256 para SSH. Para ayudar a mejorar la seguridad de nuestros clientes, la AWS implementación del intercambio de claves poscuánticas en SFTP y SSH sigue ese borrador. Planeamos admitir actualizaciones futuras hasta que nuestra propuesta sea adoptada por el IETF y se convierta en un estándar.

Los nuevos métodos de intercambio de claves (enumerados en la sección [Cómo funciona el establecimiento de claves híbrido poscuántico en Transfer Family](#)) podrían cambiar a medida que el borrador avance hacia la estandarización.

 Note

Post-quantum En la actualidad, se admite el uso de algoritmos para el intercambio de claves híbridas poscuánticas en TLS AWS KMS (consulte [Uso del TLS poscuántico híbrido con AWS KMS](#)) y puntos finales de API.AWS Certificate Manager AWS Secrets Manager

Post-quantum requisitos criptográficos y de intercambio de claves SSH híbridas (FIPS 140)

Para los clientes que requieren el cumplimiento de FIPS, Transfer Family proporciona FIPS-approved criptografía en SSH mediante la biblioteca criptográfica de código abierto con certificación AWS FIPS 140, -LC. AWS Los métodos de intercambio de claves híbridos poscuánticos compatibles con la TransferSecurityPolicy-FIPS-2025-03 familia Transfer Family están aprobados por la FIPS según la norma [SP 800-56Cr2 del NIST](#) (sección 2). La Oficina Federal de Seguridad de la Información de Alemania ([BSI](#)) y la Agence nationale de la sécurité des systèmes d'information ([ANSSI](#)) de Francia también recomiendan estos métodos de intercambio de claves híbrido poscuántico.

Prueba del intercambio de claves híbrido poscuántico en Transfer Family

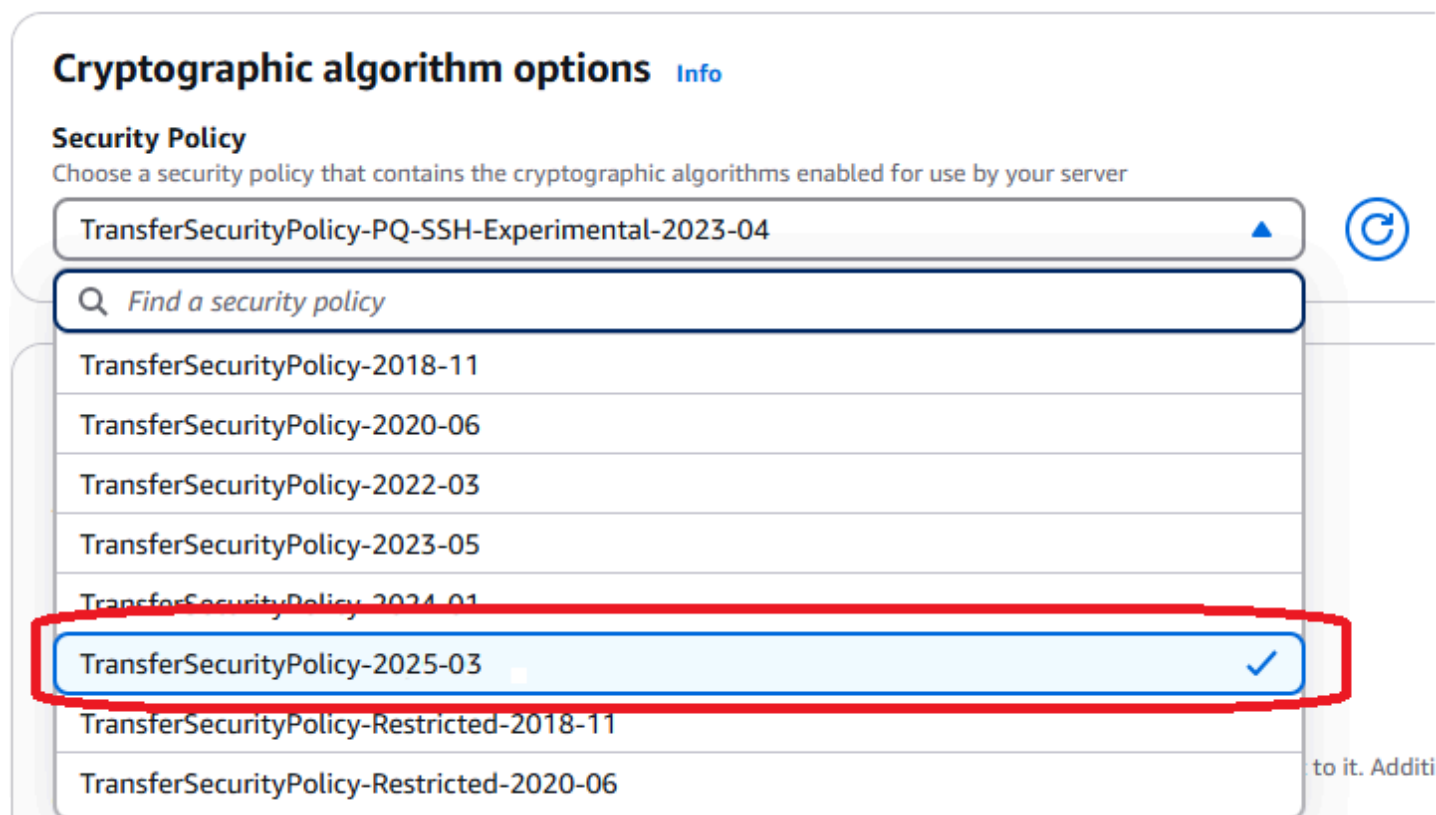
En esta sección, se describen los pasos que debe seguir para probar el intercambio de claves híbrido poscuántico.

1. [Habilite el intercambio de claves híbrido poscuántico en su punto de conexión SFTP.](#)
2. Utilice un cliente SFTP (por ejemplo, [Configuración de un cliente SFTP que admita el intercambio de claves híbrido poscuántico](#)) que admita el intercambio de claves híbrido poscuántico siguiendo las instrucciones de la especificación del borrador mencionado anteriormente.

3. Transfiera un archivo mediante un servidor de Transfer Family.
4. [Confirmación del intercambio de claves híbrido poscuántico en SFTP](#).

Habilite el intercambio de claves híbrido poscuántico en su punto de conexión SFTP

Puede elegir la política SSH al crear un nuevo punto de conexión de servidor SFTP en Transfer Family o al editar las opciones del algoritmo criptográfico en un punto de conexión SFTP existente. La siguiente instantánea muestra un ejemplo en el que Consola de administración de AWS se actualiza la política de SSH.



Los nombres de las políticas de SSH que admiten el intercambio de claves poscuánticas son y. TransferSecurityPolicy-2025-03TransferSecurityPolicy-FIPS-2025-03 Para obtener más información sobre las políticas de Transfer Family, consulte [Políticas de seguridad para AWS Transfer Family servidores](#).

Configuración de un cliente SFTP que admita el intercambio de claves híbrido poscuántico

Tras seleccionar la política SSH poscuántica correcta en el punto de conexión SFTP de Transfer Family, puede experimentar con el SFTP poscuántico en Transfer Family. Instale el cliente OpenSSH más reciente (por ejemplo, la versión 9.9) en su sistema local para realizar la prueba.

Note

Asegúrese de que su cliente sea compatible con uno o más de los ML-KEM algoritmos enumerados anteriormente. Puede ver los algoritmos compatibles con su versión de OpenSSH ejecutando este comando: `ssh -Q kex`

Puede ejecutar el cliente SFTP de ejemplo para conectarse a su terminal SFTP (por ejemplos-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com) mediante los métodos de intercambio de claves híbridos poscuánticos, como se muestra en el siguiente comando.

```
sftp -v -o \
  KexAlgorithms=mlkem768x25519-sha256 \
  -i username_private_key_PEM_file \
  username@server-id.server.transfer.region-id.amazonaws.com
```

En el siguiente comando, reemplace los elementos siguientes con su propia información:

- *username_private_key_PEM_file* Sustitúyalo por el archivo de clave privada del usuario de SFTP PEM-encoded
- *username* Sustitúyalo por el nombre de usuario de SFTP
- *server-id* Sustitúyalo por el ID del servidor de Transfer Family
- *region-id* Sustitúyalo por la región real en la que se encuentra el servidor de Transfer Family

Confirmación del intercambio de claves híbrido poscuántico en SFTP

Para confirmar que se utilizó el intercambio de claves híbrido poscuántico durante una conexión SSH para SFTP a Transfer Family, compruebe la salida del cliente. Si lo desea, puede utilizar un programa de captura de paquetes. Si utiliza el cliente OpenSSH 9.9, el resultado debería tener un aspecto similar al siguiente (omitiendo información irrelevante por motivos de brevedad):

```
% sftp -o KexAlgorithms=mlkem768x25519-sha256 -v -o IdentitiesOnly=yes -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_9.9p2, OpenSSL 3.4.1 11 Feb 2025
debug1: Reading configuration data /Users/username/.ssh/config
debug1: /Users/username/.ssh/config line 146: Applying options for *
debug1: Reading configuration data /Users/username/.ssh/bastions-config
debug1: Reading configuration data /opt/homebrew/etc/ssh/ssh_config
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
[xxx.yyy.zzz.nnn] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_9.9
debug1: Remote protocol version 2.0, remote software version AWS_SFTP_1.1
debug1: compat_banner: no match: AWS_SFTP_1.1
debug1: Authenticating to s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com:22 as 'username'
debug1: load_hostkeys: fopen /Users/username/.ssh/known_hosts2: No such file or
directory
[...]
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: mlkem768x25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: kex: client->server cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:Ic1Ti0cdDmFdStj06rfU0cmmNccwAha/ASH2unr6zX0
[...]
debug1: rekey out after 4294967296 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 4294967296 blocks
[...]
Authenticated to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
([xxx.yyy.zzz.nnn]:22) using "publickey".
debug1: channel 0: new session [client-session] (inactive timeout: 0)
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
```

```
sftp>
```

La salida muestra que la negociación con el cliente se llevó a cabo mediante el método híbrido poscuántico `m1kem768x25519-sha256` y que se estableció correctamente una sesión SFTP.

Protección y cifrado de datos

El modelo de [responsabilidad AWS compartida modelo](#) se aplica a la protección de datos en AWS Transfer Family (Transfer Family). Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se basa toda la AWS nube. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye las tareas de configuración y administración de la seguridad de AWS los servicios que utiliza. Para obtener más información sobre la privacidad de datos, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación del blog [Modelo de responsabilidad compartida de AWS](#) y RGPD en el blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja las credenciales de las AWS cuentas y configure cuentas de usuario individuales con ellas AWS IAM Identity Center. De esta manera, cada usuario recibe únicamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes maneras:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Úselo SSL/TLS para comunicarse con AWS los recursos. Admitimos TLS 1.2.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados de AWS los servicios.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, números de cuenta de sus clientes, en los campos de formato libre, como el

campo Nombre. Esto incluye cuando trabajas con Transfer Family u otros AWS servicios mediante la consola, la API o AWS los SDK. AWS CLI Cualquier dato de configuración que escriba en la configuración del servicio Transfer Family o en las configuraciones de otros servicios se puede incluir en los registros de diagnóstico. Cuando proporcione una URL a un servidor externo, no incluya información de credenciales en la URL para validar la solicitud para ese servidor.

Por el contrario, los datos de las operaciones de carga y descarga que entran y salen de los servidores de Transfer Family se consideran completamente privados y nunca existen fuera de los canales cifrados, como una conexión SFTP o FTPS. Solo las personas autorizadas pueden acceder a estos datos.

Cifrado de datos en Transfer Family

AWS Transfer Family utiliza las opciones de cifrado predeterminadas que ha establecido para su bucket de Amazon S3 para cifrar sus datos. Cuando se habilita el cifrado en un bucket, todos los objetos se cifran en el momento de almacenarse en el bucket. Los objetos se cifran mediante el cifrado del lado del servidor con claves administradas de Amazon S3 (SSE-S3) o claves administradas AWS Key Management Service (AWS KMS) (SSE-KMS). Para obtener más información sobre el cifrado del servidor, consulte [Protección de datos con el cifrado del lado del servidor](#) en la Guía del usuario de Amazon Simple Storage Service.

Los siguientes pasos le muestran cómo cifrar los datos. AWS Transfer Family

Para permitir el cifrado en AWS Transfer Family

1. Habilitación del cifrado predeterminado en un bucket de Amazon S3. Para obtener instrucciones, consulte [Cifrado predeterminado de Amazon S3 para los buckets de S3](#) en la Guía del usuario de Amazon Simple Storage Service.
2. Actualice la política de funciones AWS Identity and Access Management (IAM) asociada al usuario para conceder los permisos necesarios AWS Key Management Service (AWS KMS).
3. Si utiliza una política de sesión para el usuario, la política de sesión debe conceder los AWS KMS permisos necesarios.

El siguiente ejemplo muestra una política de IAM que concede los permisos mínimos necesarios cuando se utiliza AWS Transfer Family con un bucket de Amazon S3 que está habilitado para el AWS KMS cifrado. Incluya esta política de ejemplo en la política del rol de IAM del usuario y en la política de ámbito reducido, si utiliza alguna.


```
{
  "Sid": "Stmt1544140969635",
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:GetPublicKey",
    "kms:ListKeyPolicies"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

Note

El ID de clave de KMS especificado en esta política debe ser el mismo que el especificado para el cifrado predeterminado en el paso 1.

La política AWS KMS clave debe permitir la raíz, o la función de IAM que se utiliza para el usuario. Para obtener información sobre la política AWS KMS clave, consulte [Uso de políticas clave en AWS KMS en](#) la Guía para AWS Key Management Service desarrolladores.

AWS Transfer Family cifrado en reposo

Como AWS Transfer Family es un servicio de transferencia de archivos, no administra los datos de almacenamiento en reposo. Los servicios y sistemas de almacenamiento AWS Transfer Family compatibles son responsables de proteger los datos en ese estado. Sin embargo, hay algunos datos relacionados con el servicio que se AWS Transfer Family administran en reposo.

¿Qué se cifra?

Los únicos datos que se AWS Transfer Family gestionan en reposo se refieren a los detalles que se necesitan para hacer funcionar los servidores de transferencia de archivos y procesar las transferencias. AWS Transfer Family almacena los siguientes datos con cifrado completo en reposo en Amazon DynamoDB:

- Configuraciones del servidor (por ejemplo, ajustes del servidor, configuraciones de protocolo y detalles del punto final).

- Datos de autenticación del usuario, incluidas las claves públicas de SSH y los metadatos del usuario.
- Detalles de la ejecución del flujo de trabajo y configuraciones de los pasos.
- Configuraciones de conectores y credenciales de autenticación para sistemas de terceros. Estas credenciales se cifran mediante claves de cifrado AWS Transfer Family gestionadas.

Administración de claves

No puede administrar las claves de cifrado que se AWS Transfer Family utilizan para almacenar información en DynamoDB relacionada con el funcionamiento de los servidores y el procesamiento de las transferencias. Esta información incluye las configuraciones del servidor, los datos de autenticación de los usuarios, los detalles del flujo de trabajo y las credenciales del conector.

¿Qué no está cifrado?

Aunque AWS Transfer Family no controla la forma en que se cifran los datos de almacenamiento en reposo, te recomendamos configurar las ubicaciones de almacenamiento 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 AWS KMS claves (SSE-KMS).

Obtenga más información sobre cómo los servicios AWS de almacenamiento cifran los datos en reposo:

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

Administración de claves SSH y PGP en Transfer Family

En esta sección, encontrará información sobre las claves SSH, inclusive cómo generarlas y cómo rotarlas. Para obtener más información sobre el uso de Transfer Family with AWS Lambda para administrar las claves, consulte la entrada del blog [Habilitar la administración de claves de autoservicio del usuario con AWS Transfer Family y AWS Lambda](#). Para la implementación y la administración automatizadas de usuarios con varias claves SSH, consulte. [Módulos Transfer Family Terraform](#)

Note

AWS Transfer Family acepta claves RSA, ECDSA y ED25519 para la autenticación SSH.

En esta sección también se explica cómo generar y administrar las claves Pretty Good Privacy (PGP).

Para obtener una descripción general completa de todos los algoritmos de cifrado y clave compatibles, incluidas las recomendaciones para los distintos casos de uso, consulte. [Descripción general de los algoritmos clave y de cifrado](#)

Descripción general de los algoritmos clave y de cifrado

AWS Transfer Family admite diferentes tipos de algoritmos para diferentes propósitos. Saber qué algoritmos usar para su caso de uso específico ayuda a garantizar transferencias de archivos seguras y compatibles.

Referencia rápida de algoritmos

Caso de uso	Algoritmo recomendado	Cumple con FIPS	Notas
SSH/SFTP Autentic	RSA (rsa-sha2-256/512), ECDSA o ED25519	RSA: Sí, ECDSA: Sí, ED25519: No	Compatible con todos los clientes y servidores SSH
Generación de claves PGP	RSA o ECC (NIST)	Sí	Para el descifrado del flujo de trabajo
Cifrado de archivos PGP	AES-256	Sí	Determinado por el software PGP

Algoritmos de autenticación SSH

Estos algoritmos se utilizan para la SSH/SFTP autenticación entre clientes y AWS Transfer Family servidores. Elija uno de estos al generar pares de claves SSH para la autenticación de usuarios o las claves de host del servidor.

RSA (recomendado)

Compatible con todos los clientes y servidores SSH, y. FIPS-compliant Úselo con el SHA-2 hash para mejorar la seguridad:

- `rsa-sha2-256`- Recomendado para la mayoría de los casos de uso
- `rsa-sha2-512`- Opción de mayor seguridad

ED25519

Moderna y eficiente. Llaves de menor tamaño con una gran seguridad:

- `ssh-ed25519`- Rápido y seguro, pero no FIPS-compliant

ECDSA

Opción de curva elíptica. Buen equilibrio entre seguridad y rendimiento:

- `ecdsa-sha2-nistp256`- Curva estándar
- `ecdsa-sha2-nistp384`- Curva de seguridad más alta
- `ecdsa-sha2-nistp521`- La curva de seguridad más alta

Note

`ssh-rsa`Admitimos el SHA1 para las políticas de seguridad más antiguas. Para obtener más información, consulte [Algoritmos criptográficos](#).

Elegir el algoritmo SSH correcto

- Para la mayoría de los usuarios: utilice RSA con o `rsa-sha2-256` `rsa-sha2-512`
- Para cumplir con las normas FIPS: utilice los algoritmos RSA o ECDSA
- Para entornos modernos: el ED25519 ofrece una seguridad y un rendimiento excelentes

Algoritmos de cifrado y descifrado PGP

PGP (Pretty Good Privacy) utiliza dos tipos de algoritmos que funcionan juntos para cifrar y descifrar archivos en los flujos de trabajo:

1. Algoritmos de pares de claves: se utilizan para generar los pares de public/private claves para el cifrado y las firmas digitales
2. Algoritmos simétricos: se utilizan para cifrar los datos reales del archivo (los algoritmos de pares de claves cifran la clave simétrica)

Algoritmos de key pair PGP

Elija uno de estos algoritmos al generar pares de claves PGP para el descifrado del flujo de trabajo:

RSA (recomendado)

Recomendado para la mayoría de los usuarios. Ampliamente respaldado, bien establecido y FIPS-compliant. Proporciona un buen equilibrio entre seguridad y compatibilidad.

ECC (criptografía de curva elíptica)

Más eficiente que RSA con tamaños de clave más pequeños y, al mismo tiempo, mantiene una seguridad sólida:

- Curvas NIST: curvas estándar ampliamente compatibles y FIPS-compliant
- BrainPool curvas: curvas alternativas para requisitos de conformidad específicos
- Curve25519: curva moderna de alto rendimiento que ofrece una gran seguridad con un cálculo eficiente

ElGamal

Algoritmo heredado. Compatible con sistemas antiguos. Utilice RSA o ECC para las nuevas implementaciones.

Para obtener instrucciones detalladas sobre cómo generar claves PGP, consulte. [Generar claves PGP](#)

Algoritmos de cifrado simétrico PGP

Estos algoritmos cifran los datos reales de sus archivos. El algoritmo utilizado depende de cómo el software PGP haya creado el archivo PGP:

FIPS-compliant algoritmos (recomendados para entornos regulados)

- AES-128, AES-192, AES-256 - Estándar de cifrado avanzado (recomendado)
- 3DES: estándar de triple cifrado de datos (antiguo, utilice AES siempre que sea posible)

Otros algoritmos compatibles

- IDEA, CAST5, Blowfish, DES,,, TwoFish CAMELLIA-128 CAMELLIA-192 CAMELLIA-256

Note

El algoritmo simétrico no se elige directamente cuando se utilizan los AWS Transfer Family flujos de trabajo, sino que lo determina el software PGP utilizado para crear el archivo cifrado. Sin embargo, puedes configurar tu software PGP para que prefiera FIPS-compliant algoritmos similares. AES-256

Para obtener más información sobre los algoritmos simétricos compatibles, consulte [Algoritmos de cifrado simétrico compatibles](#)

Genere claves SSH para los usuarios administrados por el servicio

Puede configurar su servidor para que autentique a los usuarios aplicando el método de autenticación administrada por el servicio, con el que los nombres de usuario y las claves SSH se almacenan en el servicio. La clave pública SSH del usuario se carga en el servidor como una propiedad de usuario. El servidor utiliza esta clave como parte de un proceso de autenticación estándar basado en claves. Cada usuario puede tener varias claves SSH públicas en un mismo servidor. Para conocer los límites en la cantidad de claves que se pueden almacenar por usuario, consulte los [puntos de conexión y cuotas de AWS Transfer Family](#) en Referencia general de Amazon Web Services.

Como alternativa al método de autenticación gestionado por el servicio, puede autenticar a los usuarios mediante un proveedor de identidad personalizado, o. AWS Directory Service for Microsoft Active Directory Para obtener más información, consulte [Uso de proveedores de identidad personalizados](#) o [Uso AWS de Directory Service para Microsoft Active Directory](#).

Un servidor solo puede autenticar a los usuarios mediante un método (administrado por el servicio, servicio de directorio o proveedor de identidad personalizado), y ese método no se puede cambiar una vez creado el servidor.

Temas

- [Creación de claves SSH en macOS, Linux o Unix](#)
- [Creación de claves SSH en Microsoft Windows](#)
- [Convertir una clave SSH2 al formato de clave pública SSH](#)

Creación de claves SSH en macOS, Linux o Unix

En los sistemas operativos macOS, Linux o Unix, se utiliza el comando `ssh-keygen` para crear una clave pública SSH y una clave privada SSH, también conocidas como par de claves.

Note

En los ejemplos siguientes, no especificamos una frase de contraseña: en este caso, la herramienta le pide que introduzca la frase de contraseña y, a continuación, que la repita para verificarla. La creación de una frase de contraseña ofrece una mejor protección para la clave privada y, también, podría mejorar la seguridad general del sistema. No puede recuperar la frase de contraseña: si la olvida, debe crear una clave nueva.

Sin embargo, si va a generar una clave de host de servidor, debe especificar una frase de contraseña vacía especificando la opción `-N ""` en el comando (o pulsando **Enter** dos veces cuando se le solicite), ya que los servidores de Transfer Family no pueden solicitar una contraseña al inicio.

Creación claves SSH en un sistema operativo macOS, Linux o Unix

1. En los sistemas operativos macOS, Linux o Unix, abra una terminal de comandos.
2. AWS Transfer Family acepta RSA, ECDSA y claves. ED25519-formatted Elija el comando apropiado en función del tipo de par de claves que esté generando.

Consejo: *key_name* Sustitúyalo por el nombre real del archivo de key pair SSH.

- Para generar un par de claves RSA de 4096 bits:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Para generar un par de claves ECDSA de 521 bits (el ECDSA tiene tamaños de bits de 256, 384 y 521):

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Para generar un par de claves ED25519:

```
ssh-keygen -t ed25519 -f key_name
```

A continuación se muestra un ejemplo del resultado `ssh-keygen`.

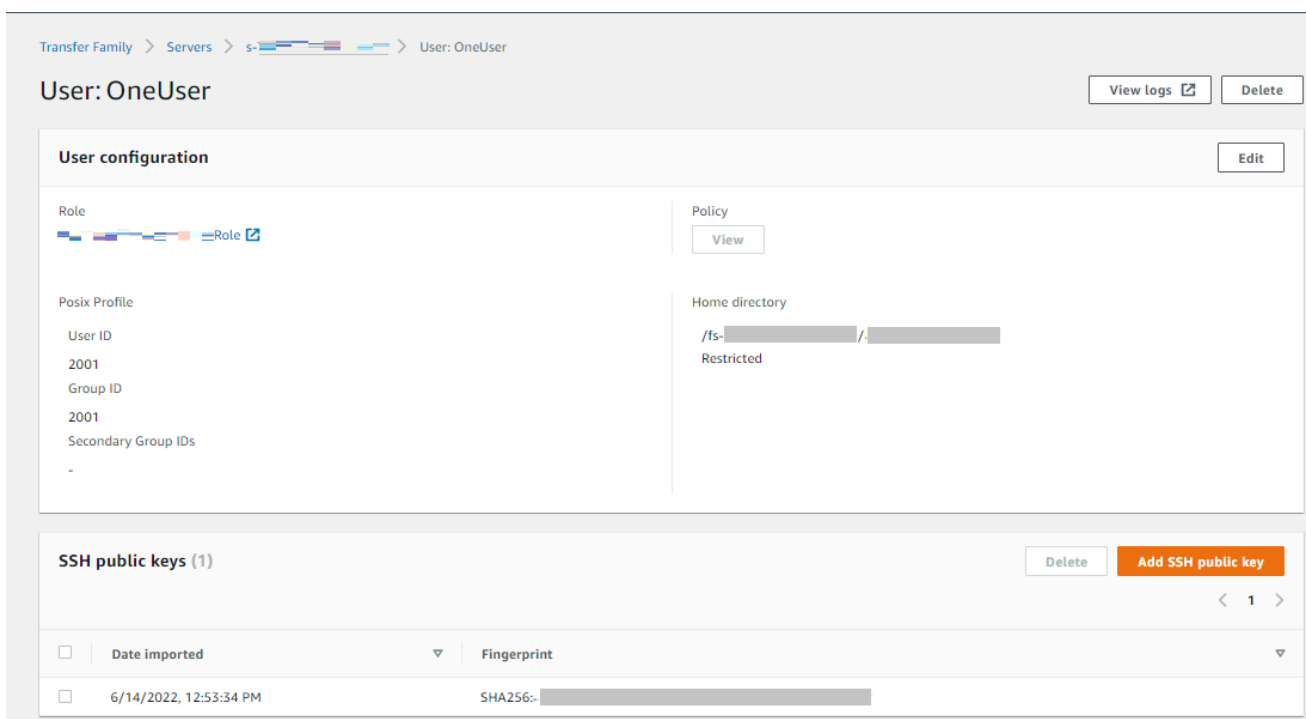
```
ssh-keygen -t rsa -b 4096 -f key_name
Generating public/private rsa key pair.

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_name.
Your public key has been saved in key_name.pub.
The key fingerprint is:
SHA256:8tDDwPmanTFcEzjTwPGETVW0GW1nVz+gtCCE8hL7PrQ bob.amazon.com
The key's randomart image is:
+---[RSA 4096]-----+
|  . . . . .E      |
|  .  =  ...      |
| . . . = ..o      |
|  . o +  oo =     |
|  + =  .S.= *     |
|  . o o ..B + o   |
|    .o+. * .      |
|    =o*+* .       |
|    ..*o*+ .      |
+-----[SHA256]-----+
```

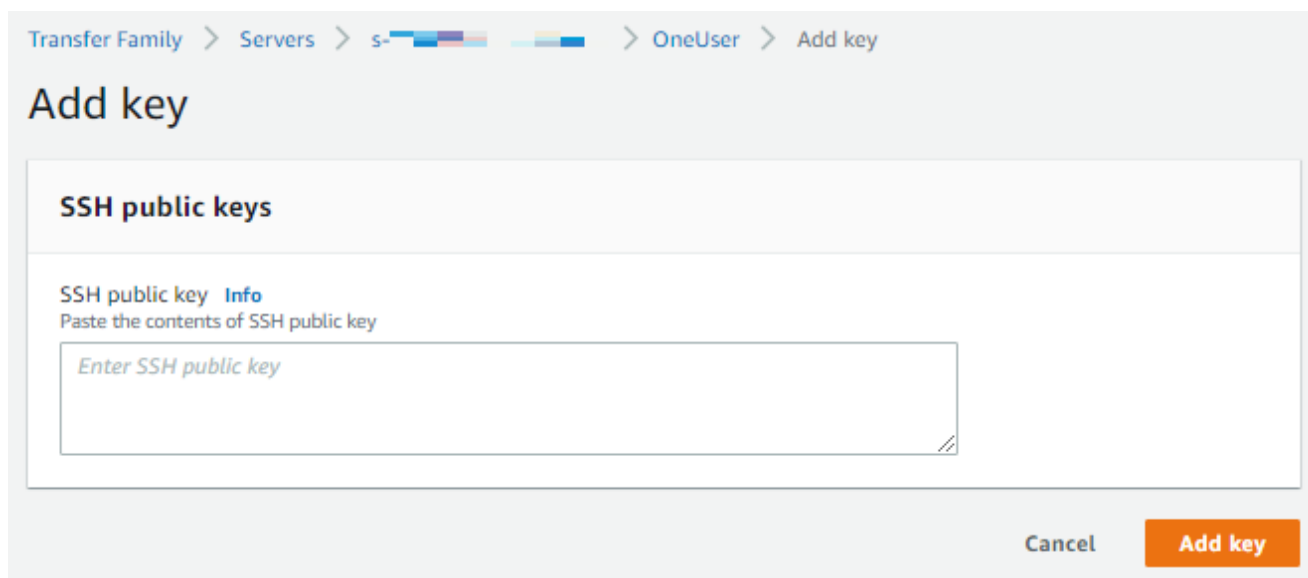
Consejo: Al ejecutar el `ssh-keygen` comando como se muestra anteriormente, crea las claves pública y privada como archivos en el directorio actual.

Tu par de claves SSH ya está listo para usarse. Siga los pasos 3 y 4 para almacenar la clave pública SSH para los usuarios gestionados por el servicio. Estos usuarios utilizan las claves cuando transfieren archivos en los puntos finales del servidor Transfer Family.

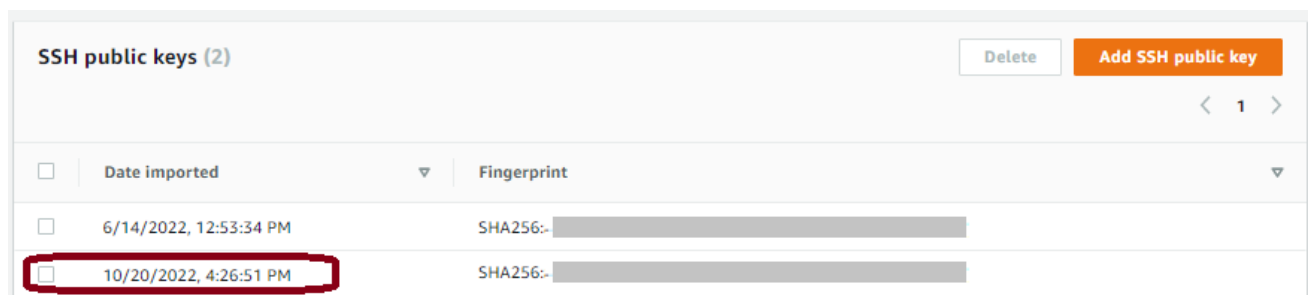
3. Desplácese hasta el archivo *key_name*.pub y ábralo.
4. Copie el texto y péguelo en la clave pública SSH del usuario administrado por el servicio.
 - a. Abra la AWS Transfer Family consola en y <https://console.aws.amazon.com/transfer/>, a continuación, seleccione Servidores en el panel de navegación.
 - b. En la página Servidores, seleccione el ID de servidor para el servidor que contiene el usuario que desea actualizar.
 - c. Seleccione el usuario para el que va a añadir una clave pública.
 - d. En el panel de claves públicas SSH, seleccione Añadir clave pública SSH.



- e. Pegue el texto de la clave pública que ha generado en el cuadro de texto de la clave pública SSH y, a continuación, seleccione Añadir clave.



La clave nueva aparece en el panel de claves públicas SSH.



SSH public keys (2)		Delete	Add SSH public key
		< 1 >	
☐	Date imported ▾	Fingerprint ▾	
☐	6/14/2022, 12:53:34 PM	SHA256:- [fingerprint]	
☐	10/20/2022, 4:26:51 PM	SHA256:- [fingerprint]	

Creación de claves SSH en Microsoft Windows

Windows incluye OpenSSH como función integrada, que puede utilizar para generar claves SSH en el mismo formato que en Linux o macOS. Como alternativa, puedes usar herramientas de terceros como el generador de claves de PuTTY (PuttyGen).

Uso del OpenSSH integrado en Windows

Las versiones recientes de Windows incluyen OpenSSH de forma predeterminada. Puede usar los mismos `ssh-keygen` comandos que se describen en la macOS/Linux sección:

1. Abra Windows PowerShell o la línea de comandos.
2. Ejecute uno de los siguientes comandos en función del tipo de clave que desee generar:
 - Para generar un par de claves RSA de 4096 bits:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Para generar un par de claves ECDSA de 521 bits:

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Para generar un par de claves ED25519:

```
ssh-keygen -t ed25519 -f key_name
```

3. Siga los mismos pasos que en la macOS/Linux sección para cargar su clave pública. AWS Transfer Family

Uso de PuttyGen (herramienta de terceros)

Algunos clientes SSH de terceros para Windows, como PuTTY, utilizan diferentes formatos de clave. PuTTY usa el PPK formato para las claves privadas. Si utilizas PuTTY o herramientas relacionadas como WinSCP, puedes usar PuttyGen para crear claves en este formato.

Note

Si en WinSCP elige un archivo de clave privada que no está en formato .ppk, ese cliente le ofrecerá convertir la clave automáticamente al formato .ppk.

[Para ver un tutorial sobre cómo crear claves SSH mediante PuttyGen, consulta el sitio web. SSH.com](#)

Convertir una clave SSH2 al formato de clave pública SSH

AWS Transfer Family solo acepta claves públicas. SSH-formatted Si tiene una clave pública SSH2, debe convertirla. Una clave pública SSH2 tiene el siguiente formato:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: "rsa-key-20160402"  
AAAAB3NzaC1yc2EAAAABJQAAAQEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI  
:  
:  
----- END SSH2 PUBLIC KEY -----
```

Una clave pública SSH tiene el siguiente formato:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

Ejecute el siguiente comando para convertir una clave SSH2-formatted pública en una clave SSH-formatted pública. `ssh2-key` Sustitúyala por el nombre de la clave SSH2 y `ssh-key` por el nombre de la clave SSH.

```
ssh-keygen -i -f ssh2-key.pub > ssh-key.pub
```

Rotar claves SSH

Por seguridad, la rotación de las claves SSH es una buena práctica que recomendamos. Normalmente, la rotación se especifica como parte de una política de seguridad y se implementa con algún mecanismo automático. En función del nivel de seguridad, para comunicaciones altamente confidenciales puede que un par de claves SSH se utilice una sola vez. Esto elimina cualquier riesgo derivado del almacenamiento de las claves. Sin embargo, es mucho más habitual almacenar las credenciales SSH durante cierto periodo de tiempo y establecer un intervalo que no suponga una carga excesiva para los usuarios. Un intervalo de tres meses es habitual.

Note

Para obtener información sobre la rotación automática de claves SSH utilizando la infraestructura como código, consulte [Módulos Transfer Family Terraform](#).

Existen dos métodos para realizar la rotación de claves SSH:

- En la consola, puede cargar una clave pública SSH nueva y eliminar una clave pública SSH existente.
- Con la API, puede actualizar los usuarios existentes mediante la [DeleteSshPublicKey](#) API para eliminar la clave pública de Secure Shell (SSH) de un usuario y la [ImportSshPublicKey](#) API para añadir una nueva clave pública de Secure Shell (SSH) a la cuenta del usuario.

Console

Cómo realizar una rotación de claves en la consola

1. Abra la AWS Transfer Family consola en. <https://console.aws.amazon.com/transfer/>
2. Navegue a la página Servidores.
3. Elija el identificador en la columna ID de servidor para ver la página Detalles del servidor.
4. En Usuarios, seleccione la casilla del usuario cuya clave pública SSH quiere rotar, luego, seleccione Acciones y, a continuación, seleccione Añadir clave para ver la página Añadir clave.

o

Seleccione el nombre de usuario para ver la página de Detalles del usuario y, a continuación, Añadir clave pública SSH para ver la página Añadir clave.

5. Introduzca la nueva clave pública de SSH y seleccione Añadir clave.



Important

El formato de la clave pública SSH depende del tipo de clave que haya generado.

- En el caso de las claves RSA, el formato es `ssh-rsa` *string*.
- En el caso de las claves ED25519, el formato es `ssh-ed25519` *string*.
- En el caso de las claves ECDSA, la clave comienza por `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384` o `ecdsa-sha2-nistp521`, según el tamaño de la clave que haya generado. A continuación, la cadena inicial va seguida de *string*, de forma similar a los demás tipos de clave.

Volverá entonces a la pantalla Detalles de usuario en cuya sección de claves SSH públicas aparecerá la nueva clave pública SSH.

6. Seleccione las casillas de verificación situadas junto a las claves que desea eliminar y seleccione Eliminar.
7. Confirme la operación de eliminación escribiendo la palabra `delete` y, a continuación, seleccione Eliminar.

API

Cómo realizar una rotación de claves mediante la API

1. En los sistemas operativos macOS, Linux o Unix, abra una terminal de comandos.
2. Recupere la clave SSH que desea eliminar al ingresar el siguiente comando. Para usar este comando, reemplace *serverID* por el ID del servidor de su servidor de Transfer Family y reemplace *username* por su nombre de usuario.

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

El comando devuelve detalles sobre el usuario. Copie el contenido del campo "SshPublicKeyId":. Tendrá que introducir este valor más tarde en este mismo procedimiento.

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":  
  "keyID",  
  "DateImported": 1621969331.072 } ],
```

3. A continuación, importe una nueva clave SSH para su usuario. Cuando se le solicite, introduzca el comando siguiente. Para usar este comando, reemplace *serverID* por el ID del servidor de su servidor de Transfer Family, reemplace *username* por su nombre de usuario, y reemplace *public-key* por la huella digital de su clave pública nueva.

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'  
  --ssh-public-key-body='public-key'
```

Si el comando se ejecuta correctamente, no se muestra ningún resultado.

4. Por último, elimine la clave anterior mediante el siguiente comando. Para usar este comando, reemplace *serverID* por el ID del servidor de su servidor de Transfer Family, reemplace *username* por su nombre de usuario, y reemplace *keyID-from-step-2* por el valor de identificador de clave que copió en el paso 2 de este procedimiento

```
aws transfer delete-ssh-public-key --server-id='serverID' --user-name='username'  
  --ssh-public-key-id='keyID-from-step-2'
```

5. (Opcional) Para confirmar que la clave anterior ya no existe, repita el paso 2.

Generar claves PGP

Puede utilizar el descifrado de Pretty Good Privacy (PGP) con los archivos que Transfer Family procesa mediante flujos de trabajo. Para utilizar el descifrado en un paso del flujo de trabajo, proporcione una clave PGP. Para obtener información detallada sobre los algoritmos clave de PGP, incluidas las recomendaciones y el cumplimiento de las normas FIPS, consulte. [Algoritmos de key pair PGP](#)

El blog sobre AWS almacenamiento tiene una entrada que describe cómo descifrar archivos de forma sencilla sin escribir ningún código mediante los flujos de trabajo gestionados por Transfer Family, [cifrar y descifrar archivos con PGP](#) y. AWS Transfer Family

El operador que utilice para generar las claves PGP dependerá del sistema operativo y de la versión del software de generación de claves que utilice.

Si utiliza Linux o Unix, utilice el instalador de paquetes para realizar la instalación de gpg. Dependiendo de su distribución de Linux, uno de los siguientes comandos debería funcionar para usted.

```
sudo yum install gnupg
```

```
sudo apt-get install gnupg
```

Para Windows o macOS, puedes descargar lo que necesites de <https://gnupg.org/download/>.

Después de instalar el software generador de claves PGP, ejecute `gpg --full-gen-key` o el comando `gpg --gen-key` para generar un par de claves.

Note

Si utiliza la versión 2.3.0 o posterior de GnuPG, debe ejecutar `gpg --full-gen-key`. Cuando se le pida el tipo de clave que desea crear, elija RSA o Elliptic Curve Cryptography (ECC, criptografía de curva elíptica). Si elige ECC, puede elegir NIST entre BrainPool y Curve25519 para la curva elíptica.

Subcomandos de **gpg** útiles

Los siguientes son algunos subcomandos útiles para gpg:

- `gpg --help`: este comando muestra las opciones disponibles y puede incluir algunos ejemplos.
- `gpg --list-keys`— Este comando muestra los detalles de todos los pares de claves que ha creado.
- `gpg --fingerprint`— Este comando muestra los detalles de todos los pares de claves, incluida la huella digital de cada clave.
- `gpg --export -a user-name`: este comando exporta la parte de la clave pública de la clave para *user-name* que se utilizó cuando se generó la clave.

Administración de claves PGP

Para administrar sus claves PGP, utilice AWS Secrets Manager.

Note

Su nombre secreto incluye su ID de servidor de Transfer Family. Esto significa que ya debe haber identificado o creado un servidor antes de poder almacenar la información de su clave PGP en AWS Secrets Manager.

Si quiere usar una clave y una frase de contraseña para todos sus usuarios, puede almacenar la información del bloque de claves PGP bajo el nombre secreto `aws/transfer/server-id/@pgp-default`, en el que *server-id* es el ID de su servidor de Transfer Family. Transfer Family usa esta clave predeterminada si no hay ninguna clave que *user-name* coincida con el usuario que ejecuta el flujo de trabajo.

Puede crear una clave para un usuario específico. En este caso, el formato del nombre secreto es `aws/transfer/server-id/user-name`, donde *user-name* coincide con el usuario que ejecuta el flujo de trabajo de un servidor Transfer Family.

Note

Puede almacenar un máximo de 3 claves privadas PGP, por servidor de Transfer Family y por usuario.

Configuración de las claves PGP para su uso con el descifrado

1. Según la versión de GPG que utilice, ejecute uno de los siguientes comandos para generar un key pair de PGP.

- Si utiliza la versión 2.3.0 de **GnuPG** o posterior, ejecute el siguiente comando:

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

Puede elegir **rsa**, si lo desea **ECC**, puede elegir una **BrainPool** o **Curve25519** para la **NIST** curva elíptica. Si se ejecuta `gpg --gen-key` en su lugar, se crea un key pair que utiliza el algoritmo de cifrado ECC Curve 25519.

- Para las versiones de **GnuPG** anteriores a la 2.3.0, puede usar el siguiente comando, ya que RSA es el tipo de cifrado predeterminado.

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

Important

Durante el proceso de generación de claves, debe proporcionar una frase de contraseña y una dirección de correo electrónico. Asegúrese de tomar nota de estos valores. Debe proporcionar la contraseña al introducir los detalles de la clave más adelante en AWS Secrets Manager este procedimiento. Además, debe proporcionar la misma dirección de correo electrónico para exportar la clave privada en el siguiente paso.

2. Ejecute el siguiente comando para exportar la clave privada. Para usar este comando, reemplace *private.pgp* por el nombre del archivo en el que se va a guardar el bloque de clave privada, y reemplace *marymajor@example.com* por la dirección de correo electrónico que utilizó al generar el par de claves.

```
gpg --output private.pgp --armor --export-secret-key marymajor@example.com
```

3. Utilícela AWS Secrets Manager para almacenar la clave PGP.
 - a. Inicie sesión en Consola de administración de AWS y abra la AWS Secrets Manager consola en <https://console.aws.amazon.com/secretsmanager/>.
 - b. En el panel de navegación izquierdo, seleccione Secretos.

- c. En la página Secretos, seleccione Almacenar un nuevo secreto.
- d. En la página Seleccionar tipo de secreto, en Tipo de secreto, seleccione Otro tipo de secreto.
- e. En la sección de Key/value parejas, selecciona la Key/valuepestaña.

- Clave: introduzca **PGPPrivateKey**.

 Note

Debe introducir la cadena **PGPPrivateKey** con precisión: no añada espacios antes o entre los caracteres.

- valor: pegue el texto de su clave privada en el campo valor. Puede encontrar el texto de la clave privada en el archivo (por ejemplo, `private.pgp`) que especificó al exportar la clave al principio de este procedimiento. La clave comienza con `-----BEGIN PGP PRIVATE KEY BLOCK-----` y termina con `-----END PGP PRIVATE KEY BLOCK-----`.

 Note

Asegúrese de que el bloque de texto contenga solo la clave privada y que no contenga también la clave pública.

- f. Seleccione Añadir fila y, en la sección de Key/value pares, elija la Key/valuepestaña.

- Clave: introduzca **PGPPassphrase**.

 Note

Debe introducir la cadena **PGPPassphrase** con precisión: no añada espacios antes o entre los caracteres.

- valor: introduzca la contraseña que utilizó al generar su par de claves PGP.

Choose secret type

Secret type [Info](#)

☐ Credentials for Amazon RDS database
 ☐ Credentials for Amazon DocumentDB database
 ☐ Credentials for Amazon Redshift cluster

☐ Credentials for other database
 ☒ Other type of secret
API key, OAuth token, other.

Key/value pairs [Info](#)

Key/value	Plaintext	
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----	Remove
PGPPassphrase	my passphrase	Remove
+ Add row		

Encryption key [Info](#)

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

[Add new key](#) [🔗](#)

Note

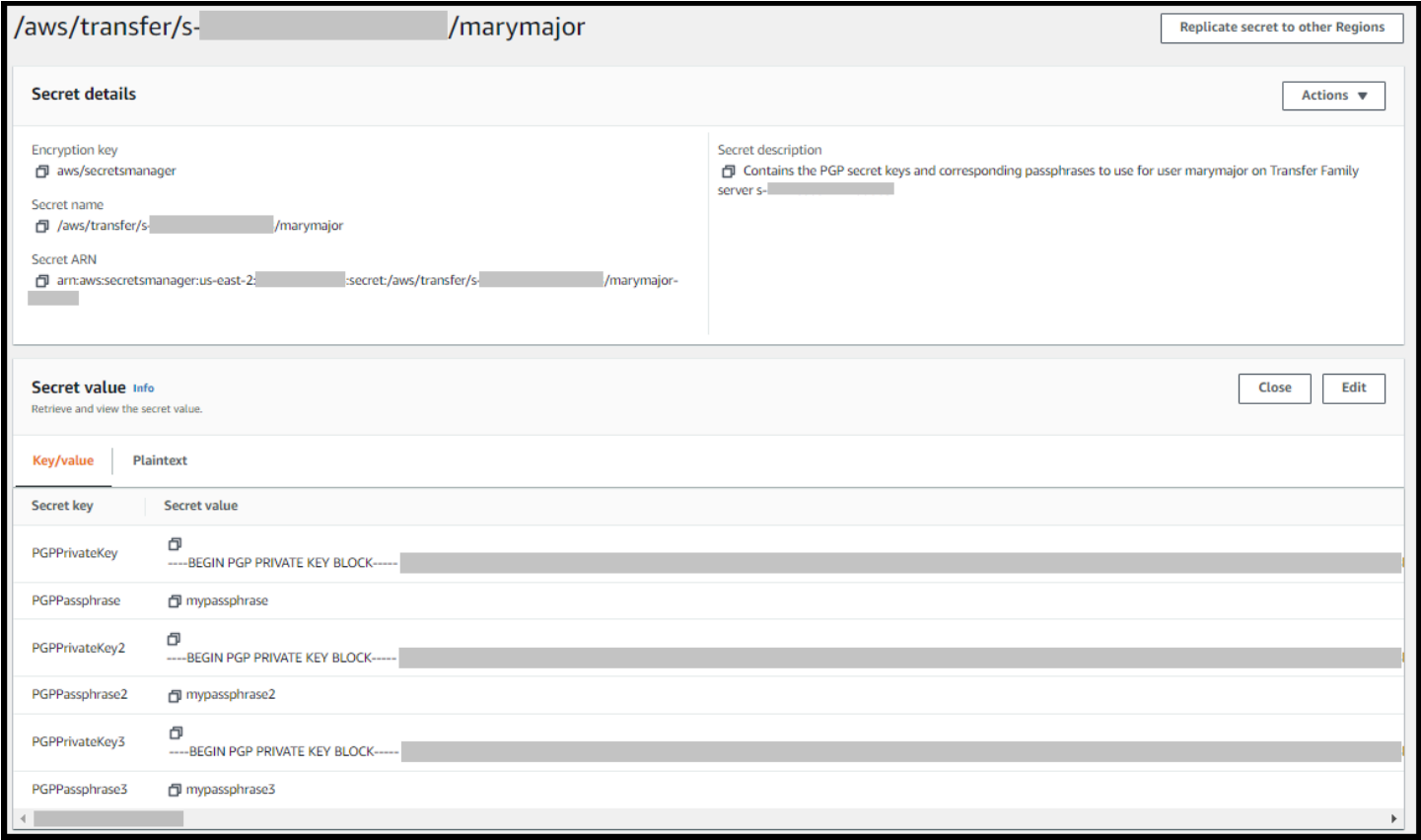
Puede agregar hasta 3 conjuntos de claves y frases de contraseña. Para añadir un segundo conjunto, añada dos filas nuevas, introduzca **PGPPrivateKey2** y **PGPPassphrase2** para las claves, y pegue otra clave privada y frase de contraseña. Para añadir un tercer conjunto, los valores de la clave deben ser **PGPPrivateKey3** y **PGPPassphrase3**.

- g. Seleccione Siguiente.
- h. En la página Configurar secreto, introduzca un nombre y una descripción para el secreto.
 - Si va a crear una clave predeterminada, es decir, una clave que pueda utilizar cualquier usuario de Transfer Family, introduzca **aws/transfer/*server-id*/@pgp-default**. Reemplace *server-id* por el ID del servidor que contiene el flujo de trabajo que tiene un paso de descifrado.
 - Si va a crear una clave para que la utilice un usuario específico de Transfer Family, introduzca **aws/transfer/*server-id*/*user-name***. Reemplace *server-id* por el ID del servidor que contiene el flujo de trabajo que tiene un paso de descifrado y reemplace

user-name por el nombre del usuario que ejecuta el flujo de trabajo. *user-name* se almacena en el proveedor de identidad que utiliza el servidor de Transfer Family.

- i. Seleccione Siguiente y acepte los valores predeterminados de la página Configurar rotación. A continuación, seleccione Siguiente.
- j. En la página de Revisión, elija Guardar para crear y almacenar el secreto.

La siguiente captura de pantalla muestra los detalles del usuario **marymajor** para un servidor de Transfer Family específico. En este ejemplo, se muestran tres claves y sus frases de contraseñas correspondientes.



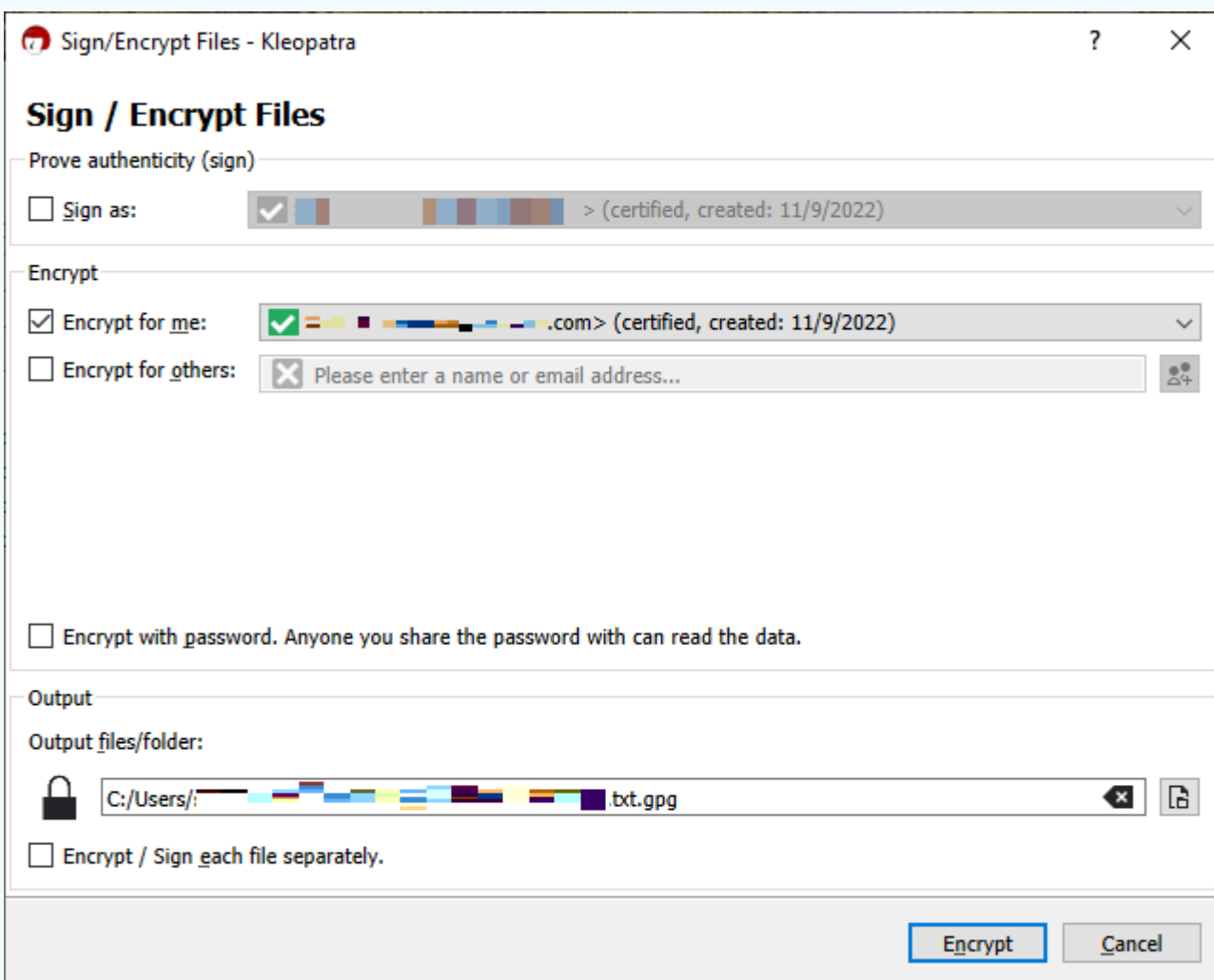
Cientes PGP admitidos

Se probaron los siguientes clientes con Transfer Family y se pueden usar para generar claves PGP y para cifrar los archivos que se pretende descifrar con un flujo de trabajo.

- Gpg4win + Kleopatra.

Note

Cuando seleccione Firmar/cifrar archivos, asegúrese de borrar la selección de Firmar como: actualmente no se admite la firma de archivos cifrados.



Si firmas el archivo cifrado e intentas subirlo a un servidor de Transfer Family con un flujo de trabajo de descifrado, recibirás el siguiente error:

Encrypted file with signed message unsupported

- Versiones principales de GnuPG: 2.4, 2.3, 2.2, 2.0 y 1.4.

Tenga en cuenta que es posible que otros clientes de PGP también funcionen, pero solo los clientes mencionados aquí se han probado con Transfer Family.

Administración de identidad y acceso para AWS Transfer Family

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Transfer Family La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración del acceso con políticas](#)
- [Cómo AWS Transfer Family funciona con IAM](#)
- [AWS Transfer Family ejemplos de políticas basadas en identidades](#)
- [AWS Transfer Family ejemplos de políticas basadas en etiquetas](#)
- [Resolución de problemas AWS Transfer Family identidad y acceso](#)
- [Los requisitos de la IAM para el gobierno organizacional](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte [Resolución de problemas AWS Transfer Family identidad y acceso](#)).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte [Cómo AWS Transfer Family funciona con IAM](#)).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte [AWS Transfer Family ejemplos de políticas basadas en identidades](#)).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la Cuenta de AWS](#) en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte [AWS Signature Version 4 para solicitudes de API](#) en la Guía del usuario de IAM.

Usuario raíz de la cuenta de AWS

Al crear una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz, que tiene acceso completo a todos los Servicios de AWS recursos. Se recomienda encarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte [¿Qué es el Centro de identidades de IAM?](#) en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte [Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte [Casos de uso para usuarios de IAM](#) en la Guía del usuario de IAM.

Roles de IAM

Un [Rol de IAM](#) es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol [cambiando de un rol de usuario a uno de IAM \(consola\)](#) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte [Métodos para asumir un rol](#) en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Administración del acceso con políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte [Información general de políticas de JSON](#) en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas integradas (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte [Selección entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe [especificar una entidad principal](#) en una política basada en recursos.

Resource-based las políticas son políticas integradas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte [Información general de Lista de control de acceso \(ACL\)](#) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte [Políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte [Políticas de control de recursos \(RCP\)](#) en la Guía del usuario de AWS Organizations .
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

Cómo AWS Transfer Family funciona con IAM

Antes de utilizar AWS Identity and Access Management (IAM) para gestionar el acceso AWS Transfer Family, debe comprender las funciones de IAM disponibles para su uso. AWS Transfer FamilyPara obtener una visión general de cómo funcionan con IAM AWS Transfer Family y otros AWS servicios, consulte los [AWS servicios que funcionan con IAM en la Guía del usuario de IAM](#).

Temas

- [AWS Transfer Family políticas basadas en identidad](#)
- [AWS Transfer Family políticas basadas en recursos](#)
- [Autorización basada en AWS Transfer Family etiquetas](#)
- [AWS Transfer Family Roles de IAM](#)

AWS Transfer Family políticas basadas en identidad

Con las políticas basadas en identidad de IAM, puede especificar las acciones permitidas o denegadas y los recursos además de las condiciones en las que se permiten o deniegan las acciones. AWS Transfer Family admite acciones, recursos y claves de condiciones específicos. Para obtener más información acerca de los elementos que utiliza en una política de JSON, consulte [Referencia de los elementos de las políticas de JSON de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

Acciones

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas AWS Transfer Family utilizan el siguiente prefijo antes de la acción: `transfer:`. Por ejemplo, para conceder a alguien permiso para crear un servidor con la operación de la API `CreateServer` de Transfer Family, debe incluir la acción `transfer:CreateServer` en la política. Las instrucciones de política deben incluir un elemento `Action` o `NotAction`. AWS Transfer Family define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones en una sola sentencia, sepárelas con comas como se indica a continuación.

```
"Action": [  
    "transfer:action1",  
    "transfer:action2"
```

Puede utilizar caracteres comodín (*) para especificar varias acciones. Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción.

```
"Action": "transfer:Describe*"
```

Para ver una lista de AWS Transfer Family acciones, consulte [las acciones definidas AWS Transfer Family en la](#) Referencia de autorización del servicio.

Recursos

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

El recurso del servidor de Transfer Family tiene el siguiente ARN.

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

Por ejemplo, para especificar un `s-01234567890abcdef` servidor de Transfer Family en la instrucción, utilice el siguiente ARN.

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

Para obtener más información sobre el formato de los ARN, consulte los [nombres de recursos de Amazon \(ARN\)](#) en la referencia de autorización del servicio o los [ARN de IAM](#) en la Guía del usuario de IAM.

Para especificar todas las instancias que pertenecen a una cuenta específica, utilice el carácter comodín (*).

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/*"
```

Algunas AWS Transfer Family acciones se realizan en varios recursos, como los que se utilizan en las políticas de IAM. En dichos casos, debe utilizar el carácter comodín (*).

```
"Resource": "arn:aws:transfer*:123456789012:server/*"
```

En algunos casos, debe especificar más de un tipo de recurso, por ejemplo, si crea una política que permita el acceso a los servidores y usuarios de Transfer Family. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

Para ver una lista de AWS Transfer Family recursos, consulte los [tipos de recursos definidos AWS Transfer Family en la](#) Referencia de autorización de servicios.

Claves de condición

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para

ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del usuario de IAM.

AWS Transfer Family define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver una lista de claves de AWS Transfer Family condición, consulte las [claves de condición AWS Transfer Family](#) en la Referencia de autorización de servicio.

Ejemplos

Para ver ejemplos de políticas AWS Transfer Family basadas en la identidad, consulte. [AWS Transfer Family ejemplos de políticas basadas en identidades](#) Para conocer las políticas de IAM específicas de los puntos finales de la VPC, consulte. [Limitar el acceso a los terminales de VPC para los servidores Transfer Family](#)

AWS Transfer Family políticas basadas en recursos

Resource-based las políticas son documentos de políticas de JSON que especifican qué acciones puede realizar un responsable específico en el AWS Transfer Family recurso y en qué condiciones. Amazon S3 admite políticas de permisos basadas en recursos para Amazon S3. *buckets* Resource-based las políticas le permiten conceder permisos de uso a otras cuentas por recurso. También puede usar una política basada en recursos para permitir que un AWS servicio acceda a su Amazon S3. *buckets*

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la [entidad principal de una política basada en recursos](#). Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Si el principal y el recurso están en AWS cuentas diferentes, también debe conceder permiso a la entidad principal para acceder al recurso. Conceda permiso asociando a la entidad una política basada en identidades. Sin embargo, si la política basada en recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de AWS Identity and Access Management .

El servicio Amazon S3 solo admite un tipo de política basada en recursos denominada *bucket* política, que se adjunta a. *bucket* Esta política define las entidades principales (cuentas, usuarios, roles y usuarios federados) que pueden realizar acciones en el objeto.

Ejemplos

Para ver ejemplos de políticas AWS Transfer Family basadas en recursos, consulte [AWS Transfer Family ejemplos de políticas basadas en etiquetas](#)

Autorización basada en AWS Transfer Family etiquetas

Puede adjuntar etiquetas a AWS Transfer Family los recursos o pasarles etiquetas en una solicitud AWS Transfer Family. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `transfer:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Para obtener información sobre cómo utilizar las etiquetas para controlar el acceso a AWS Transfer Family los recursos, consulte [AWS Transfer Family ejemplos de políticas basadas en etiquetas](#).

AWS Transfer Family Roles de IAM

Un [rol de IAM](#) es una entidad de tu AWS cuenta que tiene permisos específicos.

Usar credenciales temporales con AWS Transfer Family

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen llamando a operaciones de AWS STS API como [AssumeRole](#) o [GetFederationToken](#).

AWS Transfer Family admite el uso de credenciales temporales.

AWS Transfer Family ejemplos de políticas basadas en identidades

De forma predeterminada, los usuarios y los roles de IAM no tienen permiso para crear, ver ni modificar recursos de AWS Transfer Family. Tampoco pueden realizar tareas con la AWS API Consola de administración de AWS AWS CLI, o. Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe asociar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de JSON de ejemplo, consulte [Creación de políticas en la pestaña JSON](#) en la Guía del usuario de AWS Identity and Access Management.

Temas

- [Prácticas recomendadas sobre las políticas](#)

- [Uso de AWS Transfer Family consola](#)
- [Permitir a los usuarios consultar sus propios permisos](#)

Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear AWS Transfer Family recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de tarea](#) en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte [Validación de políticas con el Analizador de acceso de IAM](#) en la Guía del usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte [Acceso seguro a la API con MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

Uso de AWS Transfer Family consola

Para acceder a la AWS Transfer Family consola, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los AWS Transfer Family recursos de su AWS cuenta. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política. Para obtener más información, consulte [Adición de permisos a un usuario](#) en la Guía del usuario de AWS Identity and Access Management .

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

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



```

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

```

AWS Transfer Family ejemplos de políticas basadas en etiquetas

Los siguientes son ejemplos de cómo controlar el acceso a AWS Transfer Family los recursos en función de las etiquetas.

Uso de etiquetas para controlar el acceso a AWS Transfer Family recursos

Las condiciones de las políticas de IAM forman parte de la sintaxis que se utiliza para especificar los permisos de los recursos de AWS Transfer Family . Puede controlar el acceso a AWS Transfer Family los recursos (como los usuarios, los servidores, los roles y otras entidades) en función de las etiquetas de esos recursos. Las etiquetas son pares de clave-valor. Para obtener más información sobre el etiquetado de recursos, consulte [Etiquetar AWS recursos](#) en Referencia general de AWS

En AWS Transfer Family, los recursos pueden tener etiquetas y algunas acciones pueden incluirlas. Cuando crea una política de IAM, puede utilizar claves de condición de etiqueta para controlar lo siguiente:

- Qué usuarios pueden realizar acciones en un AWS Transfer Family recurso, en función de las etiquetas que tenga el recurso.
- Las etiquetas que se pueden pasar en la solicitud de una acción.

- Si se pueden utilizar claves de etiqueta específicas en una solicitud.

Al utilizar el control de acceso basado en etiquetas, puede aplicar un control más preciso que a nivel de API. También puede aplicar un control más dinámico que mediante el control de acceso basado en recursos. Puede crear políticas de IAM que permitan o no una operación basada en las etiquetas que se proporcionan en la solicitud (etiquetas de solicitud). También puede crear políticas de IAM basadas en las etiquetas del recurso en el que se está operando (etiquetas de recurso). En general, las etiquetas de recursos son para las etiquetas que ya están en los recursos, mientras que las etiquetas de solicitud son para cuando se añaden etiquetas a un recurso o se quitan etiquetas de este.

Para conocer la sintaxis y la semántica completa de las claves de condición de las etiquetas, consulte [Control del acceso a los recursos de AWS mediante etiquetas de recursos](#) en la Guía del usuario de IAM. Para obtener más información sobre cómo especificar las políticas de IAM con la API Gateway, consulte [Control access to an API with IAM permissions \(Controlar el acceso a una API con permisos de IAM\)](#) en la Guía para desarrolladores de API Gateway.

Ejemplo 1: Denegar acciones en función de etiquetas de recursos

Puede denegar la realización de una acción en un recurso basándose en las etiquetas. El siguiente ejemplo de política deniega las operaciones TagResource, UntagResource, StartServer, StopServer, DescribeServer y DescribeUser, si el recurso de usuario o servidor está etiquetado con la clave stage y el valor prod.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "transfer:TagResource",
        "transfer:UntagResource",
        "transfer:StartServer",
        "transfer:StopServer",
        "transfer:DescribeServer",
        "transfer:DescribeUser"
      ],
      "Resource": "*",
      "Condition": {
```

```

        "StringEquals": {
            "aws:ResourceTag/stage": "prod"
        }
    }
}

```

Ejemplo 2: Permitir acciones en función de etiquetas de recursos

Puede permitir la realización de una acción en un recurso basándose en las etiquetas. El siguiente ejemplo de política permite realizar las operaciones TagResource, UntagResource, StartServer, StopServer, DescribeServer y DescribeUser, y si el recurso de usuario o servidor está etiquetado con la clave stage y el valor prod.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "transfer:TagResource",
        "transfer:UntagResource",
        "transfer:StartServer",
        "transfer:StopServer",
        "transfer:DescribeServer",
        "transfer:DescribeUser"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/stage": "prod"
        }
      }
    }
  ]
}

```

Ejemplo 3: denegar la creación de un usuario o servidor en función de las etiquetas de solicitud

El siguiente ejemplo contiene dos instrucciones. La primera sentencia deniega la operación `CreateServer` en todos los recursos si la clave del centro de costos de la etiqueta no tiene ningún valor.

La segunda afirmación deniega la operación `CreateServer` si la clave del centro de costo de la etiqueta contiene cualquier otro valor además de 1, 2 o 3.

Note

Esta política sí permite crear o eliminar un recurso que contenga una clave llamada `costcenter` y un valor de 1, 2 o 3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "transfer:CreateServer"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/costcenter": "true"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "transfer:CreateServer",
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAnyValue:StringNotEquals": {
          "aws:RequestTag/costcenter": [
```

```
    "1",  
    "2",  
    "3"  
  ]  
}  
}  
}  
]  
}
```

Resolución de problemas AWS Transfer Family identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con un AWS Transfer Family IAM.

Temas

- [No estoy autorizado a realizar ninguna acción en AWS Transfer Family](#)
- [No estoy autorizado a realizar lo siguiente: PassRole](#)
- [Quiero permitir que personas ajenas a mi AWS cuenta para acceder a mi AWS Transfer Family recursos](#)

No estoy autorizado a realizar ninguna acción en AWS Transfer Family

Si Consola de administración de AWS le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM, mateojackson, intenta utilizar la consola para ver detalles sobre una *widget*, pero no tiene permisos `transfer:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:  
transfer:GetWidget on resource: my-example-widget
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *my-example-widget* mediante la acción `transfer;:GetWidget`.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS Transfer Family.

Algunos Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS Transfer Family. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

En el siguiente ejemplo de política se incluye el permiso para transferir un rol a AWS Transfer Family. **123456789012** Sustitúyalo por el ID de su cuenta de AWS y **MyTransferRole** por el nombre real de su función de IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/MyTransferRole",
      "Effect": "Allow"
    }
  ]
}
```

Quiero permitir que personas ajenas a mi AWS cuenta para acceder a mi AWS Transfer Family recursos

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si AWS Transfer Family es compatible con estas funciones, consulte [Cómo AWS Transfer Family funciona con IAM](#).
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte [Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en](#) la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta [Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

Los requisitos de la IAM para el gobierno organizacional

AWS Transfer Family proporciona claves de condición de IAM que permiten restringir las configuraciones de recursos en cualquier política de IAM. Estas claves de condición se pueden usar en políticas basadas en la identidad asociadas a los usuarios o funciones, o en las políticas de control de servicios (SCP) para el gobierno organizacional.

Las políticas de control de servicios son políticas de IAM que se aplican a toda AWS la organización y proporcionan barreras preventivas en varias cuentas. Cuando se utilizan en los SCP, estas claves de condición ayudan a hacer cumplir los requisitos de seguridad y conformidad en toda la organización.

Véase también

- [Acciones, recursos y claves de condición de Transfer Family](#)
- [Políticas de control de servicios \(SCP\)](#)
- Vea [este vídeo](#) que describe cómo hacer cumplir las barandillas preventivas mediante políticas de control de servicios

Claves de condición disponibles

AWS Transfer Family admite las siguientes claves de condición para su uso en las políticas de IAM:

`transfer:RequestServerEndpointType`

Restringe la creación y las actualizaciones del servidor en función del tipo de punto final (PUBLIC, VPC, VPC_ENDPOINT). Se suele utilizar para evitar que los puntos finales estén orientados al público.

`transfer:RequestServerProtocols`

Restringe la creación y las actualizaciones de servidores en función de los protocolos compatibles (SFTP, FTPS, FTP, AS2).

`transfer:RequestServerDomain`

Restringe la creación de servidores en función del tipo de dominio (S3, EFS).

`transfer:RequestConnectorProtocol`

Restringe la creación de conectores según el protocolo (AS2, SFTP).

Acciones admitidas

Las claves de condición se pueden aplicar a las siguientes acciones: AWS Transfer Family

- `CreateServer`: Soporta `RequestServerEndpointType` y `RequestServerDomain` condiciona las claves `RequestServerProtocols`
- `UpdateServer`: Soporta `RequestServerEndpointType` y `RequestServerProtocols` condiciona las claves
- `CreateConnector`: Soporta la clave de `RequestConnectorProtocol` condición

Ejemplo de política SCP

El siguiente ejemplo de SCP impide la creación de AWS Transfer Family servidores públicos en toda la organización:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyPublicTransferServers",
    "Effect": "Deny",
    "Action": ["transfer:CreateServer", "transfer:UpdateServer"],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "transfer:RequestServerEndpointType": "PUBLIC"
      }
    }
  }]
}
```

Validación de conformidad para AWS Transfer Family

Third-party los auditores evalúan la seguridad y el cumplimiento AWS Transfer Family como parte de varios programas de cumplimiento. AWS Esto incluye SOC, PCI, HIPAA y otros. Para ver la lista completa, consulte [AWS los servicios incluidos en el ámbito de aplicación por programa de conformidad](#).

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte [AWS los servicios incluidos en el ámbito de aplicación por programa de cumplimiento](#). Para obtener información general, consulte [Programas de conformidad de AWS](#).

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descargar informes en AWS Artifact](#).

Su responsabilidad de conformidad al AWS Transfer Family 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:

- [Guías de inicio rápido sobre seguridad y cumplimiento](#): estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- Documento técnico [sobre cómo diseñar una arquitectura basada en la seguridad y el cumplimiento de la HIPAA: este documento técnico describe cómo](#) las empresas pueden utilizarlo para crear aplicaciones. AWS HIPAA-compliant
- [Recursos de conformidad de AWS](#): este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- [AWS Config](#)— Este AWS servicio evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- [AWS Security Hub CSPM](#)— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Transfer Family

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS 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, puede 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.

AWS Transfer Family admite hasta 3 zonas de disponibilidad y está respaldado por una flota redundante y con escalado automático para sus solicitudes de conexión y transferencia.

Para todos los terminales de Transfer Family:

- La Zone-level redundancia de disponibilidad está integrada en el servicio.
- Hay flotas redundantes para cada zona de disponibilidad.
- Esta redundancia se proporciona automáticamente.

 Note

Para los puntos finales de una Nube Privada Virtual (VPC), es posible proporcionar una única subred. Sin embargo, le recomendamos que cree puntos de conexión en varias zonas de disponibilidad dentro de su VPC para reducir el riesgo de interrupciones en el servicio durante las interrupciones de la zona de disponibilidad.

Véase también

- Para obtener más información sobre cómo crear servidores Transfer Family en una VPC, consulte [Creación de un servidor en una nube privada virtual \(VPC\)](#)
- Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte la [infraestructura AWS global](#).
- Para ver un ejemplo sobre cómo lograr una mayor redundancia y minimizar la latencia de la red mediante el Latency-based enrutamiento, consulte la entrada del blog [Minimice la latencia de la red con sus AWS Transfer Family servidores](#).

Cree una conexión privada entre una VPC y AWS Transfer Family API

Puede establecer una conexión privada entre su VPC y las AWS Transfer Family API mediante la creación de un punto final de VPC de interfaz, con la tecnología de [AWS PrivateLink](#). Puede acceder a AWS Transfer Family las API como si estuviera en su VPC, sin utilizar una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión Direct AWS Connect. Las instancias de su VPC no necesitan direcciones IP públicas para comunicar con las API de AWS Transfer Family .

Creemos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Para obtener más información, consulte [Acceder a AWS los servicios AWS PrivateLink](#) en la AWS PrivateLink Guía. Antes de configurar un punto final de VPC de interfaz para AWS Transfer Family las API, consulte las [consideraciones](#) de la AWS PrivateLink guía.

Control del acceso mediante políticas de puntos finales de VPC

De forma predeterminada, se permite el acceso total a AWS Transfer Family las API a través del punto final. Puede controlar el acceso al punto de conexión de la interfaz mediante políticas de punto

de conexión de VPC. Puede adjuntar una política de punto final a su punto final de VPC que controle el acceso a las AWS Transfer Family API. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para más información, consulte [Control del acceso a los servicios con puntos de enlace de la VPC](#) en la Guía del usuario de Amazon VPC.

El siguiente es un ejemplo de una política de puntos finales para AWS Transfer Family las API. Cuando se adjunta a un punto final, esta política otorga acceso a todas las acciones de las AWS Transfer Family API en todos los recursos, excepto a las que están etiquetadas con la clave `Environment` y el valor `Test`.

```
{
  "Statement": [{
    "Effect": "Deny",
    "Action": "transfer:StartFileTransfer",
    "Principal": "*",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Environment": "Test"
      }
    }
  }, {
    "Effect": "Allow",
    "Action": "transfer:*",
    "Principal": "*",
    "Resource": "*"
  }]
}
```

Cree un punto final de VPC de interfaz para AWS Transfer Family API

Puede crear un punto final de VPC para AWS Transfer Family las API mediante la consola de Amazon VPC o la interfaz de línea de AWS comandos ().AWS CLI Para obtener más información, consulte [Create a VPC endpoint](#) (Creación de un punto de conexión de VPC) en la Guía de AWS PrivateLink.

Cree un punto final de VPC para AWS Transfer Family las API con uno de los siguientes nombres de servicio:

- `com.amazonaws.region.transfer`
- `com.amazonaws.region.transfer-fips`— Crear un punto final de VPC de interfaz que cumpla con la norma federal de procesamiento de información (FIPS), publicación 140-3, del gobierno de EE. UU.

Si habilita el DNS privado para el punto final, puede realizar solicitudes de API a las AWS Transfer Family API utilizando su nombre de DNS predeterminado para la región, por ejemplo. `transfer.us-east-1.amazonaws.com`

Seguridad de la infraestructura en AWS Transfer Family

Como servicio gestionado, AWS Transfer Family 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 AWS Transfer Family 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.
- Paquetes de cifrado con perfecto secreto directo (PFS), como el DHE (Ephemeral) o el ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Evite colocar los NLB y los NAT delante de AWS Transfer Family servidores

Note

Los servidores configurados con los protocolos FTP y FTPS solo permiten una configuración con una VPC: no hay ningún punto final público disponible para ello. FTP/FTPS

Muchos clientes configuran un Network Load Balancer (NLB) para enrutar el tráfico a su servidor. AWS Transfer Family Por lo general, lo hacen porque crearon su servidor antes de que AWS se les ofreciera una forma de acceder a él desde su VPC y desde Internet, o para admitir FTP en Internet. Esta configuración no solo aumenta los costes para los clientes, sino que también puede provocar otros problemas, que se describen en esta sección.

Las pasarelas NAT son un componente obligatorio cuando los clientes se conectan desde la red privada de un cliente a través de un firewall corporativo. Sin embargo, debe tener en cuenta que cuando muchos clientes están detrás de la misma puerta de enlace NAT, esto puede afectar al rendimiento y a los límites de conexión. Si hay un NLB o NAT en la ruta de comunicación entre el cliente y el servidor FTP o FTPS, el servidor no puede reconocer con precisión la dirección IP del cliente, ya que solo AWS Transfer Family ve la dirección IP del NLB o NAT.

Si utiliza la configuración de un servidor Transfer Family detrás de un NLB, le recomendamos que se traslade a un punto final de VPC y utilice una dirección IP elástica en lugar de utilizar un NLB. Cuando utilice puertas de enlace NAT, tenga en cuenta las limitaciones de conexión que se describen a continuación.

Si utiliza el protocolo FTPS, esta configuración no solo reduce su capacidad de auditar quién accede a su servidor, sino que también puede afectar al rendimiento. AWS Transfer Family utiliza la dirección IP de origen para dividir las conexiones en nuestro plano de datos. En el caso de FTPS, esto significa que, en lugar de tener 10 000 conexiones simultáneas, los servidores Transfer Family con puertas de enlace NLB o NAT en la ruta de comunicación están limitados a solo 300 conexiones simultáneas.

Si bien recomendamos evitar los balanceadores de carga de red delante de AWS Transfer Family los servidores, si la implementación de FTP o FTPS requiere un NLB o NAT en la ruta de comunicación del cliente, siga estas recomendaciones:

- En el caso de un NLB, utilice el puerto 21 para las comprobaciones de estado, en lugar de los puertos 8192-8200.
- Para el AWS Transfer Family servidor, habilite la reanudación de la sesión TLS mediante la configuración. `TlsSessionResumptionMode = ENFORCED`

Note

Este es el modo recomendado, ya que proporciona una seguridad mejorada:

- Requiere que los clientes utilicen la reanudación de la sesión TLS para las conexiones posteriores.

- Ofrece garantías de seguridad más sólidas al garantizar la coherencia de los parámetros de cifrado.
 - Ayuda a prevenir posibles ataques de degradación.
 - Mantiene el cumplimiento de los estándares de seguridad a la vez que optimiza el rendimiento.
- Si es posible, deje de usar un NLB para aprovechar al máximo los límites de AWS Transfer Family rendimiento y conexión.

Para obtener más información sobre las alternativas de NLB, póngase en contacto con el equipo de gestión de AWS Transfer Family productos a través de AWS Support. Para obtener más información sobre cómo mejorar su postura de seguridad, consulte la entrada del blog [Seis consejos para mejorar la seguridad de su AWS Transfer Family servidor](#).

Seguridad de la infraestructura de conectividad de VPC

Los conectores SFTP con salida de VPC proporcionan una seguridad de infraestructura mejorada mediante el aislamiento de la red y la conectividad privada:

Ventajas del aislamiento de la red

- Tráfico de red privada: todo el tráfico de los conectores a los servidores SFTP privados permanece dentro de la VPC y nunca pasa por la Internet pública.
- Salida controlada: en el caso de los puntos finales públicos a los que se accede mediante VPC, el tráfico se enruta a través de las puertas de enlace NAT, lo que le permite controlar las direcciones IP de salida y las políticas de red.
- Controles de seguridad de VPC: aproveche los grupos de seguridad de VPC, las ACL de red y las tablas de enrutamiento existentes para controlar el acceso a la red de los conectores.
- Conectividad híbrida: acceda a los servidores SFTP locales a través de conexiones VPN o Direct Connect establecidas sin exposición adicional a Internet.

Resource Gateway: consideraciones de seguridad

Las pasarelas de recursos proporcionan puntos de entrada seguros para el acceso a los Cross-VPC recursos:

- Multi-AZ implementación: las pasarelas de recursos requieren subredes en al menos dos zonas de disponibilidad para una alta disponibilidad y tolerancia a errores.
- Controles de grupos de seguridad: configure los grupos de seguridad para restringir el acceso a los puertos SFTP (normalmente el puerto 22) únicamente desde fuentes autorizadas.
- Ubicación de subredes privadas: implemente pasarelas de recursos en subredes privadas cuando se conecte a servidores SFTP privados para mantener el aislamiento de la red.
- Límites de conexión: cada Resource Gateway admite hasta 350 conexiones simultáneas con un tiempo de espera de 350 segundos para las conexiones TCP.

Agregue un cortafuegos de aplicaciones web

AWS WAF es un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las API de los ataques. Le permite configurar un conjunto de reglas denominadas lista de control de acceso web (Web ACL) que permiten, bloquean o cuentan solicitudes web en función de las reglas y condiciones de seguridad web personalizables que defina. Para obtener más información, consulte [AWS WAF Utilización para proteger las API](#).

Para añadir AWS WAF

1. Abra la consola de API Gateway en <https://console.aws.amazon.com/apigateway/>.
2. En el panel de navegación de las API y, a continuación, elija su plantilla de proveedor de identidades personalizada.
3. Seleccione Etapas.
4. En el panel Etapas, seleccione el nombre de la etapa.
5. En el panel Editor de etapas, seleccione la pestaña Configuración.
6. Realice una de las siguientes acciones:
 - En Web application firewall (WAF), para Web ACL, seleccione la web ACL que desea asociar a esta etapa.
 - Si la ACL web que necesita no existe, tendrá que crear una de la siguiente manera:
 1. Seleccione Crear ACL web.
 2. En la página de inicio AWS del servicio WAF, elija Crear ACL web.
 3. En Detalles de la ACL web, en Nombre, escriba el nombre de la ACL web.
 4. En Reglas, elija Agregar reglas y, a continuación, elija Agregar mis propias reglas y grupos de reglas.

5. En Tipo de regla, seleccione conjunto de direcciones IP para identificar una lista específica de direcciones IP.
 6. En Regla, introduzca el nombre de la regla.
 7. Para el Conjunto de IP, elija un conjunto de IP existente. Para crear un conjunto de IP, consulte [Creating an IP set](#).
 8. Para que la dirección IP se utilice como dirección de origen, seleccione la dirección IP en el encabezado.
 9. En el Nombre del campo de encabezado, introduzca SourceIP.
 10. En Posición dentro del encabezado, elija Primera dirección IP.
 11. En Reserva para una dirección IP faltante, seleccione Coincidencia o No coincidencia en función de cómo quiera gestionar una dirección IP no válida (o faltante) en el encabezado.
 12. En Acción, elija la acción del conjunto de direcciones IP.
 13. Para la acción de ACL web predeterminada para las solicitudes que no coincidan con ninguna regla, elija Permitir o Bloquear y, a continuación, haga clic en Siguiente.
 14. Para los pasos 4 y 5, seleccione Siguiente.
 15. En Revisar y crear, revise sus opciones y, a continuación, elija Crear ACL web.
7. Elija Save changes (Guardar cambios).
 8. Elija Recursos.
 9. Para Acciones, elija Implementar API.

Para obtener información sobre el grado de seguridad de Transfer Family con un firewall de aplicaciones AWS web, consulte [Proteger Transfer Family con un firewall de AWS aplicaciones y Amazon API Gateway](#) en el blog AWS de almacenamiento.

Cross-service confusa prevención de diputados

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. Cross-service la suplantación de identidad puede producirse cuando un servicio (el servicio de llamadas) llama a otro servicio (el servicio al que se llama). El servicio de llamadas que se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente a los que de otra manera no tendría permiso para acceder. Para evitarlo, AWS

proporciona herramientas que le 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. Para obtener una descripción detallada de este problema, consulte [el problema del suplente confuso](#) en la Guía del usuario de IAM.

Recomendamos 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 AWS Transfer Family tiene para el recurso. Si se utilizan ambas claves contextuales de condición global, el valor `aws:SourceAccount` y la cuenta del valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilicen en la misma declaración de política.

La forma más eficaz de protegerse contra el problema del suplente confuso es utilizar el nombre de recurso de Amazon (ARN) exacto del recurso que desea permitir. Si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con caracteres comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:transfer::region::account-id:server/*`.

AWS Transfer Family utiliza los siguientes tipos de funciones:

- **Función de usuario:** permite a los usuarios gestionados por el servicio acceder a los recursos de Transfer Family necesarios. AWS Transfer Family asume esta función en el contexto del ARN de un usuario de Transfer Family.
- **Rol de acceso:** proporciona acceso únicamente a los archivos de Amazon S3 que se están transfiriendo. Para las transferencias AS2 entrantes, el rol de acceso utiliza el nombre de recurso de Amazon (ARN) para el acuerdo. Para las transferencias AS2 salientes, el rol de acceso utiliza el ARN para el conector.
- **Rol de invocación:** para usar con Amazon API Gateway como proveedor de identidad personalizado del servidor. Transfer Family asume este rol en el contexto de un ARN de servidor de Transfer Family.
- **Función de registro:** se utiliza para registrar entradas en Amazon CloudWatch. Transfer Family utiliza este rol para registrar los detalles de éxito y error junto con la información sobre las transferencias de archivos. Transfer Family asume este rol en el contexto de un ARN de servidor de Transfer Family. Para las transferencias AS2 salientes, el rol de acceso utiliza el ARN del conector.
- **Rol de ejecución:** permite a un usuario de Transfer Family llamar e iniciar flujos de trabajo. Transfer Family asume este rol en el contexto de un ARN de flujo de trabajo de Transfer Family.

Para obtener más información, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.

 Note

En los siguientes ejemplos, sustituya cada uno *user input placeholder* por su propia información.

 Note

En nuestros ejemplos, utilizamos tanto `ArnLike` como `ArnEquals`. Funcionalmente son idénticos y, por lo tanto, puede utilizar cualquiera de los dos al crear sus políticas. La documentación de Transfer Family utiliza `ArnLike` cuando la condición contiene un carácter comodín, y utiliza `ArnEquals` para indicar una condición de coincidencia exacta.

AWS El rol de usuario de Transfer Family, prevención de problemas entre servicios

En el siguiente ejemplo de política, se permite que cualquier servidor de la cuenta asuma el rol.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/"
        }
      }
    }
  ]
}
```

```

    }
  }
]
}

```

En el siguiente ejemplo de política se permite que cualquier usuario de un servidor específico asuma el rol.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/server-id/"
        }
      }
    }
  ]
}

```

En el siguiente ejemplo de política se permite que cualquier usuario específico de un servidor específico asuma el rol.

```

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

```

```

    "Effect": "Allow",
    "Principal": {
      "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:user/server-id/user-name"
      }
    }
  }
]
}

```

AWS Función de flujo de trabajo de Transfer Family, prevención policial confusa entre servicios

En el siguiente ejemplo de política, se permite que cualquier flujo de trabajo de la cuenta asuma el rol.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-
west-2:111122223333:workflow/*"
        }
      }
    }
  ]
}

```

```
    ]
  }
}
```

La política del ejemplo siguiente permite que un flujo específico de trabajo asuma el rol.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-
west-2:111122223333:workflow/workflow-id"
        }
      }
    }
  ]
}
```

AWS El papel de Transfer Family, conector entre servicios, policía confusa, prevención

El siguiente ejemplo de política permite que cualquier conector de la cuenta asuma la función.

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

```

        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "123456789012"
            },
            "ArnLike": {
                "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/*"
            }
        }
    }
]
}

```

El siguiente ejemplo de política permite que un conector específico asuma la función.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/connector-id"
                }
            }
        }
    ]
}

```

AWS Transfer Family: función de registro e invocación, prevención adjunta confusa entre servicios

Note

Los siguientes ejemplos se pueden utilizar tanto en los roles de registro como en los de invocación.

En estos ejemplos, puede eliminar los detalles del ARN de un flujo de trabajo si el servidor no tiene ningún flujo de trabajo adjunto.

El siguiente ejemplo logging/invoction de política permite que cualquier servidor (y flujo de trabajo) de la cuenta asuma la función.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```


El siguiente ejemplo logging/invoke de política permite que un servidor (y un flujo de trabajo) específicos asuma la función.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificServerWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/server-id",
            "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-id"
          ]
        }
      }
    }
  ]
}
```

AWS políticas administradas para AWS Transfer Family

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. [Crear políticas gestionadas por el cliente AWS Identity and Access Management \(IAM\)](#) que proporcionen a tu equipo solo los permisos que necesita requiere tiempo y experiencia. 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 administradas de AWS, consulte [Políticas administradas de AWS](#) en la Guía del usuario de IAM. Para obtener una lista detallada de todas las políticas AWS administradas, consulta la [guía de referencia de políticas AWS administradas](#).

AWS los servicios mantienen y AWS actualizan las políticas 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 administrada de 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 los AWS servicios y 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: `AWSTransferConsoleFullAccess`

La `AWSTransferConsoleFullAccess` política proporciona acceso completo a Transfer Family a través de la consola AWS de administración. Para obtener más información, consulte la [Service-linked función de AWS Transfer Family](#).

AWS política gestionada: `AWSTransferFullAccess`

La política de `AWSTransferFullAccess` proporciona acceso completo a los servicios de Transfer Family. Para obtener más información, consulte la [Service-linked función de AWS Transfer Family](#).

AWS política gestionada: `AWSTransferLoggingAccess`

La `AWSTransferLoggingAccess` política otorga a AWS Transfer Family acceso completo para crear flujos de registro y grupos y guardar eventos de registro en su cuenta. Para obtener más información, consulte la [Service-linked función de AWS Transfer Family](#).

AWS política gestionada: `AWSTransferReadOnlyAccess`

La política de `AWSTransferReadOnlyAccess` proporciona acceso de solo lectura a los servicios de Transfer Family. Para obtener más información, consulte la [Service-linked función de AWS Transfer Family](#).

AWS Transfer Family actualiza a AWS políticas administradas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de AWS Transfer Family desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbete a la fuente RSS en la página de [Historial de documentos para AWS Transfer Family](#).

Cambio	Descripción	Fecha
Actualización de la documentación	Se agregaron secciones para cada una de las políticas administradas por Transfer Family.	27 de enero de 2022
AWSTransferReadOnlyAccess : actualización de una política actual	AWS Transfer Family agregó nuevos permisos para permitir la lectura de la política AWS Managed Microsoft AD.	30 de septiembre de 2021
AWS Transfer Family comenzó a rastrear los cambios	AWS Transfer Family comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	15 de junio de 2021

Módulos Transfer Family Terraform

[HashiCorpTerraform](#) es un motor de infraestructura como código (IaC) de código abierto desarrollado con el lenguaje de HashiCorp configuración (HCL). Terraform proporciona un flujo de trabajo de interfaz de línea de comandos (CLI) coherente que, junto con AWS Transfer Family para la infraestructura de back-end, puede administrar cientos de servicios en la nube y codificar las API de la nube en archivos de configuración declarativos.

Puede usar Terraform para implementar de forma segura los servidores SFTP y los conectores SFTP de AWS Transfer Family, junto con las dependencias y personalizaciones asociadas. Para ver el repositorio que contiene el código de Terraform para crear los recursos necesarios para ejecutar AWS Transfer Family, consulte el código fuente del [módulo Terraform Transfer Family](#) en GitHub.

Note

Los módulos AWS Transfer Family para Terraform son un esfuerzo apoyado por la comunidad. No forman parte de un AWS servicio. Best-effort El soporte lo proporciona la comunidad AWS de almacenamiento.

servidores SFTP

Esta automatización le proporciona un módulo Terraform personalizable y ejemplos integrales para crear un punto final SFTP (PUBLICo VPC tipos de punto final), integrarlo con Amazon CloudWatch para el registro y la supervisión, administrar las identidades de los usuarios para el acceso al punto final y configurar las funciones de IAM para acceder a los depósitos de Amazon S3 donde se almacenan los archivos. El módulo admite varias claves públicas SSH por usuario (hasta 50 claves) para mejorar la seguridad y las capacidades de rotación de claves.

Conectores SFTP

AWS El módulo Terraform Transfer Family ahora admite el despliegue de conectores SFTP para transferir archivos entre Amazon S3 y servidores SFTP remotos. Los conectores SFTP proporcionan una capacidad totalmente gestionada y de bajo código para copiar archivos entre Amazon S3 y servidores SFTP remotos.

Ahora puede usar Terraform para aprovisionar mediante programación sus conectores SFTP, las dependencias asociadas y las personalizaciones en una sola implementación. El módulo también proporciona ejemplos integrales para automatizar los flujos de trabajo de transferencia de archivos en función de un cronograma o de los desencadenantes de eventos. El uso de Terraform para la implementación elimina la necesidad de realizar configuraciones manuales que requieren mucho tiempo y son propensas a errores, y le proporciona una opción de implementación rápida, repetible y segura que se puede escalar.

COMO 2

Para mostrar la compatibilidad con las plantillas de Terraform de AS2, añada una reacción de aprobación (#) a la solicitud de funciones de plantillas [Terraform de Transfer Family](#). También puedes añadir un comentario que describa tu caso de uso.

Intercambio de datos entre empresas

Intercambio de datos de AWS B2B automatiza la transformación, la validación y la generación de documentos de intercambio electrónico de datos (EDI) desde y hacia los formatos de datos JSON y XML. [Para mostrar la compatibilidad con las plantillas de Terraform para el intercambio de datos B2B, añada una respuesta positiva \(#\) a la solicitud de función.](#) También puedes añadir un comentario que describa tu caso de uso.

Solución de problemas AWS Transfer Family

En este capítulo se proporciona información sobre la solución de problemas comunes que pueden surgir al utilizar el dispositivo AWS Transfer Family. Cada sección se centra en un área específica de funcionalidad para ayudarle a encontrar rápidamente soluciones a sus problemas.

- Si tiene problemas con IAM en Transfer Family, consulte [Resolución de problemas AWS Transfer Family identidad y acceso](#).
- Si tienes problemas con tus aplicaciones web de Transfer Family, consulta [Solución de problemas de sus aplicaciones web](#).

Temas

- [Solución de problemas de autenticación](#)
- [Solución de los problemas con el conector SFTP](#)
- [Solucionar problemas de conectividad y transferencia de SFTP](#)
- [Solucionar problemas con los proveedores de identidad personalizados](#)
- [Solucionar problemas de flujo de trabajo](#)
- [Solución de problemas de EFS](#)
- [Solucionar problemas de almacenamiento y cifrado](#)
- [Solucionar problemas de supervisión y alertas](#)
- [Solucionar problemas de transferencia entre regiones](#)
- [Solucionar problemas de implementación de Terraform](#)
- [Solución de problemas de integración de Web Application Firewall](#)
- [Solucionar problemas de usuarios gestionados por el servicio](#)
- [Solución de los problemas de AS2](#)

Solución de problemas de autenticación

En esta sección se describen las posibles soluciones para los siguientes problemas de autenticación.

Temas

- [Fallos de autenticación: SSH/SFTP](#)

- [Se gestionó un problema de dominios no coincidentes en AD](#)
- [Se han superado los límites de grupos de Active Directory](#)
- [Varios problemas de autenticación](#)
- [Solución de problemas de Amazon API Gateway](#)
- [Solución de los problemas al probar su proveedor de identidad](#)
- [Duplicar buckets de Amazon S3 en una aplicación web](#)

Fallos de autenticación: SSH/SFTP

Descripción

Al intentar conectarse con el servidor mediante el Protocolo de File Transfer (SFTP) de Secure Shell (SSH), recibirá un mensaje similar al siguiente:

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
Authentication failed.
```

Note

Si utiliza una API Gateway y recibe este error, consulte [Demasiados errores de autenticación](#).

Causa

No ha agregado un par de claves RSA para su usuario, por lo que debe autenticarse con una contraseña en su lugar.

Solución

Cuando ejecute el `sftp` comando, especifique la `-o PubkeyAuthentication=no` opción. Esta opción obliga al sistema a solicitar la contraseña. Por ejemplo:

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

Se gestionó un problema de dominios no coincidentes en AD

Descripción

El dominio de un usuario y el dominio de su grupo deben coincidir. Ambos deben estar en el dominio predeterminado o ambos deben estar en el dominio de confianza.

Causa

Si un usuario y su grupo no coinciden, Transfer Family no podrá autenticar al usuario. Si prueba el proveedor de identidad del usuario, recibirá el error No se ha encontrado ningún acceso asociado con los grupos de usuarios.

Solución

Haga referencia a un grupo del dominio del usuario que coincida con el dominio del grupo (predeterminado o de confianza).

Se han superado los límites de grupos de Active Directory

Descripción

Al intentar agregar más grupos de Active Directory al AWS Transfer Family servidor, aparece un error que indica que se ha alcanzado el número máximo de grupos permitido.

Causa

AWS Transfer Family tiene un límite predeterminado de 100 grupos de Active Directory por servidor.

Solución

Estas son dos posibles soluciones:

- Consolide sus grupos de Active Directory para reducir el número total necesario.
- Si su caso de uso requiere más de 100 grupos, considere la posibilidad de utilizar una solución de proveedor de identidad personalizada, tal como se describe en [Simplifique la autenticación de Active Directory con un proveedor de identidad personalizado para AWS Transfer Family](#).

Varios problemas de autenticación

Descripción

Recibe un error de autenticación y ninguna de las demás soluciones funciona

Causa

Es posible que haya especificado un destino para un directorio lógico que contiene una barra inicial o final (/).

Solución

Actualice el directorio de destino lógico para asegurarse de que comience con una barra y no contenga una barra final. Por ejemplo, /amzn-s3-demo-bucket/images es aceptable, pero amzn-s3-demo-bucket/images no /amzn-s3-demo-bucket/images/ lo es.

Solución de problemas de Amazon API Gateway

En esta sección se describen las posibles soluciones para los siguientes problemas de API Gateway.

Temas

- [Demasiados errores de autenticación](#)
- [Conexión cerrada](#)

Demasiados errores de autenticación

Descripción

Al intentar conectarse al servidor mediante el Protocolo de File Transfer (SFTP) de Secure Shell (SSH), aparece el siguiente error:

```
Received disconnect from 3.15.127.197 port 22:2: Too many authentication failures
Authentication failed.
Couldn't read packet: Connection reset by peer
```

Causa

Es posible que haya introducido una contraseña incorrecta de su usuario. Vuelva colocar de nuevo la contraseña correcta.

Si la contraseña es correcta, es posible que el problema se deba a un nombre de recurso de Amazon (ARN) del rol que no es válido. Para confirmar que este es el problema, pruebe el proveedor de identidad de su servidor. Si ve una respuesta similar a la siguiente, el rol ARN es solo un marcador de posición, como lo indica el valor del ID del rol compuesto exclusivamente por ceros:

```
{
  "Response": "{\\"Role\\": \\"arn:aws:iam::000000000000:role/MyUserS3AccessRole\\",
  \\"HomeDirectory\\": \\"/\\"}",
  "StatusCode": 200,
  "Message": "",
  "Url": "https://api-gateway-ID.execute-api.us-east-1.amazonaws.com/prod/
servers/transfer-server-ID/users/myuser/config"
}
```

Solución

Reemplace el rol ARN de marcador de posición por un rol real que tenga permiso para acceder al servidor.

Para actualizar el rol

1. Abra la CloudFormation consola en <https://console.aws.amazon.com/cloudformation>.
2. En el panel de navegación izquierdo, seleccione Stacks (Pilas).
3. En la lista de Pilas, seleccione la pila y, a continuación, la pestaña Parámetros.
4. Seleccione Actualizar. En la página Actualizar pila, seleccione Usar la plantilla actual y, a continuación, seleccione Siguiente.
5. UserRoleArn Sustitúyalo por un ARN de rol que tenga permisos suficientes para acceder al servidor Transfer Family.

Note

Para conceder los permisos necesarios, puede agregar las políticas administradas AmazonAPIGatewayAdministrator y AmazonS3FullAccess a su rol.

6. Seleccione Siguiente y de nuevo Siguiente. En la *stack* página de revisión, seleccione Acepto que AWS CloudFormation podría crear recursos de IAM y, a continuación, elija Actualizar pila.

Conexión cerrada

Descripción

Al intentar conectarse al servidor mediante el Protocolo de File Transfer (SFTP) de Secure Shell (SSH), aparece el siguiente error:

Connection closed

Causa

Una posible causa de este problema es que tu función de CloudWatch registro en Amazon no tiene una relación de confianza con Transfer Family.

Solución

Asegúrese de que el rol de registro del servidor tenga una relación de confianza con Transfer Family. Para obtener más información, consulte [Para establecer una relación de confianza](#).

Solución de los problemas al probar su proveedor de identidad

Descripción

Si pruebas tu proveedor de identidad mediante la consola o la operación de la TestIdentityProvider API, el Response campo estará vacío. Por ejemplo:

```
{
  "Response": "{}",
  "StatusCode": 200,
  "Message": ""
}
```

Causa

La causa más probable es que la autenticación haya fallado debido a un nombre de usuario o contraseña incorrectos.

Solución

Asegúrese de utilizar las credenciales correctas para su usuario y actualice el nombre de usuario o la contraseña, si es necesario.

Duplicar buckets de Amazon S3 en una aplicación web

Descripción

El mismo bucket de Amazon S3 aparece varias veces en la interfaz de la aplicación web Transfer Family.

Causa

Esto ocurre cuando un usuario pertenece a varios grupos de Active Directory que tienen concesiones para el mismo bucket de Amazon S3. La aplicación web muestra todas las concesiones de nivel superior asociadas al UID o GID del usuario, incluidas las concesiones duplicadas a la misma ubicación del depósito.

Solución

Para evitar la duplicación de listados, consolide las concesiones para que cada usuario tenga solo una concesión por ubicación de Amazon S3. Revise la configuración de las concesiones de acceso de Amazon S3 y elimine las concesiones redundantes para el mismo depósito en distintos grupos de Active Directory.

Solución de los problemas con el conector SFTP

En esta sección se describen las posibles soluciones para los problemas relacionados con los conectores SFTP.

Temas

- [Solución de los problemas al agregar claves de host confiables para su conector SFTP](#)
- [La negociación clave falla](#)
- [Regulación del conector SFTP](#)
- [Optimización del rendimiento del conector SFTP](#)
- [Solucionar problemas de conectividad de VPC](#)
- [Problemas varios con el conector SFTP](#)

Solución de los problemas al agregar claves de host confiables para su conector SFTP

Descripción

Al crear o editar un conector SFTP y añadir una clave de host de confianza, aparece el siguiente error: Failed to edit connector details (Invalid host key format.)

Causa

Si pegas una clave pública correcta, el problema puede ser que hayas incluido esa comment parte de la clave. AWS Transfer Family actualmente no acepta la parte de comentarios de la clave.

Solución

Elimine la parte de comentario de la clave al pegarla en el campo de texto. Por ejemplo, supongamos que su clave tiene un aspecto similar al siguiente:

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

Elimine el texto que sigue a los == caracteres y pegue solo la parte de la clave que llegue hasta el ==.

```
ssh-rsa AAAA...==
```

La negociación clave falla

Descripción

Recibe un error en el que falla la negociación de intercambio de claves. Por ejemplo:

```
Key exchange negotiation failed due to incompatible host key algorithms.  
Client offered: [ecdsa-sha2-nistp256, ecdsa-sha2-nistp384,  
ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256] Server offered: [ssh-rsa]
```

Causa

Este error se debe a que no hay superposición entre los algoritmos de clave de host compatibles con el servidor y los que admite el conector.

Solución

Asegúrese de que el servidor remoto admita al menos uno de los algoritmos clave del host del cliente que aparecen en el mensaje de error. Para ver la lista de los algoritmos admitidos, consulte [Políticas de seguridad para AWS Transfer Family Conectores SFTP](#).

Regulación del conector SFTP

Descripción

Al utilizar los conectores SFTP para la transferencia de archivos, se producen errores como los siguientes:

```
{"type": "ExecutionThrottled", "details": {}, "connectorId": "c-1234567890abcdef0"}
```

O bien, observa que las transferencias de archivos se retrasan o fallan de forma intermitente durante operaciones de gran volumen.

Causa

Los conectores SFTP tienen cuotas de servicio que limitan la cantidad de transferencias de archivos y operaciones de API simultáneas. Cuando se superan estos límites, se produce una limitación para proteger el servicio y garantizar un uso justo por parte de todos los clientes.

Solución

Para solucionar los problemas del conector SFTP, pruebe las siguientes soluciones:

1. Implemente una lógica de retroceso exponencial y reintento en sus aplicaciones. Por ejemplo, cree una función que reintente automáticamente las operaciones fallidas aumentando los tiempos de espera entre intentos.
2. Implemente la limitación de velocidad en su aplicación:
 - Limite el número de transferencias simultáneas.
 - Añada demoras entre lotes de transferencias.
3. Controle su uso comparándolo con las cuotas de servicio:
 - Usa CloudWatch métricas para hacer un seguimiento del uso de la API.
 - Configura alarmas para que te notifiquen cuando te acerques a los límites de la cuota.
4. Para ver las opciones para escalar los conectores SFTP, consulte [Escalar sus conectores SFTP](#).
5. Si la limitación persiste y afecta a sus operaciones empresariales, solicite un aumento de cuota a través de la consola Service Quotas.

Optimización del rendimiento del conector SFTP

Descripción

Las transferencias del conector SFTP son más lentas de lo esperado o el rendimiento no es uniforme.

Causa

El rendimiento del conector SFTP puede verse afectado por varios factores, como las condiciones de la red, el tamaño de los archivos, la configuración del servidor remoto y los límites de transferencia simultánea.

Solución

Para optimizar el rendimiento del conector SFTP:

- Configure su servidor SFTP remoto para obtener un rendimiento óptimo:
 - Aumente el número máximo de sesiones y transferencias por sesión
 - Optimice los tamaños de las ventanas TCP para conexiones de alta latencia
 - Utilice la compresión si ambos extremos la admiten
- Considere la optimización de la red, colocando el conector Transfer Family en una región cercana a su servidor SFTP remoto.
- Implemente una estrategia de monitoreo para identificar los cuellos de botella en el rendimiento:
 - Supervise el rendimiento y la latencia de la red
 - Analice los registros para detectar patrones en las transferencias lentas

Solucionar problemas de conectividad de VPC

En esta sección, se describen las soluciones para los problemas más comunes de los conectores VPC_ SFTPLATTICE-enabled .

El conector está atascado en estado PENDIENTE

Descripción

El conector LATTICE-enabled SFTP VPC_ permanece en PENDING estado durante un período prolongado (más de 10 minutos).

Causa

Esto puede ocurrir debido a retrasos en la resolución del DNS, problemas de configuración de Resource Gateway o problemas de asociación de redes del servicio VPC Lattice.

Solución

Póngase en contacto con [AWS Support](#) en [contacto con Contact AWS](#) para que le ayuden a analizar la causa raíz del problema. También puede probar la siguiente solución alternativa.

1. Compruebe que su Resource Gateway esté en ACTIVE estado:

```
aws vpc-lattice get-resource-gateway --resource-gateway-  
identifier rgw-1234567890abcdef0
```

2. Compruebe que la configuración de recursos esté correctamente configurada y activa:

```
aws vpc-lattice get-resource-configuration --resource-configuration-  
identifier rcfg-1234567890abcdef0
```

3. Asegúrese de que su Resource Gateway tenga subredes en al menos dos zonas de disponibilidad que admitan VPC Lattice.
4. Si el problema persiste, elimine y vuelva a crear el conector con la misma configuración.

Conector en estado ERRÓNEO

Descripción

El conector LATTICE-enabled SFTP VPC_ muestra el ERRORRED estado con detalles del error.

Causa

Las causas más comunes incluyen un ARN de configuración de recursos no válido, direcciones IP insuficientes en las subredes de VPC o intentos de compartir recursos entre regiones.

Solución

1. Compruebe los detalles del error mediante: `describe-connector`

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

2. Compruebe que el ARN de la configuración de recursos sea correcto y se encuentre en la misma región que el conector.
3. Asegúrese de que las subredes de VPC tengan suficientes direcciones IP disponibles para Resource Gateway.
4. Compruebe que se pueda acceder a su destino de configuración de recursos (dirección IP o nombre DNS) desde su VPC.

Error: la dirección IP pública no es compatible

Descripción

Aparece un error al intentar crear una configuración de recursos con una dirección IP pública:
`ValidationException: IP address x.x.x.x is not in allowed ranges.`

Causa

Las configuraciones de recursos para los puntos finales públicos deben usar nombres DNS, no direcciones IP.

Solución

Utilice el nombre DNS público del servidor SFTP en lugar de su dirección IP al crear la configuración de recursos:

```
aws vpc-lattice create-resource-configuration \
  --name my-public-server-config \
  --resource-gateway-identifier rgw-1234567890abcdef0 \
  --resource-configuration-definition dnsResource={domainName="my.sftp.server.com"} \
  --port-ranges 22
```

Error: zona de disponibilidad no admitida

Descripción

Aparece un error al crear una puerta de enlace de recursos: `Subnet subnet-xxx is not valid because it is not in a supported Availability Zone.`

Causa

No todas las zonas de disponibilidad admiten el acceso a los recursos de VPC Lattice Cross-VPC . El mensaje de error muestra las zonas de disponibilidad compatibles en su región.

Solución

1. Cree subredes en las zonas de disponibilidad compatibles que aparecen en el mensaje de error.
2. Actualice su Resource Gateway para que utilice únicamente subredes de las zonas de disponibilidad compatibles.

3. Asegúrese de tener al menos dos subredes en diferentes AZ compatibles.

Tiempos de espera de conexión con conectores VPC_LATTICE

Descripción

Las transferencias de archivos a través de conectores de VPC agotan el tiempo de espera o fallan de forma intermitente.

Causa

VPC Lattice tiene límites de conexión (350 conexiones por recurso) y tiempos de espera de inactividad (350 segundos para TCP).

Solución

1. Supervise las conexiones simultáneas para mantenerse dentro del límite de 350 conexiones por recurso.
2. Implemente la agrupación de conexiones y la reutilización en sus aplicaciones.
3. Configure los valores de tiempo de espera adecuados en sus aplicaciones cliente de SFTP (menos de 350 segundos).
4. Considere la posibilidad de crear varias configuraciones de recursos para el mismo destino a fin de distribuir la carga.

Problemas varios con el conector SFTP

Descripción

Recibes un error después de ejecutarlo `StartFileTransfer`, pero no conoces la causa del problema y solo se devuelve el ID del conector tras la llamada a la API.

Causa

Este error puede deberse a varias causas. Para solucionar el problema, le recomendamos que pruebe el conector y busque en CloudWatch los registros.

Solución

- Pruebe el conector: consulte [Prueba de un conector SFTP](#). Si la prueba no es satisfactoria, el sistema muestra un mensaje de error en función del motivo por el que no se ha realizado la

prueba. En esa sección se describe cómo probar el conector desde la consola o mediante el comando [TestConnectionAPI](#).

- Ver CloudWatch los registros de su conector: consulte [Ejemplos de entradas de registro para conectores SFTP](#). En este tema se proporcionan ejemplos de las entradas de registro del conector SFTP y de la convención de nomenclatura para ayudarle a encontrar los registros adecuados.

Solucionar problemas de conectividad y transferencia de SFTP

En esta sección se describen las posibles soluciones para los problemas de conectividad SFTP y transferencia de archivos.

Temas

- [Solucionar problemas de conectividad de SFTP](#)
- [Solucione los problemas del cliente SFTP](#)
- [Solución de los problemas de carga de archivos](#)
- [Solucionar problemas con el conector SFTP del tipo de salida de la VPC](#)

Solucionar problemas de conectividad de SFTP

Descripción

El cliente SFTP no puede iniciar la conexión. Este problema puede producirse de forma continua o intermitente. Por ejemplo, es posible que vea la siguiente secuencia de eventos en los registros de depuración del cliente SFTP:

```
sftp -vvv username@1.1.1.1
.....
debug1: Local version string .....
kex_exchange_identification: read: Connection reset by peer
Connection reset by 1.1.1.1 port 22
Connection closed.
```

Causa

Hay un caso extremo en el que el TCP ACK (ACK sin datos) de cero bytes, también conocido como protocolo de enlace de tres vías, se omite o se retrasa.

Solución

Como solución alternativa, Transfer Family ofrece una solución que utiliza una configuración diferente para resolver este problema, pero que puede provocar problemas de compatibilidad con clientes antiguos. Por ese motivo, esta solución solo está disponible en el puerto 2223.

En el procedimiento para crear un servidor Transfer Family en una VPC ([Creación de un servidor en una nube privada virtual \(VPC\)](#)), al especificar un grupo de seguridad, configure el tráfico SSH para que utilice el puerto 2223.

Solucione los problemas del cliente SFTP

Los mensajes del lado del cliente SFTP se describen en [Mensajes SFTP](#). La mejor forma de solucionar los problemas del cliente SFTP es comprobar los registros del cliente SFTP y, si es necesario, ponerse en contacto con el administrador de la red.

Solución de los problemas de carga de archivos

En esta sección se describen las posibles soluciones para los siguientes problemas de carga de archivos.

Temas

- [Solución de los problemas de errores de carga de archivos de Amazon S3](#)
- [Solución de los problemas de nombres de archivo ilegibles](#)

Solución de los problemas de errores de carga de archivos de Amazon S3

Descripción

Cuando intenta cargar un archivo al almacenamiento de Amazon S3 mediante Transfer Family, recibe el siguiente mensaje de error: AWS Transfer no admite escrituras con acceso aleatorio a objetos de S3.

Causa

Cuando utiliza Amazon S3 para el almacenamiento de su servidor, Transfer Family no admite múltiples conexiones para una sola transferencia.

Solución

Si su servidor de Transfer Family utiliza Amazon S3 para su almacenamiento, desactive todas las opciones del software cliente que mencionen el uso de varias conexiones para una sola transferencia.

Solución de los problemas de nombres de archivo ilegibles

Descripción

Ve nombres de archivos corruptos en algunos de los archivos que ha subido. A veces, los usuarios tienen problemas con las transferencias FTP y SFTP, que confunden algunos caracteres de los nombres de los archivos, como las diéresis, las letras acentuadas o algunos sistemas de escritura, como el chino o el árabe.

Causa

Si bien los protocolos FTP y SFTP permiten que los clientes negocien la codificación de caracteres de los nombres de los archivos, Amazon S3 y Amazon EFS no lo hacen. En su lugar, requieren la codificación de UTF-8 caracteres. Como resultado, algunos caracteres no se representan correctamente.

Solución

Para solucionar este problema, revise la aplicación cliente para comprobar la codificación de caracteres del nombre de archivo y asegúrese de que está configurada en UTF-8.

Solucionar problemas con el conector SFTP del tipo de salida de la VPC

Si tiene problemas con los conectores SFTP del tipo de salida de la VPC, compruebe lo siguiente:

El estado del conector es PENDIENTE

Descripción

El conector de tipo de salida de VPC permanece en estado PENDIENTE durante varios minutos después de su creación y TestConnection devuelve el mensaje «Conector no disponible».

Causa

La resolución de DNS para los conectores de VPC puede tardar varios minutos en completarse después de la creación.

Solución

Espere a que el estado del conector pase a ser **ACTIVO** antes de intentar transferir los archivos. Este es el comportamiento normal de los conectores de tipo salida de VPC.

Tiempos de espera de conexión

Descripción

Se agota el tiempo de espera del conector de tipo de salida de la VPC al intentar conectarse al servidor SFTP.

Causa

Es posible que los grupos de seguridad no permitan el tráfico en el puerto 22 entre las subredes de Resource Gateway y el servidor SFTP de destino.

Solución

Compruebe que los grupos de seguridad permiten el tráfico en el puerto 22 entre las subredes de Resource Gateway y el servidor SFTP de destino.

Errores de configuración de recursos

Descripción

El conector de tipo de salida de la VPC no se puede conectar debido a problemas de configuración de recursos.

Causa

La configuración de recursos puede indicar una dirección IP o un nombre de DNS incorrectos, o la puerta de enlace de recursos puede no estar en la misma VPC que su servidor SFTP (para puntos finales privados).

Solución

Asegúrese de que la configuración de recursos apunte a la dirección IP o el nombre DNS correctos y que la puerta de enlace de recursos esté en la misma VPC que su servidor SFTP (para puntos finales privados). Para obtener más información, consulte [Configuraciones de recursos](#) en la Guía del usuario de Amazon VPC Lattice.

Problemas con los terminales públicos

Descripción

El conector de tipo de salida de la VPC no se puede conectar a puntos finales SFTP públicos.

Causa

Para los puntos finales públicos, debe usar un nombre DNS (no una dirección IP) en la configuración de recursos y su VPC debe tener una puerta de enlace NAT para el acceso saliente a Internet.

Solución

Asegúrese de utilizar un nombre DNS, no una dirección IP, en la configuración de recursos. Compruebe que la VPC tenga una puerta de enlace NAT para el acceso saliente a Internet.

Problemas con la zona de disponibilidad

Descripción

No puede crear una puerta de enlace de recursos debido a las limitaciones de la zona de disponibilidad.

Causa

Las puertas de enlace de recursos requieren subredes en al menos 2 zonas de disponibilidad y no todas las AZ admiten VPC Lattice.

Solución

Compruebe las zonas de disponibilidad compatibles para VPC Lattice en su región y asegúrese de tener subredes en al menos 2 zonas de disponibilidad compatibles.

Solucionar problemas con los proveedores de identidad personalizados

En esta sección se describen las posibles soluciones para los problemas relacionados con los proveedores de identidad personalizados con Transfer Family.

Temas

- [Solucionar errores de integración de API Gateway](#)
- [Solucionar problemas de tiempos de espera de funciones Lambda](#)
- [Solucione problemas constantes de tiempo de espera de Lambda](#)

- [Solucione los problemas de las excepciones KeyError](#)

Solucionar errores de integración de API Gateway

Descripción

Los usuarios no pueden autenticarse con su servidor Transfer Family y, al probar su proveedor de identidad, aparecen errores como:

```
{
  "Response": "",
  "StatusCode": 500,
  "Message": "Internal server error"
}
```

Causa

Los errores de integración de API Gateway pueden producirse debido a:

- Configuración de API Gateway incorrecta
- Los errores de la función Lambda no se gestionan correctamente
- Problemas de permisos entre API Gateway y Lambda
- Respuestas malformadas de la función Lambda

Solución

Para solucionar los errores de integración de API Gateway:

1. Consulte los registros de funciones de Lambda para obtener información detallada sobre los errores:
 - En la CloudWatch consola, vaya a Grupos de registros >/aws/lambda/your-function-name
 - Busca mensajes de error o rastros de pila que indiquen la causa raíz
2. Compruebe que la función Lambda devuelva las respuestas con el formato correcto:

```
{
  "Role": "arn:aws:iam::123456789012:role/TransferUserRole",
  "HomeDirectory": "/mybucket/home/username"
}
```


3. Habilite el CloudWatch registro detallado para API Gateway:

- En la consola de API Gateway, selecciona tu API y elige Stages
- Seleccione su etapa y, en, a continuación Logs/Tracing, active CloudWatch los registros
- Establezca el nivel de registro en ERROR o INFO

4. Pruebe su punto final de API Gateway directamente:

```
curl -X POST https://your-api-id.execute-api.region.amazonaws.com/prod/servers/your-server-id/users/username/config \
-H "Content-Type: application/json" \
-d '{"Password": "password"}'
```

5. Compruebe los permisos entre API Gateway y Lambda:

- Asegúrese de que API Gateway tenga permiso para invocar su función Lambda
- Compruebe que el rol de ejecución de la función Lambda tenga los permisos necesarios

Solucionar problemas de tiempos de espera de funciones Lambda

Descripción

Cuando los usuarios intentan autenticarse en su servidor Transfer Family mediante un proveedor de identidad personalizado, sufren grandes retrasos seguidos de errores de autenticación. En sus registros Lambda, ve errores de tiempo de espera.

Causa

Las funciones Lambda que se utilizan para los proveedores de identidad personalizados tienen un tiempo de espera predeterminado de 3 segundos. Si la lógica de autenticación tarda más que este tiempo de espera (por ejemplo, al consultar bases de datos externas o realizar llamadas a la API a proveedores de identidad de terceros), se agotará el tiempo de espera de la función y se producirá un error en la autenticación.

Solución

Para resolver problemas de tiempo de espera de Lambda:

1. Aumente el tiempo de espera de la función Lambda:

- En la consola Lambda, vaya a su función y seleccione la pestaña Configuración
- En Configuración general, haga clic en Editar

- Aumente el valor de tiempo de espera (se recomienda un máximo de 15 segundos para las funciones de autenticación)
2. Optimice el código de su función Lambda:
 - Utilice la agrupación de conexiones para las consultas a la base de datos
 - Implemente el almacenamiento en caché para los datos a los que se accede
 - Minimice las llamadas a la API externa durante la autenticación
 3. Considere la posibilidad de utilizar la simultaneidad aprovisionada de Lambda para eliminar los arranques en frío:

```
aws lambda put-provisioned-concurrency-config \
  --function-name my-authentication-function \
  --qualifier prod \
  --provisioned-concurrent-executions 5
```

4. Supervise el rendimiento de Lambda mediante CloudWatch métricas y configure alarmas para los umbrales de duración

Solucione problemas constantes de tiempo de espera de Lambda

Descripción

Los usuarios experimentan tiempos de espera constantes cuando utilizan una función Lambda para la autenticación.

Causa

Lambda no puede acceder al AWS servicio correspondiente utilizado para la autenticación (como DynamoDB, Secrets Manager u otro proveedor de identidad).

Solución

Compruebe que las subredes puedan acceder a los servicios. AWS O bien, si se conecta a un proveedor de identidad de Internet (como Okta), compruebe que la subred de la función Lambda pueda acceder a Internet a través de una puerta de enlace NAT

Solucione los problemas de las excepciones **KeyError**

Descripción

En tus entradas de registro de Transfer Family, observas KeyError «» excepciones.

Causa

La causa más probable es que el usuario o `identity_provider` registro tenga un formato incorrecto o falten campos obligatorios.

Solución

Revise el ERRORS registro, que se encuentra en el grupo de `/aws/transfer/your-server-id` registros, para obtener pistas.

Solucionar problemas de flujo de trabajo

En esta sección se describen las posibles soluciones para los problemas relacionados con los flujos de trabajo gestionados.

Temas

- [Solución de problemas de flujos de trabajo administrados](#)
- [Solución de los problemas de descifrado del flujo de trabajo](#)

Solución de problemas de flujos de trabajo administrados

En esta sección se describen las posibles soluciones para los siguientes problemas del flujo de trabajo.

Temas

- [Solucionar errores relacionados con el flujo de trabajo con Amazon CloudWatch](#)
- [Solución de los errores de copia del flujo de trabajo](#)

Solucionar errores relacionados con el flujo de trabajo con Amazon CloudWatch

Descripción

Si tienes problemas con tus flujos de trabajo, puedes recurrir CloudWatch a Amazon para investigar la causa.

Causa

Las causas pueden ser diversas. Usa Amazon CloudWatch Logs para investigar.

Solución

Transfer Family emite el estado de ejecución del flujo de trabajo en CloudWatch Logs. En los CloudWatch registros pueden aparecer los siguientes tipos de errores de flujo de trabajo:

- "type": "StepErrored"
- "type": "ExecutionErrored"
- "type": "ExecutionThrottled"
- "Service failure on starting workflow"

Puede filtrar los registros de ejecución de su flujo de trabajo con una sintaxis de filtro y patrón diferente. Por ejemplo, puede crear un filtro de registro en sus CloudWatch registros para capturar los registros de ejecución del flujo de trabajo que contienen el ExecutionErrored mensaje. Para obtener más información, consulte [Real-time Procesamiento de datos de registro con suscripciones y Sintaxis de filtros y patrones](#) en la Guía del usuario de Amazon CloudWatch Logs.

StepErrored

```
2021-10-29T12:57:26.272-05:00
    {"type":"StepErrored","details":
{"errorType":"BAD_REQUEST","errorMessage":"Cannot
    tag Efs file","stepType":"TAG","stepName":"successful_tag_step"},
    "workflowId":"w-
abcdef01234567890","executionId":"1234abcd-56ef-78gh-90ij-1234klmno567",
    "transferDetails":
{"serverId":"s-1234567890abcdef0","username":"lhr","sessionId":"1234567890abcdef0"}}
```

Aquí, StepErrored indica que un paso del flujo de trabajo ha generado un error. En un solo flujo de trabajo, puede configurar varios pasos. Este error indica el paso en el que se produjo el error y proporciona un mensaje de error. En este ejemplo concreto, el paso se configuró para etiquetar un archivo; sin embargo, no se admite el etiquetado de un archivo en un sistema de archivos de Amazon EFS, por lo que el paso generó un error.

ExecutionErrored

```
2021-10-29T12:57:26.618-05:00
    {"type":"ExecutionErrored","details":{},"workflowId":"w-w-
abcdef01234567890",
```

```
"executionId":"1234abcd-56ef-78gh-90ij-1234klmno567","transferDetails":
{"serverId":"s-1234567890abcdef0",
  "username":"lhr","sessionId":"1234567890abcdef0"}}
```

Cuando un flujo de trabajo no puede ejecutar ningún paso, genera un mensaje de `ExecutionErrored`. Por ejemplo, si ha configurado un solo paso en un flujo de trabajo determinado y el paso no se puede ejecutar, se producirá un error en el flujo de trabajo general.

Executionthrottled

La ejecución se limita si un flujo de trabajo se activa a una velocidad superior a la que el sistema puede soportar. Este mensaje de registro indica que debe reducir la velocidad de ejecución de los flujos de trabajo. [Si no puede reducir la tasa de ejecución de su flujo de trabajo, póngase en contacto con At Contact AWS Support . AWS](#)

Fallo en el servicio al iniciar el flujo de trabajo

Cada vez que elimine un flujo de trabajo de un servidor y lo reemplace por uno nuevo o actualice la configuración del servidor (lo que afecta al rol de ejecución del flujo de trabajo), debe esperar, aproximadamente, 10 minutos antes de ejecutar el nuevo flujo de trabajo. El servidor de Transfer Family almacena en caché los detalles del flujo de trabajo y tarda 10 minutos en actualizar su caché.

Además, debe cerrar sesión en cualquier sesión de SFTP activa y volver a iniciarla después del período de espera de 10 minutos para ver los cambios.

Solución de los errores de copia del flujo de trabajo

Descripción

Si está ejecutando un flujo de trabajo que contiene un paso para copiar el archivo cargado, es posible que aparezca el siguiente error:

```
{
  "type": "StepErrored", "details": {
    "errorType": "BAD_REQUEST", "errorMessage": "Bad Request (Service: Amazon S3;
    Status Code: 400; Error Code: 400 Bad Request;
    Request ID: request-ID; S3 Extended Request ID: request-ID Proxy: null)",
    "stepType": "COPY", "stepName": "copy-step-name" },
    "workflowId": "workflow-ID",
    "executionId": "execution-ID",
    "transferDetails": {
      "serverId": "server-ID",
```

```
    "username": "user-name",  
    "sessionId": "session-ID"  
  }  
}
```

Causa

El archivo de origen se encuentra en un bucket de Amazon S3 que se encuentra en un bucket Región de AWS diferente al de destino.

Solución

Si está ejecutando un flujo de trabajo que incluye un paso de copia, asegúrese de que los buckets de origen y destino estén en el mismo archivo Región de AWS.

Solución de los problemas de descifrado del flujo de trabajo

En esta sección, se describen las posibles soluciones para los siguientes problemas relacionados con los flujos de trabajo cifrados.

Temas

- [Solucione problemas de cifrado de destinatarios anónimos](#)
- [Solucione el error del archivo de cifrado firmado](#)
- [Solucione el error de un algoritmo FIPS](#)

Solucione problemas de cifrado de destinatarios anónimos

Descripción

El flujo de trabajo de descifrado falla al procesar determinados archivos cifrados, pero funciona con otros.

Causa

Es posible que los archivos se hayan cifrado sin especificar un destinatario (cifrado anónimo), lo que dificulta que el flujo de trabajo determine qué clave utilizar para el descifrado.

Solución

Cifre siempre los archivos con un destinatario que no sea anónimo mediante el parámetro. -r Por ejemplo:

```
gpg -e -r user@example.com --openpgp file.txt
```

Para comprobar si un archivo se cifró con un destinatario específico o de forma anónima, utilice el comando: `--list-packets`

```
gpg --list-packets file.txt.gpg
```

Este comando muestra la estructura del paquete del GPG-encrypted archivo sin descifrar su contenido. Busque un resultado que incluya la información del destinatario, como:

```
:pubkey enc packet: version 3, algo 1, keyid 1A2B3C4D5E6F7G8H
```

Si ves información sobre el identificador clave, significa que el archivo se cifró para un destinatario específico. Si falta esta información, es posible que el archivo se haya cifrado de forma anónima, lo que puede provocar errores de descifrado en los flujos de trabajo de Transfer Family.

También puede usar este comando para verificar:

- Qué algoritmos de cifrado se utilizaron
- Métodos de compresión (si los hay)
- Marcas de tiempo de creación

Para ver la lista de algoritmos de cifrado compatibles con tu instalación de GPG, usa:

```
gpg --version
```

Esta información puede ayudarle a asegurarse de que utiliza algoritmos de cifrado compatibles con los flujos de trabajo de Transfer Family, especialmente cuando se requiere la conformidad con FIPS.

Solucione el error del archivo de cifrado firmado

Descripción

Se produce un error en el flujo de trabajo de descifrado y aparece el siguiente error:

```
"Encrypted file with signed message unsupported"
```

Causa

Actualmente, Transfer Family no admite la firma de archivos cifrados.

Solución

En tu cliente PGP, si hay una opción para firmar el archivo cifrado, asegúrate de borrar la selección, ya que Transfer Family no admite actualmente la firma de archivos cifrados.

Solucione el error de un algoritmo FIPS

Descripción

Se produce un error en el flujo de trabajo de descifrado y el mensaje de registro es similar al siguiente:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "File encryption algorithm not supported with FIPS mode
enabled.",
    "stepType": "DECRYPT",
    "stepName": "step-name"
  },
  "workflowId": "workflow-ID",
  "executionId": "execution-ID",
  "transferDetails": {
    "serverId": "server-ID",
    "username": "user-name",
    "sessionId": "session-ID"
  }
}
```

Causa

Su servidor de Transfer Family tiene el modo FIPS activado y un paso de flujo de trabajo de descifrado asociado. Al cifrar los archivos antes de cargarlos en el servidor de Transfer Family, el cliente de cifrado puede generar archivos cifrados que utilizan algoritmos de cifrado simétrico no aprobados por FIPS. En este escenario, el flujo de trabajo no puede descifrar los archivos. En el siguiente ejemplo, la versión 2.4.0 de GnuPG utiliza OCB (un modo de cifrado por bloques que no es FIPS) para cifrar archivos, lo que provoca un error en el flujo de trabajo.

Solución

Debe editar la clave GPG que utilizó para cifrar los archivos y, a continuación, volver a cifrarlos. El siguiente procedimiento describe los pasos que debe seguir.

Edición de las claves PGP

1. Identifique la clave que debe editar ejecutando `gpg --list-keys`

Esto devuelve una lista de claves. Cada clave tiene detalles similares a los siguientes:

```
pub   ed25519 2022-07-07 [SC]
       wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
uid           [ultimate] Mary Major <marymajor@example.com>
sub   cv25519 2022-07-07 [E]
```

2. Identifique la clave que desea editar. En el ejemplo mostrado en el paso anterior, el ID es `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.
3. Ejecute `gpg --edit-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.

El sistema responde con detalles sobre el programa GnuPG y la clave especificada.

4. Cuando se `gpg>` le solicite, escriba `showpref`. Se devuelven los siguientes detalles:

```
[ultimate] (1). Mary Major <marymajor@example.com>
  Cipher: AES256, AES192, AES, 3DES
  AEAD: OCB
  Digest: SHA512, SHA384, SHA256, SHA224, SHA1
  Compression: ZLIB, BZIP2, ZIP, Uncompressed
  Features: MDC, AEAD, Keyserver no-modify
```

Tenga en cuenta que se muestran los algoritmos preferidos que se almacenan en la clave.

5. Queremos editar la clave para retener todos los algoritmos excepto el OCB. Ejecute el `setpref` comando especificando todos los algoritmos que desee retener:

```
gpg> setpref AES256, AES192, AES, 3DES, SHA512, SHA384, SHA256, SHA224, SHA1, ZLIB,
  BZIP2, ZIP, Uncompressed
```

Devuelve lo siguiente detalles:

```
Set preference list to:
  Cipher: AES256, AES192, AES, 3DES
  AEAD:
```

```
Digest: SHA512, SHA384, SHA256, SHA224, SHA1
Compression: ZLIB, BZIP2, ZIP, Uncompressed
Features: MDC, Keyserver no-modify
Really update the preferences? (y/N)
```

6. Introduzca y para actualizar y, a continuación, introduzca su contraseña cuando se le pida que confirme el cambio.
7. Guarde los cambios.

```
gpg> save
```

Antes de volver a ejecutar el flujo de trabajo de descifrado, debe volver a cifrar los archivos con la clave editada.

Solución de problemas de EFS

En esta sección se describen las posibles soluciones para los problemas relacionados con el almacenamiento de Amazon EFS.

Temas

- [Solución de problemas de Amazon EFS](#)

Solución de problemas de Amazon EFS

En esta sección se describen las posibles soluciones para los siguientes problemas de Amazon EFS.

Temas

- [Solución de los problemas de los usuarios administrados por el servicio de Amazon EFS](#)
- [Solución de los problemas del perfil POSIX faltante](#)
- [Solución de los problemas de directorios lógicos con Amazon EFS](#)

Solución de los problemas de los usuarios administrados por el servicio de Amazon EFS

Descripción

Al ejecutar el comando `sftp`, el mensaje no aparece y, en su lugar, aparece el siguiente mensaje:

```
Couldn't canonicalize: Permission denied
Need cwd
```

Causa

El rol de su usuario AWS Identity and Access Management (IAM) no tiene permiso para acceder a Amazon Elastic File System (Amazon EFS).

Solución

Aumente los permisos de política para el rol de su usuario. Puede añadir una política AWS gestionada, como `AmazonElasticFileSystemClientFullAccess`.

Solución de los problemas del perfil POSIX faltante

Descripción

Si utiliza el almacenamiento de Amazon EFS para su servidor y utiliza un proveedor de identidad personalizado, debe proporcionar a su AWS Lambda función un perfil POSIX.

Causa

Una posible causa es que las plantillas que proporcionamos para crear un método AWS Lambda respaldado por Amazon API Gateway no contienen actualmente información POSIX.

Si proporcionó información POSIX, es posible que Transfer Family no esté analizando correctamente el formato que utilizó para proporcionar la información POSIX.

Solución

Asegúrese de proporcionar un elemento JSON a Transfer Family para el parámetro `PosixProfile`.

Por ejemplo, si utiliza Python, puede añadir la siguiente línea en la que se analiza el `PosixProfile` parámetro:

```
if PosixProfile:
    response_data["PosixProfile"] = json.loads(PosixProfile)
```

O bien JavaScript, puede añadir la siguiente línea, donde *uid-value* y *gid-value* son números enteros, 0 o mayores, que representan el ID de usuario (UID) y el ID de grupo (GID), respectivamente:

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

Estos ejemplos de código envían el parámetro PosixProfile a Transfer Family como un objeto JSON, en lugar de como una cadena.

Además, dentro de él AWS Secrets Manager, debe almacenar el PosixProfile parámetro de la siguiente manera. Sustituya *your-uid* y *your-gid* por sus valores reales para el GID y el UID.

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

Solución de los problemas de directorios lógicos con Amazon EFS

Descripción

Si el directorio de inicio del usuario no existe y este ejecuta un comando `ls`, el sistema responde de la siguiente manera:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Causa

Si su servidor de Transfer Family utiliza Amazon EFS, el directorio de inicio del usuario debe crearse con acceso de lectura y escritura para que el usuario pueda trabajar en su directorio de inicio lógico. El usuario no puede crear este directorio por sí mismo, ya que carecería de permisos para `mkdir` en su directorio de inicio lógico.

Solución

Un usuario con acceso administrativo al directorio de inicio debe crear el directorio de inicio lógico del usuario.

Solucionar problemas de almacenamiento y cifrado

En esta sección se describen las posibles soluciones para los problemas de almacenamiento y cifrado.

Temas

- [Solución de problemas de políticas para buckets de Amazon S3 cifrados](#)
- [Solución de los problemas con la excepción ResourceNotFound](#)

Solución de problemas de políticas para buckets de Amazon S3 cifrados

Descripción

Cuenta con un bucket de Amazon S3 cifrado que utiliza como almacenamiento para su servidor de Transfer Family. Si intenta subir un archivo al servidor, recibirá un mensaje de error `Couldn't close file: Permission denied`.

Y si consulta los registros del servidor, verá los siguientes errores:

```
ERROR Message="Access denied" Operation=CLOSE Path=/bucket/user/test.txt BytesIn=13  
ERROR Message="Access denied"
```

Causa

La política de su usuario de IAM no tiene permiso para acceder al bucket cifrado.

Solución

Debe especificar permisos adicionales en su política para conceder los permisos necesarios AWS Key Management Service (AWS KMS). Para obtener más información, consulte [Protección y cifrado de datos](#).

Solución de los problemas con la excepción **ResourceNotFound**

Descripción

Recibe un error en el que no se encuentra el recurso. Por ejemplo, si ejecuta `UpdateServer`, puede que obtenga el siguiente error:

```
An error occurred (ResourceNotFoundException) when calling the UpdateServer operation:  
Unknown server
```

Causa

Existen varios motivos para recibir un `ResourceNotFoundException` mensaje. En la mayoría de los casos, el recurso que especificó en el comando de la API no existe. Si especificó un recurso existente, la causa más probable es que la región predeterminada sea diferente de la región del recurso. Por ejemplo, si su región predeterminada es `us-east-1` y su servidor de Transfer Family está en `us-east-2`, recibirá una excepción de recurso desconocido.

Para obtener más información sobre cómo configurar una región predeterminada, consulte [Configuración rápida con `aws configure`](#).

Solución

Agregue un parámetro de región a su comando de API para especificar de forma explícita dónde encontrar un recurso concreto.

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

Solucionar problemas de supervisión y alertas

En esta sección se proporciona información sobre la resolución de problemas de supervisión y alerta AWS Transfer Family, incluidas las CloudWatch métricas ausentes o incompletas y EventBridge los eventos faltantes.

Temas

- [Solucione problemas con las métricas faltantes o incompletas CloudWatch](#)
- [Solucione problemas de eventos faltantes EventBridge](#)

Solucione problemas con las métricas faltantes o incompletas CloudWatch

Descripción

CloudWatch faltan las métricas de sus servidores Transfer Family, están incompletas o no se actualizan como se esperaba.

Causa

Las métricas faltantes o incompletas pueden deberse a varios factores:

- Registrar problemas de configuración
- Niveles de actividad bajos que no generan métricas en el plazo esperado

- Visualización de métricas con dimensiones o intervalos de tiempo incorrectos

Solución

Para resolver problemas relacionados con CloudWatch métricas faltantes o incompletas:

1. Asegúrese de que el registro esté configurado correctamente para su servidor Transfer Family:
 - En la consola de Transfer Family, compruebe que el registro esté activado en Detalles del servidor > Detalles adicionales > Función de registro.
 - Es muy importante que la función de registro tenga los permisos y las relaciones de confianza necesarios.
2. Al ver las métricas en la CloudWatch consola:
 - Utilice las dimensiones correctas, por ejemplo ServerId, para las métricas a nivel de servidor
 - Ajuste el intervalo de tiempo para asegurarse de que cubre los períodos de actividad
 - Compruebe que estás en el correcto Región de AWS
3. Genere actividad de prueba en su servidor Transfer Family para garantizar que se generen las métricas.

Solucione problemas de eventos faltantes EventBridge

Descripción

Has configurado EventBridge las reglas de Amazon para incluir los eventos de Transfer Family, pero los eventos no se envían a tus destinos de destino ni provocan las acciones esperadas.

Causa

La falta de EventBridge eventos puede deberse a:

- Patrones de eventos configurados incorrectamente
- Problemas de permisos con los objetivos de los eventos
- Límites o limitaciones del servicio
- Los eventos no se generan debido a la configuración del servidor

Solución

Para solucionar problemas de EventBridge eventos faltantes:

1. Comprueba que el patrón de eventos tenga el formato correcto para que coincida con los eventos de Transfer Family:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["Transfer State Change"],
  "detail": {
    "serverId": ["s-1234567890abcdef0"]
  }
}
```

2. Comprueba que el objetivo de tu evento tenga los permisos necesarios:
 - Para los objetivos Lambda, asegúrese de que la política de recursos de la función Lambda permita invocarla EventBridge
 - En el caso de los destinos de SQS, compruebe que la política de colas permita enviar mensajes EventBridge
 - En el caso de los destinos de SNS, confirme que la política del tema permite EventBridge publicar en ellos
3. Pon a prueba tu regla generando eventos de muestra:
 - Usa la EventBridge consola para crear un evento de prueba que coincida con tu patrón
 - Realice acciones en su servidor Transfer Family que deberían generar eventos
4. Habilite las métricas de EventBridge reglas para monitorear las invocaciones y los errores de las reglas:

```
aws events put-rule --name "TransferStateChangeRule" --event-pattern '{...}' --state
ENABLED --metrics-enabled
```

5. Compruebe CloudWatch los registros para ver si hay algún mensaje de error relacionado con errores en la entrega de eventos

Solucionar problemas de transferencia entre regiones

En esta sección se describen las posibles soluciones para los problemas relacionados con la transferencia de archivos de un lado a otro Regiones de AWS.

Temas

- [Solucionar problemas de permisos de transferencia entre regiones](#)
- [Solucione los problemas de rendimiento de las transferencias entre regiones](#)

Solucionar problemas de permisos de transferencia entre regiones

Descripción

Al intentar transferir archivos entre buckets de Amazon S3 en diferentes regiones mediante flujos de trabajo de Transfer Family, se producen errores como los siguientes:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "Access Denied (Service: Amazon S3; Status Code: 403; Error Code: AccessDenied)",
    "stepType": "COPY",
    "stepName": "cross_region_copy"
  }
}
```

Causa

Cross-region las transferencias requieren permisos de IAM específicos para los buckets de origen y destino. Es posible que la función de IAM utilizada por su servidor o flujo de trabajo de Transfer Family no tenga permisos suficientes para acceder a los buckets de otras regiones.

Solución

Para resolver problemas de permisos de transferencia entre regiones:

1. Asegúrese de que su función de IAM tenga permisos tanto para los depósitos de origen como de destino:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
```

```

        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::source-bucket-name/*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:::destination-bucket-name/*"
  }
]
}

```

2. Si utilizas el cifrado KMS, añade permisos para las claves KMS de origen y destino:

```

{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": [
    "arn:aws:kms:source-region:account-id:key/source-key-id",
    "arn:aws:kms:destination-region:account-id:key/destination-key-id"
  ]
}

```

3. Compruebe que las políticas de bucket de ambas regiones permiten el acceso desde la función de IAM de su servidor Transfer Family
4. Para las transferencias entre cuentas, asegúrate de que estén configurados los permisos entre cuentas adecuados

Solucione los problemas de rendimiento de las transferencias entre regiones

Descripción

Cross-region las transferencias son considerablemente más lentas de lo esperado o se agotan durante las transferencias de archivos grandes.

Causa

Cross-region Las transferencias implican de forma inherente una mayor latencia y pueden verse afectadas por las condiciones de la red, el tamaño de los archivos y los límites del servicio. Los archivos grandes o los grandes volúmenes de archivos pequeños pueden sufrir una degradación del rendimiento.

Solución

Para mejorar el rendimiento de las transferencias entre regiones:

- Para archivos de gran tamaño, considere la posibilidad de utilizar Amazon S3 Transfer Acceleration:

```
aws s3 cp --source-region us-east-1 --region us-west-2 \  
s3://source-bucket/large-file.zip s3://destination-bucket/large-file.zip \  
--acl bucket-owner-full-control --s3-accelerate
```

- Para varios archivos pequeños, agréguelos antes de transferirlos:
 - Usa la compresión para combinar varios archivos
 - Utilice las operaciones por lotes de Amazon S3 para transferencias a gran escala
- Considere la posibilidad de utilizar conectores SFTP de Transfer Family con la configuración de tiempo de espera adecuada para transferencias grandes
- Para las transferencias recurrentes, considere la posibilidad de replicar los datos mediante Amazon S3 Cross-Region Replication (CRR) en lugar de transferencias ad hoc
- Supervisa el rendimiento de las transferencias con CloudWatch las métricas de Amazon para identificar los cuellos de botella

Solucionar problemas de implementación de Terraform

En esta sección se describen las posibles soluciones para los problemas relacionados con la implementación de los recursos de Transfer Family mediante Terraform. Para obtener información general sobre los módulos de Terraform para Transfer Family, consulte [Módulos Transfer Family Terraform](#).

Temas

- [Solucione los errores de creación de recursos de Terraform](#)

- [Solucione los problemas de administración del estado de Terraform](#)

Solucione los errores de creación de recursos de Terraform

Descripción

Al intentar crear recursos de Transfer Family con Terraform, se producen errores como:

```
Error: error creating Transfer Server: InvalidRequestException: The request is not valid.  
Error: error creating Transfer User: InvalidRequestException: Unable to create the user because the server endpoint type is incompatible with the home directory type.
```

Causa

Estos errores suelen producirse debido a parámetros de configuración incompatibles o a la falta de dependencias en la configuración de Terraform. Entre las causas comunes, se incluyen las siguientes:

- Configuraciones de almacenamiento y tipo de punto final incompatibles
- Faltan las funciones o políticas de IAM requeridas
- Especificaciones de la política de seguridad incorrectas
- Problemas de configuración de terminales de VPC

Solución

Para resolver los problemas de implementación de Terraform:

- Asegúrese de que su configuración de Terraform utilice combinaciones de parámetros compatibles:
 - En el caso de los puntos de enlace públicos, asegúrese de utilizar Amazon S3 para el almacenamiento.
 - En el caso de los puntos finales de la VPC, compruebe la configuración adecuada de la VPC y del grupo de seguridad.
- Utilice dependencias explícitas con el `depends_on` atributo para garantizar que los recursos se creen en el orden correcto.

- Compruebe que todas las funciones de IAM tengan las relaciones de confianza y los permisos necesarios.
- Utilice la última versión del AWS proveedor de Terraform para garantizar la compatibilidad con todas las funciones de Transfer Family.
- Para despliegues complejos y casos de uso sencillos, considere utilizar los módulos oficiales de Transfer Family Terraform disponibles en GitHub . <https://github.com/aws-ia/terraform-aws-transfer-family> Estos módulos proporcionan ejemplos exhaustivos que cubren casos de uso simples y complejos de los clientes, siguen las AWS mejores prácticas y pueden simplificar la implementación para los clientes que necesitan ayuda con la configuración de la infraestructura como código (IaC).

Solucione los problemas de administración del estado de Terraform

Descripción

Después de realizar cambios en tus recursos de Transfer Family fuera de Terraform (a través de la consola o AWS CLI), te encuentras con cambios de estado o errores al ejecutar `terraform plan` o `terraform apply`.

Causa

Terraform mantiene un archivo de estado que rastrea los recursos que administra. Cuando se realizan cambios fuera de Terraform, el archivo de estado deja de estar sincronizado con los recursos reales, lo que provoca errores o un comportamiento inesperado durante las operaciones posteriores de Terraform.

Solución

Para resolver los problemas de administración del estado de Terraform con los recursos de Transfer Family:

1. Úselo `terraform import` para poner los recursos existentes bajo la administración de Terraform:

```
terraform import <transfer_family_server.example> s-<server-id>
terraform import <transfer_family_server.example> s-<server-id>/username
```

2. Se utiliza `terraform refresh` para actualizar el archivo de estado con la infraestructura actual del mundo real

3. En el caso de los recursos que no se puedan importar o que tengan problemas de estado complejos, considere `terraform state rm` eliminarlos del archivo de estado y volver a crearlos con Terraform
4. Implemente una política para administrar los recursos de Transfer Family exclusivamente a través de Terraform para evitar futuros cambios de estado
5. Utilice el almacenamiento de estado remoto con bloqueo para evitar modificaciones simultáneas cuando trabaje en equipo

Solución de problemas de integración de Web Application Firewall

En esta sección se describen las posibles soluciones para los problemas relacionados AWS WAF con la integración con Transfer Family.

Temas

- [Solucione los problemas del WAF que bloquea el tráfico legítimo](#)
- [Solucione los problemas de integración de WAF con proveedores de identidad personalizados](#)

Solucione los problemas del WAF que bloquea el tráfico legítimo

Descripción

Tras realizar la configuración AWS WAF con su terminal Transfer Family, los usuarios legítimos no pueden conectarse o sufren fallos de conexión intermitentes. Es posible que veas respuestas HTTP 403 (prohibidas) en tus registros.

Causa

Es posible que tus AWS WAF reglas sean demasiado restrictivas o estén mal configuradas, lo que provoque falsos positivos que bloqueen el tráfico legítimo. Entre las causas comunes, se incluyen las siguientes:

- IP-based reglas que bloquean inadvertidamente las redes corporativas o las VPN
- Rate-based reglas con umbrales demasiado bajos para sus patrones de tráfico normales
- Grupos de reglas gestionados que son demasiado agresivos para su caso de uso

Solución

Para resolver problemas de falsos positivos:

1. Habilite el AWS WAF registro para identificar qué reglas están activando los bloqueos. Para obtener instrucciones, consulte [Registrar el tráfico de ACL AWS WAF web](#).
2. Revisa tus registros para identificar patrones en las solicitudes bloqueadas.
3. Ajusta tus reglas de la siguiente manera:
 - Añadir direcciones IP o rangos a una lista de direcciones IP permitidas
 - Aumentar los límites de velocidad para las reglas basadas en tasas
 - Establecer reglas específicas para el modo de recuento en lugar del modo de bloqueo para monitorear sin bloquear
 - Crear excepciones para reglas específicas mediante exclusiones de grupos de reglas
4. Pruebe la configuración actualizada con una muestra representativa de tráfico legítimo antes de implementarla por completo.

Solucione los problemas de integración de WAF con proveedores de identidad personalizados

Descripción

Tras configurarlo AWS WAF con el servidor Transfer Family que usa un proveedor de identidad personalizado, la autenticación falla o los usuarios experimentan problemas de autenticación intermitentes.

Causa

Al utilizar un proveedor de identidad personalizado con API Gateway, AWS WAF las reglas pueden interferir con las llamadas a la API entre Transfer Family y tu proveedor de identidad. Esto puede suceder porque AWS WAF está inspeccionando y potencialmente bloqueando el tráfico de la API en función de sus conjuntos de reglas.

Solución

Para resolver problemas con AWS WAF los proveedores de identidad personalizados, haz lo siguiente:

- Asegúrese de que su AWS WAF configuración incluya excepciones para los puntos de enlace de API Gateway utilizados por su proveedor de identidad personalizado.

- Agrega al director del servicio Transfer Family (transfer.amazonaws.com) a una lista de permitidos en tus reglas. AWS WAF
- Si utilizas grupos de reglas administrados, revísalos para ver si hay reglas que puedan afectar a los flujos de autenticación de la API y considera la posibilidad de deshabilitar esas reglas específicas.
- Prueba su proveedor de identidad directamente mediante la operación de la TestIdentityProvider API para comprobar que funciona correctamente sin AWS WAF interferencias.

Solucionar problemas de usuarios gestionados por el servicio

En esta sección se describen las posibles soluciones para los problemas de los usuarios gestionados por el servicio.

Temas

- [Solución de los problemas de los usuarios administrados por el servicio](#)

Solución de los problemas de los usuarios administrados por el servicio

En esta sección, se describen las posibles soluciones para los siguientes problemas.

Temas

- [Solución de problemas con cuerpo de la clave pública demasiado largo](#)
- [Solución de problemas no pudo agregar la clave pública SSH](#)

Solución de problemas con cuerpo de la clave pública demasiado largo

Descripción

Cuando intenta crear un usuario administrado por el servicio, recibe el siguiente error:

```
Failed to create user (1 validation error detected:  
'sshPublicKeyBody' failed to satisfy constraint: Member must have length less than or  
equal to 2048)
```

Causa

Es posible que esté introduciendo una clave PGP para el cuerpo de la clave pública y que AWS Transfer Family no admita las claves PGP para los usuarios gestionados por el servicio.

Solución

Si la clave PGP lo es RSA-based, puede convertirla al formato PEM. Por ejemplo, Ubuntu proporciona una herramienta de conversión aquí: <https://manpages.ubuntu.com/manpages/jammy/en/man1/openpgp2ssh.1.html>

Solución de problemas no pudo agregar la clave pública SSH

Descripción

Cuando intenta añadir una clave pública para un usuario administrado por el servicio, recibe el siguiente error:

```
Failed to add SSH public key (Unsupported or invalid SSH public key format)
```

Causa

Puede que estés intentando importar una clave SSH2-formatted pública y que AWS Transfer Family no las admita para los SSH2-formatted usuarios gestionados por el servicio.

Solución

Debe convertir la clave al formato OpenSSH. Este proceso se describe en [Convertir una clave SSH2 al formato de clave pública SSH](#).

Solución de los problemas de AS2

En esta sección se describen las posibles soluciones para los problemas relacionados con las transferencias AS2.

Temas

- [Solución de los problemas de AS2](#)
- [Problemas con el certificado AS2](#)
- [Problemas con los recibos de AS2 MDN](#)
- [Problemas de supervisión del vencimiento de los certificados](#)

Solución de los problemas de AS2

[Códigos de error de AS2](#), los mensajes y las sugerencias de solución de problemas para los servidores compatibles con la Declaración de Aplicabilidad 2 (AS2) se describen en la sección de códigos de error AS2 de esta guía.

Problemas con el certificado AS2

Descripción

Está experimentando errores relacionados con los certificados con las transferencias de AS2.

Causa

Entre las causas más comunes se incluyen los certificados caducados, los formatos de certificado incorrectos o las cadenas de certificados que no coinciden.

Solución

Pruebe las siguientes soluciones:

- Compruebe que sus certificados no estén caducados
- Asegúrese de que los certificados estén en el formato correcto (PEM para AWS Transfer Family)
- Compruebe que la cadena de certificados esté completa y sea válida
- Confirme que los certificados de firma y cifrado coinciden entre los socios comerciales
- Rote los certificados mucho antes de que caduquen para evitar interrupciones

Problemas con los recibos de AS2 MDN

Descripción

No recibes las notificaciones de disposición de mensajes (mDNS) esperadas para las transferencias AS2.

Causa

Los problemas de MDN pueden deberse a problemas de conectividad de red, a configuraciones incorrectas de los terminales o a discordancias entre los formatos de MDN.

Solución

Considera estas soluciones:

- Verifica que la URL de MDN esté correctamente configurada y accesible
- Compruebe la conectividad de red entre el servidor AS2 y el punto final MDN
- Asegúrese de que ambos socios comerciales estén configurados para el mismo tipo de MDN (síncrono o asíncrono)
- Revisa los registros de AS2 para ver si hay errores relacionados con el procesamiento de MDN
- Si utilizas mDNS sincrónico, verifica que los tiempos de espera estén configurados adecuadamente

Problemas de supervisión del vencimiento de los certificados

En esta sección se proporcionan soluciones para problemas comunes relacionados con la monitorización de la caducidad de los certificados y la DaysUntilExpiry métrica.

DaysUntilExpiry la métrica no aparece

Problema: la DaysUntilExpiry métrica no está visible en Amazon CloudWatch después de importar un certificado.

Solución:

- Espere hasta 24 horas después de importar el certificado. Transfer Family puede tardar hasta un día completo en emitir la métrica a tu cuenta.
- Asegúrate de buscar en la AWS región correcta y debajo del espacio de AWS/Transfer nombres. CloudWatch

Las alarmas de caducidad de los certificados no se activan

Problema: CloudWatch las alarmas de caducidad de los certificados no se activan cuando se esperaba.

Solución:

- Compruebe que la alarma esté configurada con la Maximum estadística y un período de 1 día.
- Compruebe que la comparación de umbrales esté configurada en Less than or equal to el número de días deseado.

- Asegúrese de que `Treat missing data as good (not breaching)` esté seleccionado en la configuración de la alarma.
- Compruebe que las dimensiones de la alarma coincidan con las del certificado `CertificateId` y la descripción (si se proporcionan).
- Compruebe que las acciones de alarma (temas de SNS, notificaciones por correo electrónico) estén configuradas y activas correctamente.

AWS Transfer Family referencia de la API

La guía completa de referencia de API para Transfer Family está disponible en [AWS Transfer Family API Reference](#).

AWS Transfer Family es un servicio de transferencia segura que puede utilizar para transferir archivos desde y hacia el almacenamiento del Amazon Simple Storage Service (Amazon S3) mediante los siguientes protocolos:

- Protocolo de File Transfer (SFTP) Secure Shell (SSH)
- Protocolo seguro de File Transfer (FTPS)
- Protocolo de File Transfer (FTP)
- Declaración de aplicabilidad 2 (AS2)

Los servidores, usuarios y roles se identifican por su nombre de recurso de Amazon (ARN). Puede asignar etiquetas, que son pares clave-valor, a las entidades con un ARN. Las etiquetas son metadatos que se pueden utilizar para agrupar o buscar estas entidades. Un ejemplo donde las etiquetas resultan útiles es en contabilidad.

En los formatos de AWS Transfer Family identificación se respetan las siguientes convenciones:

- Los valores `ServerId` adoptan la forma `s-01234567890abcdef`.
- Los valores `SshPublicKeyId` adoptan la forma `key-01234567890abcdef`.

Los formatos del nombre de recurso de Amazon (ARN) adoptan esta forma:

- En el caso de los servidores, los ARN adoptan la forma `arn:aws:transfer:region:account-id:server/server-id`.

Un ejemplo de ARN de un servidor es `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

- En el caso de los usuarios, los ARN adoptan la forma `arn:aws:transfer:region:account-id:user/server-id/username`.

Un ejemplo es `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

Las entradas de DNS (puntos de conexión) en uso son:

- Los puntos de enlace de la API adoptan la forma `transfer.region.amazonaws.com`.
- Los puntos de enlace de servidor adoptan la forma `server-id.server.transfer.region.amazonaws.com`.

Esta referencia de interfaz API para AWS Transfer Family contiene documentación sobre una interfaz de programación que puede usar para administrar AWS Transfer Family. La estructura de la referencia es la siguiente:

- Para obtener una lista alfabética de las acciones, consulte la [Actions](#).
- Para ver una lista de tipos de datos ordenada alfabéticamente, consulte [Types](#).
- Para ver una lista de parámetros de consulta comunes, consulte el tema relacionado con los [parámetros comunes](#).
- Para ver las descripciones de los códigos de error, consulte el tema relacionado con los [errores comunes](#).

Tip

En lugar de ejecutar un comando, puede usar el parámetro `--generate-cli-skeleton` con cualquier llamada a la API para generar y mostrar una plantilla de parámetros. Después puede utilizar la plantilla generada para personalizarla y utilizarla como entrada en un comando posterior. Para más información, consulte [Generar y usar un archivo básico de parámetros](#).

Cómo realizar solicitudes a la API

Además de usar la consola, puede usar la AWS Transfer Family API para configurar y administrar sus servidores mediante programación. En esta sección se describen las AWS Transfer Family operaciones, la firma de solicitudes para la autenticación y la gestión de errores. Para obtener más información acerca de las regiones y los puntos de conexión disponibles para Transfer Family, consulte los [puntos de conexión y cuotas de AWS Transfer Family](#) en Referencia general de AWS.

Note

También puede utilizar los AWS SDK al desarrollar aplicaciones con Transfer Family;. Los AWS SDK para Java, .NET y PHP envuelven la API de Transfer Family subyacente, lo que simplifica las tareas de programación. Para obtener información sobre la descarga de las bibliotecas de SDK, consulte [Código de muestra de bibliotecas](#).

Cabeceras de solicitud obligatorias para Transfer Family

En esta sección se describen los encabezados obligatorios que debe enviar con cada solicitud POST a AWS Transfer Family. Puede incluir encabezados HTTP para identificar información clave sobre la solicitud, incluidas la operación que desea invocar, la fecha de la solicitud y la información que indica su autorización como remitente de la solicitud. Los encabezados no distinguen entre mayúsculas y minúsculas y el orden de los encabezados no es importante.

El siguiente ejemplo muestra los encabezados que se utilizan en la [ListServers](#) operación.

```
POST / HTTP/1.1
Host: transfer.us-east-1.amazonaws.com
x-amz-target: TransferService.ListServers
x-amz-date: 20220507T012034Z
Authorization: AWS4-HMAC-SHA256 Credential=AKIDEXAMPLE/20220507/us-east-1/transfer/
aws4_request,
    SignedHeaders=content-type;host;x-amz-date;x-amz-target,
    Signature=13550350a8681c84c861aac2e5b440161c2b33a3e4f302ac680ca5b686de48de
Content-Type: application/x-amz-json-1.1
Content-Length: 17

{"MaxResults":10}
```

Los siguientes son los encabezados que se deben incluir con las solicitudes POST a Transfer Family. Los encabezados que se muestran a continuación y que comienzan por «x-amz» son específicos de AWS. El resto de los encabezados que se muestran son encabezados comunes utilizados en transacciones HTTP.

Entrada y firma de la solicitud de Transfer Family

Todas las entradas de la solicitud deben enviarse como parte de la carga útil de JSON en el cuerpo de la solicitud. En el caso de las acciones en las que todos los campos de solicitud son opcionales,

por ejemplo `ListServers`, tendrá que proporcionar un objeto JSON vacío en el cuerpo de la solicitud, por ejemplo, `{}`. La estructura de la carga útil de Transfer Family request/response está documentada, por ejemplo [DescribeServer](#), en la referencia de la API existente.

Transfer Family admite la autenticación mediante AWS Signature Version 4. Para obtener más información, consulte [Firmar solicitudes de API de AWS](#).

Respuestas de error

Cuando se produce un error, la información de encabezado de la respuesta contiene:

- Content-Type: `application/x-amz-json-1.1`
- Un código de estado HTTP 4xx o 5xx adecuado

El cuerpo de una respuesta de error contiene información sobre el error que se ha producido. El siguiente ejemplo de respuesta de error muestra la sintaxis de salida de los elementos de respuesta comunes a todas las respuestas de error.

```
{
  "__type": "String",
  "Message": "String", <!-- Message is lowercase in some instances -->
  "Resource": "String",
  "ResourceType": "String",
  "RetryAfterSeconds": "String"
}
```

En la tabla siguiente se explican los campos de respuesta de error JSON que se muestran en la sintaxis anterior.

`__type`

Una de las excepciones de una llamada a la API Transfer Family.

Tipo: cadena

Mensaje o mensaje

Uno de los mensajes de código de error de operación.

 Note

Algunas excepciones usan `message` y otras usan `Message`. Puede comprobar el código de la interfaz para determinar el tipo de mayúsculas y minúsculas adecuado. Como alternativa, puede probar cada opción para ver cuál funciona.

Tipo: cadena

Resource

El recurso para el que se invoca el error. Por ejemplo, si intenta crear un usuario que ya existe, el `Resource` es el nombre de usuario del usuario existente.

Tipo: cadena

ResourceType

El tipo de recurso para el que se invoca el error. Por ejemplo, si intenta crear un usuario que ya existe, el `ResourceType` es `User`.

Tipo: cadena

RetryAfterSeconds

La cantidad de segundos que se debe esperar antes de volver a intentar el comando.

Tipo: cadena

Ejemplos de respuestas de error

Si llama a la API de `DescribeServer` y especifica un servidor que no existe, se devuelve el siguiente cuerpo de JSON.

```
{
  "__type": "ResourceNotFoundException",
  "Message": "Unknown server",
  "Resource": "s-11112222333344444",
  "ResourceType": "Server"
}
```

Si la ejecución de una API provoca una limitación, se devuelve el siguiente cuerpo de JSON.

```
{
  "__type": "ThrottlingException",
  "RetryAfterSeconds": "1"
}
```

Si utiliza la API de `CreateServer` y no tiene permisos suficientes para crear un servidor de Transfer Family, se devuelve el siguiente cuerpo de JSON.

```
{
  "__type": "AccessDeniedException",
  "Message": "You do not have sufficient access to perform this action."
}
```

Si utiliza la API de `CreateUser` y especifica un usuario que ya existe, se devuelve el siguiente cuerpo de JSON.

```
{
  "__type": "ResourceExistsException",
  "Message": "User already exists",
  "Resource": "Alejandro-Rosalez",
  "ResourceType": "User"
}
```

Bibliotecas disponibles

AWS proporciona bibliotecas, códigos de muestra, tutoriales y otros recursos para los desarrolladores de software que prefieren crear aplicaciones mediante API específicas del idioma en lugar de las herramientas de línea de comandos y la API de Query. Estas bibliotecas proporcionan funciones básicas (que no se incluyen en las API), como la autenticación de solicitudes, los reintentos de solicitudes y la gestión de errores para que se pueda comenzar más fácilmente.

[Consulte Herramientas a partir de las cuales desarrollar AWS](#)

Para ver las bibliotecas y código de ejemplo en todos los idiomas, consulte [Código de muestra y bibliotecas](#).

Proveedores de identidad

AWS Transfer Family admite varios tipos de proveedores de identidad para autenticar y administrar los usuarios. Cada servidor solo puede usar un método de autenticación, que debe seleccionarse al crear el servidor.

Servicio gestionado

Con el método de `SERVICE_MANAGED` autenticación, las credenciales de usuario se almacenan y gestionan en el AWS Transfer Family. Los usuarios se autentican mediante claves públicas SSH asociadas a su nombre de usuario en el servidor.

Cada usuario puede tener una o más claves públicas de SSH almacenadas en el servicio. Cuando un cliente solicita una operación de archivo, proporciona el nombre de usuario y la clave privada de SSH, que se autentica con la clave pública almacenada.

Directory Service

El método de `AWS_DIRECTORY_SERVICE` autenticación le permite integrarse con AWS Directory Service para Microsoft Active Directory (AWS Directory Service for Microsoft Active Directory).

Esta opción le permite administrar la autenticación y el acceso de los usuarios a través de los grupos de Active Directory existentes. Los usuarios pueden autenticarse con sus credenciales de Active Directory.

Hay un límite predeterminado de 100 grupos de Active Directory por servidor, que se puede aumentar hasta un máximo de 150 grupos mediante un aumento del límite de servicio.

Lambda

El método de `AWS_LAMBDA` autenticación le permite conectarse a un proveedor de identidad personalizado mediante AWS Lambda.

Esta opción proporciona flexibilidad para integrarse con sus sistemas de administración de identidades existentes. La función Lambda es responsable de autenticar a los usuarios y devolver las políticas de acceso adecuadas.

Personalizado (API Gateway)

El método de `API_GATEWAY` autenticación (que se muestra como personalizado en la consola) permite utilizar un método de autenticación personalizado que proporciona tanto la autenticación del usuario como el control del acceso.

Este método consiste en que la Amazon API Gateway utiliza una llamada a la API del proveedor de identidad para validar las solicitudes de los usuarios. Puede utilizar este método personalizado para autenticar a los usuarios mediante un servicio de directorio, un name/password par de bases de datos o algún otro mecanismo.

Para todos los métodos de autenticación, a los usuarios se les asignan políticas que definen su acceso a los buckets de Amazon S3 o a los sistemas de archivos de Amazon Elastic File System. El servidor hereda la relación de confianza del usuario a través de un rol de IAM con una `AssumeRole` acción, lo que le permite realizar operaciones de archivos en nombre del usuario.

Convenciones de nomenclatura

AWS Transfer Family utiliza formatos estandarizados para los identificadores de recursos y los nombres de recursos de Amazon (ARN). Es importante comprender estas convenciones a la hora de trabajar con la AWS Transfer Family API.

Formatos de ID

En los formatos de AWS Transfer Family ID se respetan las siguientes convenciones:

ID de servidor

Los valores `ServerId` adoptan la forma `s-01234567890abcdef`.

ID de clave pública de SSH

Los valores `SshPublicKeyId` adoptan la forma `key-01234567890abcdef`.

ID de conector

Los valores `ConnectorId` adoptan la forma `c-01234567890abcdef`.

ID de flujo de trabajo

Los valores `WorkflowId` adoptan la forma `w-01234567890abcdef`.

IDs de perfil

Los valores `ProfileId` adoptan la forma `p-01234567890abcdef`.

WebApp IDs

Los valores `WebAppId` adoptan la forma `webapp-01234567890abcdef`.

Formatos ARN

Los formatos del nombre de recurso de Amazon (ARN) adoptan esta forma:

ARN de servidor

En el caso de los servidores, los ARN adoptan la forma

`arn:aws:transfer:region:account-id:server/server-id.`

Ejemplo: `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef.`

ARN de usuario

En el caso de los usuarios, los ARN adoptan la forma `arn:aws:transfer:region:account-id:user/server-id/username.`

Ejemplo: `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1.`

ARN de conector

En el caso de los conectores, los ARN adoptan la forma.

`arn:aws:transfer:region:account-id:connector/connector-id`

Ejemplo: `arn:aws:transfer:us-east-1:123456789012:connector/c-01234567890abcdef.`

Los ARN del flujo de trabajo

En el caso de los flujos de trabajo, los ARN adoptan la forma.

`arn:aws:transfer:region:account-id:workflow/workflow-id`

Ejemplo: `arn:aws:transfer:us-east-1:123456789012:workflow/w-01234567890abcdef.`

WebApp Los ARN

En el caso de las aplicaciones web, los ARN adoptan la forma.

`arn:aws:transfer:region:account-id:webapp/webapp-id`

Ejemplo: `arn:aws:transfer:us-east-1:123456789012:webapp/webapp-01234567890abcdef.`

Puede asignar etiquetas, que son pares clave-valor, a las entidades con un ARN. Las etiquetas son metadatos que se pueden utilizar para agrupar o buscar estas entidades. Un ejemplo donde las etiquetas resultan útiles es en contabilidad.

DNS y puntos finales

AWS Transfer Family utiliza convenciones de nomenclatura de DNS estandarizadas tanto para los puntos finales de la API como para los puntos finales del servidor. Comprender estos puntos finales es fundamental para configurar los clientes y realizar llamadas a la API.

Puntos de conexión de API

Los puntos finales de la API se utilizan para realizar llamadas a la API con el fin de gestionar los recursos AWS Transfer Family . Estos puntos finales adoptan las siguientes formas:

Puntos finales de API estándar

Los puntos finales de la API estándar adoptan la forma. `transfer.region.amazonaws.com`

Ejemplo: `transfer.us-east-1.amazonaws.com`

Dual-Stack Los puntos finales de la API

AWS Transfer Family ofrece puntos de enlace de API de doble pila a los que se puede acceder mediante solicitudes de IPv4 o IPv6:

- `https://transfer.region-code.api.aws`
- `https://transfer-fips.region-code.api.aws`

Puntos finales del servidor

Los clientes de transferencia de archivos utilizan los puntos finales del servidor para conectarse a AWS Transfer Family los servidores. Estos puntos finales adoptan las siguientes formas:

Puntos finales de servidor estándar

Los puntos finales de servidor estándar adoptan la forma. `server-id.server.transfer.region.amazonaws.com`

Ejemplo: `s-01234567890abcdef.server.transfer.us-east-1.amazonaws.com`

Nombres de host personalizados

También puede configurar nombres de host personalizados para sus servidores. AWS Transfer Family Los nombres de host personalizados se pueden usar para proporcionar una experiencia más fácil de usar o de marca para sus usuarios.

Para usar un nombre de host personalizado, debes:

1. Ser propietario del nombre de dominio
2. Proporcione un certificado válido
3. Configure los registros DNS para que apunten a su AWS Transfer Family servidor

Para obtener una lista completa de los AWS Transfer Family puntos finales por AWS región, consulte los [AWS Transfer Family puntos finales y las cuotas](#) en. Referencia general de AWS

Historial de documentos para AWS Transfer Family

En la siguiente tabla se describe la documentación de esta versión de AWS Transfer Family.

- Versión de API: transfer-2018-11-05
- Última actualización de la documentación: 19 de noviembre de 2025

Cambio	Descripción	Fecha
Compatibilidad con terminales de VPC para aplicaciones web Transfer Family	AWS Transfer Family las aplicaciones web ahora admiten puntos de enlace alojados en VPC, lo que le permite alojar el punto de enlace de su aplicación web dentro de una nube privada virtual para transferencias de datos privados hacia y desde Amazon S3 sin tener que atravesar la Internet pública. Para obtener más información, consulte Creación de una aplicación web de Transfer Family en una VPC .	19 de noviembre de 2025
Compatibilidad con IPv6	AWS Transfer Family ahora admite terminales de doble pila (IPv4 e IPv6) para terminales públicos de SFTP, terminales para conectores SFTP y AS2 SFTP/FTPS /FTP/AS2 y VPC-internal terminales API. Para obtener más información, consulte	30 de junio de 2025

Cambio	Descripción	Fecha
	Compatibilidad con IPv6 para servidores Transfer Family.	
Mejoras en la experiencia de usuario de los conectores SFTP	• Posibilidad de configurar automáticamente las conexiones simultáneas para sus conectores • Capacidad para proporcionar una clave privada SSH en formato OpenSSH que se utiliza para autenticar las conexiones • Posibilidad de descubrir la clave de host pública de los servidores remotos mediante sus conectores SFTP Para obtener más información, consulte Cree un conector SFTP con salida gestionada por el servicio.	9 de abril de 2025

Cambio	Descripción	Fecha
Los conectores SFTP permiten eliminar, cambiar el nombre y mover archivos en el servidor SFTP remoto	Ahora puede organizar los archivos almacenados en servidores SFTP remotos eliminando, cambiando el nombre o moviendo los archivos de origen a las ubicaciones de almacenamiento después de haberlos copiado del servidor remoto. Para obtener más información, consulte Mueva o cambie el nombre de los archivos o directorios del servidor SFTP remoto.	7 de abril de 2025
Support para aplicaciones AWS Transfer Family web	AWS Transfer Family las aplicaciones web son un nuevo recurso que los clientes pueden utilizar para crear una interfaz sencilla para acceder a sus datos en Amazon S3 a través de un navegador web. Para obtener más información, consulte Aplicaciones web Transfer Family.	1 de diciembre de 2024
Se trasladó la referencia de la API a una guía independiente	Para mejorar la experiencia del cliente, la referencia de la API ahora se publica por separado de la guía del usuario. Para ver la referencia independiente sobre la API, consulte Bienvenido a la AWS Transfer Family API.	31 de julio de 2024

Cambio	Descripción	Fecha
Posibilidad de que los conectores SFTP enumeren archivos y directorios remotos	Transfer Family ha añadido la posibilidad de que nuestros clientes utilicen conectores SFTP para enumerar los archivos almacenados en servidores SFTP remotos. Para obtener más información, consulte Listar el contenido de un directorio remoto	23 de abril de 2024
Posibilidad de utilizar el certificado TLS autofirmado de un socio comercial con el intercambio de mensajes AS2	AWS Transfer Family ha añadido la opción de importar y utilizar el certificado TLS público y autofirmado de un socio comercial para enviar los mensajes de la Declaración de Aplicabilidad 2 (AS2) a su servidor a través de HTTPS.	12 de abril de 2024
Se han añadido políticas de seguridad para los conectores SFTP	AWS Transfer Family ha agregado políticas de seguridad para su uso con los conectores SFTP. Para obtener más información, consulte Políticas de seguridad para AWS Transfer Family Conectores SFTP .	5 de abril de 2024

Cambio	Descripción	Fecha
Intégrelo con Amazon EventBridge	AWS Transfer Family ahora publica automáticamente los eventos en Amazon EventBridge para todas las operaciones de transferencia de archivos. Para obtener más información, consulte Administración Transfer Family eventos que utilizan Amazon EventBridge .	8 de febrero de 2024
Adición de nuevas políticas de seguridad	AWS Transfer Family ha agregado nuevas políticas de seguridad FIPS y no FIPS. Además, la política de seguridad predeterminada que se asigna a los servidores es siempre la política de seguridad más reciente. Para obtener más información, consulte Políticas de seguridad para AWS Transfer Family servidores .	5 de febrero de 2024

Cambio	Descripción	Fecha
Support para direcciones IP estáticas para conectores SFTP y AS2	Transfer Family ahora proporciona direcciones IP estáticas para conectores SFTP y AS2. Esto permite la conexión con servidores SFTP remotos que están protegidos por controles de listas de direcciones IP permitidas. En el caso del AS2, vamos a introducir direcciones IP estáticas para las respuestas MDN asíncronas de los servidores AS2.	16 de enero de 2024
La guía del usuario se ha reorganizado para adaptarla mejor a la versión más reciente de. AWS Transfer Family	Transfer Family ha agregado múltiples funciones desde que se creó la guía, por lo que fue necesaria una reestructuración de la guía.	3 de enero de 2024

Cambio	Descripción	Fecha
Mejoras en los mapeos de directorios lógicos Optimización del rendimiento de la lista Amazon S3	Transfer Family ahora admite mapeos de directorios lógicos de hasta 2,1 MB. Ahora también puede declarar si la asignación de un usuario se realiza a un archivo. Para obtener más información, consulte Reglas para el uso de directorios lógicos. Al crear o actualizar un servidor que utiliza Amazon S3 para el almacenamiento, ahora puede optimizar el rendimiento de la lista de sus directorios (o carpetas) de S3. Para obtener más información, consulte Configuración de un punto final de servidor SFTP, FTPS o FTP.	17 de noviembre de 2023
Puerto alternativo para servidores SFTP con puntos finales de nube privada virtual (VPC)	Ahora puede habilitar un puerto no estándar alternativo para los servidores de SFTP Transfer Family que tienen puntos de conexión de VPC. Para obtener más información, consulte Creación de un servidor en una nube privada virtual (VPC).	17 de noviembre de 2023

Cambio	Descripción	Fecha
Soporte para conectores SFTP	Los conectores SFTP amplían las capacidades de AWS Transfer Family comunicación con servidores remotos tanto en la nube como en las instalaciones. Para obtener más información, consulte Uso de conectores SFTP .	25 de julio de 2023
Soporte para la autenticación AS2 Basic	Transfer Family ahora admite el uso de autenticación básica para servidores que utilicen el protocolo Applicability Statement 2 (AS2). Para obtener más información, consulte Autenticación básica para conectores AS2 .	30 de junio de 2023
Soporte para el registro estructurado de JSON	Transfer Family ahora admite la entrega de registros JSON estructurados a Amazon CloudWatch, la agrupación de flujos de registros en grupos de registros personalizados y la realización de consultas de registro comunes en todos los protocolos. Para obtener más información, consulte CloudWatch Registro de Amazon para AWS Transfer Family servidores .	24 de junio de 2023

Cambio	Descripción	Fecha
Soporte para múltiples métodos de autenticación	Transfer Family admite la autenticación mediante una contraseña, un public/private key pair o ambos. Está disponible para los servidores que utilizan el protocolo SFTP y un proveedor de identidad personalizado. Para obtener más información, consulte Crea un SFTP-enabled servidor .	17 de mayo de 2023
Compatibilidad para el descifrado de Pretty Good Privacy (PGP) con los archivos que Transfer Family procesa mediante flujos de trabajo	Transfer Family cuenta con compatibilidad integrada para el descifrado Pretty Good Privacy (PGP). Puede utilizar el descifrado PGP en los archivos que se carguen mediante SFTP, FTPS o FTP a Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS). Para obtener más información, consulte Generar claves PGP y Utilizar el descifrado PGP en su flujo de trabajo .	21 de diciembre de 2022

Cambio	Descripción	Fecha
Soporte totalmente administrado para el protocolo de transferencia de archivos de Applicability Statement 2 (AS2) con servidores de Transfer Family	Puede crear servidores que utilicen el protocolo AS2 para enviar y recibir información desde y hacia socios comerciales que se encuentren dentro o fuera del AWS entorno. Para obtener más información, consulte Configuración de AS2 .	25 de julio de 2022
Soporte para mostrar banners al crear un servidor	Puede añadir mensajes personalizados al crear servidores. Puede mostrar un mensaje previo a la autenticación (todos los protocolos) y un mensaje posterior a la autenticación (para los servidores FTP y FTPS). Para obtener más información, consulte Crea un SFTP-enabled servidor , Cree un FTPS-enabled servidor o Cree un servidor FTP-enabled .	17 de febrero de 2022

Cambio	Descripción	Fecha
Support for AWS Lambda como proveedor de identidad	Ahora puede conectarse a un proveedor de identidad personalizado AWS Lambda mediante sus servidores Transfer Family. Anteriormente, tenías que proporcionar un URL Amazon API Gateway para integrar un proveedor de identidades personalizado. Para obtener más información, consulte Se utiliza AWS Lambda para integrar su proveedor de identidad .	16 de noviembre de 2021
Soporte para flujos de trabajo de File Transfer administrados	Los flujos de trabajo de File Transfer administrados le proporcionan abstracciones de procesamiento posteriores a la carga para las tareas habituales que actualmente realiza manualmente. Para obtener más información, consulte AWS Transfer Family flujos de trabajo gestionados .	2 de septiembre de 2021

Cambio	Descripción	Fecha
Support para AWS Directory Service for Microsoft Active Directory	Además de los proveedores de identidad personalizados y gestionados por el servicio, ahora puede utilizarlos AWS Directory Service for Microsoft Active Directory para gestionar el acceso de los usuarios con fines de autenticación y autorización. Para obtener más información, consulte Uso AWS de Directory Service para Microsoft Active Directory .	24 de mayo de 2021
¿Nuevo Regiones de AWS	AWS Transfer Family ya está disponible en la región de África (Ciudad del Cabo). Para más información sobre los puntos de conexión de Transfer Family, consulte Puntos de conexión y cuotas de AWS Transfer Family en Referencia general de AWS.	24 de febrero de 2021
¿Nuevo Regiones de AWS	AWS Transfer Family ya está disponible en las regiones de Asia Pacífico (Hong Kong) y Oriente Medio (Baréin). Para más información sobre los puntos de conexión de Transfer Family, consulte Puntos de conexión y cuotas de AWS Transfer Family en Referencia general de AWS.	17 de febrero de 2021

Cambio	Descripción	Fecha
Soporte para Amazon EFS como almacén de datos	Transfer Family ahora admite transferencias de archivos desde Amazon Elastic File System (Amazon EFS). Amazon EFS es un sistema de archivos NFS elástico simple, escalable y totalmente administrado. Para obtener más información, consulte Configuración de un sistema de archivos Amazon EFS .	6 de enero de 2021
Support para AWS WAF	Transfer Family ahora admite AWS WAF un firewall de aplicaciones web que ayuda a proteger las aplicaciones web y las operaciones de API de los ataques. Para obtener más información, consulte Agregue un cortafuegos de aplicaciones web .	24 de noviembre de 2020
Soporte para varios grupos de seguridad en una nube privada virtual (VPC)	Ahora puede adjuntar varios grupos de seguridad a un servidor de una VPC. Para obtener más información, consulte Creación de un servidor en una nube privada virtual (VPC) .	15 de octubre de 2020

Cambio	Descripción	Fecha
¿Nuevo Regiones de AWS	Transfer Family ya está disponible en las AWS GovCloud (US) regiones. Para obtener más información sobre los puntos de enlace de Transfer Family para AWS GovCloud (US) regiones, consulte AWS Transfer Family puntos de enlace y cuotas en. Referencia general de AWS Para obtener información sobre el uso de Transfer Family en las AWS GovCloud (US) regiones, consulte AWS Transfer Family la Guía del AWS GovCloud (US) usuario.	30 de septiembre de 2020
Ahora puede adjuntar a su servidor una política de seguridad con algoritmos criptográficos compatibles	Ahora puede adjuntar a su servidor una política de seguridad que contenga un conjunto de algoritmos criptográficos compatibles. Para obtener más información, consulte Políticas de seguridad para AWS Transfer Family servidores.	12 de agosto de 2020

Cambio	Descripción	Fecha
Compatibilidad con los puntos de conexión del estándar federal de procesamiento de información (FIPS).	FIPS-enabled Los puntos finales ya están disponibles en Norteamérica Regiones de AWS. Para obtener una lista de las regiones disponibles, consulte los puntos de conexión y cuotas de AWS Transfer Family en Referencia general de AWS. Para habilitar el FIPS para un punto final de SFTP-enabled servidor, consulte. Crea un SFTP-enabled servidor Para habilitar FIPS para un punto final de FTPS-enabled servidor, consulte. Cree un FTPS-enabled servidor Para habilitar FIPS para un punto final de FTP-enabled servidor, consulte. Cree un servidor FTP-enabled	12 de agosto de 2020
Aumento de la longitud de los caracteres del nombre de usuario y caracteres adicionales permitidos	Los nombres de usuario ahora pueden contener signos (@) y puntos (.) y pueden tener una longitud máxima de 100 caracteres. Para añadir un usuario, consulte Administración de usuarios para puntos finales de servidor.	12 de agosto de 2020

Cambio	Descripción	Fecha
Support para la creación automática de roles de Amazon CloudWatch Logging AWS Identity and Access Management (IAM)	Transfer Family ahora admite la creación automática de un rol de IAM de CloudWatch registro para ver la actividad de los usuarios finales. Para obtener más información, consulte Crea un SFTP-enabled servidor , Cree un FTPS-enabled servidor o Cree un servidor FTP-enabled .	30 de julio de 2020
AWS Transfer Family ahora admite la IP de origen como factor de autorización.	Transfer Family admite el uso de direcciones IP de origen de los usuarios finales como factor de autorización, lo que le permite aplicar una capa de seguridad adicional al autorizar el acceso a través del protocolo de File Transfer (SFTP), el protocolo de File Transfer a través de SSL (FTPS) o el protocolo de File Transfer (FTP). Para obtener más información, consulte Uso de proveedores de identidad personalizados .	9 de junio de 2020

Cambio	Descripción	Fecha
AWS Transfer for SFTP ya es compatible con FTP AWS Transfer Family y FTPS y añade soporte para ellos.	Ahora puede usar dos protocolos adicionales para las transferencias de archivos de sus usuarios: el Protocolo de File Transfer seguro (FTPS) y el Protocolo de File Transfer (FTP). Los usuarios pueden mover, ejecutar, proteger e integrar flujos de trabajo basados en FTP sobre SSL (FTPS) y FTP en texto plano AWS, además de la compatibilidad existente con el Protocolo seguro de transferencia de archivos (SFTP).	23 de abril de 2020

Cambio	Descripción	Fecha
Soporte para grupos de seguridad de nube privada virtual (VPC) y direcciones IP elásticas	Ahora puede crear una lista de direcciones IP permitidas para las direcciones IP entrantes mediante grupos de seguridad, lo que proporciona una capa adicional de seguridad para los servidores. También puede asociar direcciones IP elásticas con el punto de conexión de su servidor. De este modo, puede permitir que los usuarios que se encuentran detrás de los firewalls puedan acceder a ese punto de conexión. Para obtener más información, consulte Creación de un servidor en una nube privada virtual (VPC) .	10 de enero de 2020
Soporte para trabajar en una VPC	A partir de ahora puede crear un servidor en una VPC. Puede utilizar su servidor para transferir datos a SFTP hacia y desde un bucket de Amazon S3 sin sobrepasar la red pública de Internet. Para obtener más información, consulte Creación de un servidor en una nube privada virtual (VPC) .	27 de marzo de 2019

Cambio	Descripción	Fecha
Se lanzó la primera versión de. AWS Transfer Family	Esta versión inicial incluye la configuración de direcciones, describe cómo comenzar y proporciona información acerca de la configuración de los clientes y usuarios y la monitorización de la actividad.	25 de noviembre de 2018

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.