Guía del usuario

AWS Transfer Family

AWS Transfer Family: Guía del usuario

Table of Contents

¿Qué es AWS Transfer Family? 1
¿Cómo AWS Transfer Family funciona 4
Publicaciones de blog relevantes para Transfer Family 5
Requisitos previos 8
Regiones, puntos de conexión y cuotas 8
Inscríbase en AWS 8
Configurar almacenamiento 9
Configurar un bucket de Amazon S3 10
Configuración de un sistema de archivos Amazon EFS 14
Creación de una política y un rol de IAM 18
Creación de un rol de usuario 19
Funcionamiento de las políticas de sesión 23
Ejemplo de una política de acceso de lectura y escritura 26
Tutoriales de Transfer Family 30
Introducción a los puntos de conexión del servidor 30
Requisitos previos 31
Inicie sesión en la consola de 32
Cree un servidor compatible con SFTP 32
Añadir un usuario administrado por el servicio 33
Transferencia de un archivo mediante un cliente 35
Cree un flujo de trabajo de descifrado 37
Paso 1: creación y configuración de un rol de ejecución de IAM 37
Paso 2: creación de un flujo de trabajo administrado 39
Paso 3: agregar el flujo de trabajo a un servidor y crear un usuario 40
Paso 4: creación de un par de claves PGP 42
Paso 5: guardar la clave privada PGP en AWS Secrets Manager 42
Paso 6: cifrado de un archivo 44
Paso 7: ejecución del flujo de trabajo y visualización de los resultados 44
Cree y utilice conectores SFTP 45
Paso 1: Crear los recursos de apoyo necesarios 46
Paso 2: Crear y probar un conector SFTP 51
Paso 3: Enviar y recuperar archivos mediante el conector SFTP 55
Procedimientos para crear un servidor Transfer Family para usarlo como servidor SFTP remoto 58

Utilice un proveedor de identidad personalizado 61
Requisitos previos 61
Paso 1: Crear una CloudFormation pila 62
Paso 2: verificación de la configuración del método API Gateway para su servidor 63
Paso 3: visualización de los detalles del servidor de Transfer Family 63
Paso 4: comprobación de que el usuario puede conectarse al servidor 65
Paso 5: prueba de la conexión SFTP y la transferencia de archivos 65
Paso 6: limitación del acceso al bucket 66
Actualice Lambda si utiliza Amazon EFS 68
Configure una configuración de AS2 69
Paso 1: creación de los certificados para AS2 71
Paso 2: creación de un servidor de Transfer Family que utilice el protocolo AS2 75
Paso 3: importación de certificados como recursos de certificados de Transfer Family 78
Paso 4: creación de perfiles para usted y su socio comercial 79
Paso 5: creación de un acuerdo entre usted y su socio 80
Paso 6: creación de un conector entre usted y su socio 81
Paso 7: prueba del intercambio de archivos a través de AS2 mediante Transfer Family 82
Transfer Family para SFTP, FTPS y FTP 85
Opciones de proveedor de identidades 85
AWS Transfer Family matriz de tipos de punto final 87
Configurar un punto final de servidor Transfer Family 91
Cree un servidor compatible con SFTP 93
Cree un servidor compatible con FTPS 102
Cree un servidor compatible con FTP 111
Creación de un servidor en una VPC 119
Uso de nombres de host personalizados 141
Transfiera archivos a través del punto final del servidor 145
Comandos SFTP/FTPS/FTP disponibles 148
Encuentre su punto de conexión de Amazon VPC 149
Evite errores `setstat` 151
Uso de OpenSSH 36
Utilice WinSCP 153
Uso de Cyberduck 35
Uso FileZilla 157
Utilice un cliente Perl 158
Procesamiento de carga posterior 158

Administración de usuarios ... 160
Usuarios gestionados por servicios ... 161
Usuarios de los servicios de directorio ... 172
Proveedores de identidad personalizados ... 189
Usa directorios lógicos ... 219
Reglas para el uso de directorios lógicos ... 220
Implementar directorios lógicos y `chroot` ... 222
Ejemplo de configuración de directorios lógicos ... 225
Configuración de directorios lógicos para Amazon EFS ... 226
Respuesta personalizada AWS Lambda ... 226
Conectores SFTP ... 228
Configure los conectores SFTP ... 228
Creación de un Conector SFTP ... 229
Guarde un secreto para usarlo con un conector SFTP ... 237
Genere y formatee la clave privada del conector SFTP ... 238
Prueba de un conector SFTP ... 242
Transfiera archivos con conectores SFTP ... 244
Listar el contenido del directorio remoto ... 246
Administre los conectores SFTP ... 248
Actualizar conectores SFTP ... 248
Ver los detalles del conector SFTP ... 249
Cuotas para conectores SFTP ... 251
Transfer Family para AS2 ... 253
Casos de uso de AS2 ... 254
Configurar AS2 ... 259
Cree un servidor AS2 mediante la consola Transfer Family ... 260
Cree un servidor AS2 mediante una plantilla ... 263
Configuraciones AS2 ... 266
Características y funciones básicas de AS2 ... 272
Configure los conectores AS2 ... 274
Cree un conector AS2 ... 275
Algoritmos de conector AS2 ... 278
Autenticación básica para conectores AS2 ... 279
Habilite la autenticación básica para los conectores AS2 ... 281
Ver los detalles del conector ... 285
Gestione los socios de AS2 ... 286

Importar certificados AS2 ... 286
Rotación de certificado AS2 ... 288
Creación de perfiles de AS2 ... 290
Creación de acuerdos AS2 ... 291
Transfiere mensajes AS2 ... 292
Enviar mensajes AS2 ... 293
Reciba mensajes AS2 ... 294
Configuración de HTTPS para AS2 ... 295
Transfiera archivos con conectores AS2 ... 302
Nombres y ubicaciones de los archivos ... 303
Códigos de estado ... 305
Ejemplos de archivos de JSON ... 306
Monitor AS2 ... 308
Códigos de estado AS2 ... 310
Códigos de error de AS2 ... 311
Gestión de flujos de trabajo de procesamiento de archivos ... 325
Crear un flujo de trabajo ... 327
Configuración y ejecución de un flujo de trabajo ... 328
Visualización de flujos de trabajo ... 331
Utilice pasos predefinidos ... 334
Copiar archivo ... 334
Descifrar el archivo ... 339
Etiquetado de archivos ... 345
Eliminar archivo ... 346
Variables con nombre para los flujos de trabajo ... 347
Ejemplo de flujo de trabajo de etiquetado y eliminación ... 347
Uso de pasos de procesamiento de archivos personalizados ... 352
Uso de varias funciones de Lambda de forma consecutiva ... 354
Acceso a un archivo después de un procesamiento personalizado ... 354
Ejemplos de eventos enviados AWS Lambda al cargar un archivo ... 355
Ejemplo de función de Lambda para un paso de flujo de trabajo personalizado ... 356
Permisos de IAM para un paso personalizado ... 357
Políticas de IAM para flujos de trabajo ... 358
Relaciones de confianza del flujo de trabajo ... 360
Ejemplo de rol de ejecución: descifrado, copiado y etiquetado ... 360
Ejemplo de rol de ejecución: ejecutar un rol y eliminarlo ... 362

Gestión de excepciones para un flujo de trabajo ... 363
Monitoreo de la ejecución del flujo ... 364
CloudWatch iniciar sesión en un flujo de trabajo ... 364
CloudWatch métricas para flujos de trabajo ... 367
Creación de un flujo de trabajo a partir de una plantilla ... 367
Eliminación de un flujo de trabajo de un servidor de Transfer Family ... 371
Límites y restricciones ... 372
Administración de servidores ... 375
Ver una lista de servidores ... 375
Eliminar un servidor ... 375
Vea los detalles del servidor SFTP ... 377
Vea los detalles del servidor AS2 ... 378
Editar detalles del servidor ... 380
Edite los protocolos de transferencia de archivos ... 383
Editar los parámetros personalizados del proveedor de identidad ... 385
Editar el punto de conexión del servidor ... 388
Edite el registro ... 389
Editar la política de seguridad ... 390
Cambio del flujo de trabajo administrado ... 391
Cambiar los banners de visualización de su servidor ... 392
Puesta de un servidor de online u offline ... 393
Administración de las claves de host del servidor ... 394
Agregue una clave de host de servidor adicional ... 395
Eliminar una clave de host ... 396
Rotar las claves del host del servidor ... 397
Información adicional sobre la clave del host del servidor ... 399
Monitoree el uso dentro de la consola ... 400
Administrar los controles de acceso ... 403
Creación de una política de acceso a un bucket de S3 ... 404
Creación de una política de sesión ... 405
Impedir que los usuarios ejecuten `mkdir` en un bucket de S3 ... 409
Registro ... 410
CloudTrail registro ... 410
Habilitar el CloudTrail registro ... 412
Ejemplo de entrada de registro para crear un servidor ... 412
CloudWatch registro ... 414

Tipos de CloudWatch registro para Transfer Family 414
Crear registros para servidores 417
Administrar el registro de los flujos de trabajo 425
Configurar un rol para CloudWatch 428
Visualización de las transmisiones de registros de Transfer Family 430
Creación de CloudWatch alarmas de Amazon 434
Registro de llamadas a la API de S3 a los registros de acceso de S3 435
Ejemplos para limitar el problema del suplente confuso 435
CloudWatch estructura de registro para Transfer Family 437
Ejemplo de entradas de CloudWatch registro 442
Uso de CloudWatch métricas 447
Notificaciones de usuario 449
CloudWatch consultas 450
Gestión de eventos mediante EventBridge 453
Transfer Family eventos 454
Eventos de servidores SFTP, FTPS y FTP 454
Eventos del conector SFTP 455
Eventos A2S 456
Envío de Transfer Family eventos 456
Creación de patrones de eventos 457
Probar patrones de Transfer Family eventos para eventos 458
Permisos 459
Recursos adicionales de 459
Referencia detallada de los eventos 459
Eventos de servidor 460
Eventos de conector 464
Eventos de AS2 471
Seguridad 478
Políticas de seguridad para servidores 480
Algoritmos criptográficos 481
TransferSecurityPolítica-2024-01 490
TransferSecurityPolítica-2023-05 491
TransferSecurityPolítica-2022-03 492
TransferSecurityPolítica-2020-06 493
TransferSecurityPolítica-2018-11 494
TransferSecurityPolítica-FIPS-2024-01/ Política-FIPS-2024-05 TransferSecurity 495

TransferSecurityPolítica-FIPS-2023-05 ... 497
TransferSecurityPolítica: FIPS-2020-06 ... 498
Políticas de seguridad poscuánticas ... 499
Políticas de seguridad para conectores SFTP ... 504
Políticas de seguridad poscuánticas ... 506
Acerca del intercambio de claves híbrido poscuántico en SSH ... 507
Modo de uso ... 508
Cómo probarlo ... 509
Protección de datos ... 513
Cifrado de datos ... 514
Gestión de claves en Transfer Family ... 515
Administración de identidades y accesos ... 532
Público ... 532
Autenticación con identidades ... 533
Administración de acceso mediante políticas ... 537
¿Cómo AWS Transfer Family funciona con IAM ... 539
Ejemplos de políticas basadas en identidades ... 544
Ejemplo de política basada en etiquetas ... 547
Solución de problemas de identidades y accesos ... 551
Validación de conformidad ... 553
Resiliencia ... 554
Seguridad de la infraestructura ... 555
Cortafuegos de aplicaciones web ... 555
Prevención de la sustitución confusa entre servicios ... 557
Roles de usuario de Transfer Family ... 559
Roles del flujo de trabajo ... 560
Roles de registro e invocación de Transfer Family ... 562
AWS políticas gestionadas ... 563
AWSTransferConsoleFullAccess ... 564
AWSTransferFullAccess ... 566
AWSTransferLoggingAccess ... 567
AWSTransferReadOnlyAccess ... 568
Actualizaciones de políticas ... 569
Solución de problemas de Transfer Family ... 571
Solución de los problemas de los usuarios administrados por el servicio ... 571
Solución de los problemas de los usuarios administrados por el servicio de Amazon EFS ... 572

Solución de problemas con cuerpo de la clave pública demasiado largo 572
Solución de problemas no pudo agregar la clave pública SSH 573
Solución de problemas de Amazon API Gateway 573
Demasiados errores de autenticación 573
Conexión cerrada 575
Solución de problemas de políticas para buckets de Amazon S3 cifrados 575
Solución de problemas de autenticación 576
Fallos de autenticación: SSH/SFTP 576
Se gestionó un problema de dominios no coincidentes en AD 577
Varios problemas de autenticación 577
Solución de problemas de flujos de trabajo administrados 578
Solucionar errores relacionados con el flujo de trabajo con Amazon CloudWatch 578
Solución de los errores de copia del flujo de trabajo 580
Solución de los problemas de descifrado del flujo de trabajo 580
Solucionar el error del archivo de cifrado firmado 581
Solucione el error de un algoritmo FIPS 581
Solución de problemas de Amazon EFS 583
Solución de los problemas del perfil POSIX faltante 584
Solución de los problemas de directorios lógicos con Amazon EFS 585
Solución de los problemas al probar su proveedor de identidad 585
Solución de los problemas al agregar claves de host confiables para su conector SFTP 586
Solución de los problemas de carga de archivos 586
Solución de los problemas de errores de carga de archivos de Amazon S3 587
Solución de los problemas de nombres de archivo ilegibles 587
Solución de los problemas con la excepción `ResourceNotFound` 588
Solución de los problemas con el conector SFTP 588
La negociación de claves falla 589
Problemas varios con el conector SFTP 589
Solución de los problemas de AS2 590
Referencia de la API 591
Bienvenido 591
Acciones 594
CreateAccess 597
CreateAgreement 604
CreateConnector 610
CreateProfile 618

CreateServer ... 623
CreateUser ... 636
CreateWorkflow ... 645
DeleteAccess ... 654
DeleteAgreement ... 657
DeleteCertificate ... 660
DeleteConnector ... 662
DeleteHostKey ... 664
DeleteProfile ... 667
DeleteServer ... 669
DeleteSshPublicKey ... 672
DeleteUser ... 675
DeleteWorkflow ... 678
DescribeAccess ... 680
DescribeAgreement ... 684
DescribeCertificate ... 687
DescribeConnector ... 690
DescribeExecution ... 693
DescribeHostKey ... 698
DescribeProfile ... 701
DescribeSecurityPolicy ... 704
DescribeServer ... 708
DescribeUser ... 713
DescribeWorkflow ... 718
ImportCertificate ... 723
ImportHostKey ... 728
ImportSshPublicKey ... 732
ListAccesses ... 737
ListAgreements ... 741
ListCertificates ... 745
ListConnectors ... 749
ListExecutions ... 752
ListHostKeys ... 757
ListProfiles ... 761
ListSecurityPolicies ... 765
ListServers ... 769

ListTagsForResource ... 773
ListUsers ... 778
ListWorkflows ... 783
SendWorkflowStepState ... 786
StartDirectoryListing ... 790
StartFileTransfer ... 796
StartServer ... 802
StopServer ... 805
TagResource ... 808
TestConnection ... 812
TestIdentityProvider ... 816
UntagResource ... 823
UpdateAccess ... 826
UpdateAgreement ... 833
UpdateCertificate ... 839
UpdateConnector ... 843
UpdateHostKey ... 849
UpdateProfile ... 853
UpdateServer ... 856
UpdateUser ... 869
Data Types ... 876
As2ConnectorConfig ... 879
CopyStepDetails ... 883
CustomStepDetails ... 886
DecryptStepDetails ... 888
DeleteStepDetails ... 891
DescribedAccess ... 893
DescribedAgreement ... 897
DescribedCertificate ... 901
DescribedConnector ... 905
DescribedExecution ... 909
DescribedHostKey ... 912
DescribedProfile ... 915
DescribedSecurityPolicy ... 918
DescribedServer ... 921
DescribedUser ... 930

DescribedWorkflow 935
EfsFileLocation 937
EndpointDetails 939
ExecutionError 943
ExecutionResults 945
ExecutionStepResult 946
FileLocation 948
HomeDirectoryMapEntry 949
IdentityProviderDetails 951
InputFileLocation 954
ListedAccess 955
ListedAgreement 958
ListedCertificate 961
ListedConnector 964
ListedExecution 966
ListedHostKey 968
ListedProfile 970
ListedServer 972
ListedUser 976
ListedWorkflow 979
LoggingConfiguration 981
PosixProfile 983
ProtocolDetails 985
S3FileLocation 989
S3InputFileLocation 991
S3StorageOptions 993
S3Tag 994
ServiceMetadata 995
SftpConnectorConfig 996
SshPublicKey 998
Tag 1000
TagStepDetails 1001
UserDetails 1003
WorkflowDetail 1005
WorkflowDetails 1007
WorkflowStep 1009

Realizar solicitudes a la API 1011
Cabeceras de solicitud obligatorias para Transfer Family 1011
Entrada y firma de la solicitud de Transfer Family 1013
Respuestas de error 1014
Bibliotecas disponibles 1016
Parámetros comunes 1016
Errores comunes 1019
Historial de documentos 1021
Glosario de AWS 1037
..... mxxxviii

¿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 soporte totalmente gestionado para la transferencia de archivos a través de SFTP, AS2, FTPS y FTP directamente desde y hacia Amazon S3 o Amazon EFS. 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 -02.txt. draft-ietf-secsh-filexfer
- Protocolo seguro de File Transfer (FTPS)
- Protocolo de File Transfer (FTP)
- Declaración de aplicabilidad 2 (AS2)

> **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.
- Distribución de datos basada en suscripciones de 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
- Transacciones B usiness-to-business (B2B)
- Integraciones con los sistemas de planificación de recursos empresariales (ERP) y de gestión de relaciones con los clientes (CRM)

Con Transfer Family, obtiene acceso a un servidor compatible con el protocolo de transferencia de archivos AWS sin necesidad de ejecutar ninguna infraestructura de servidor. Puede utilizar 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 primer lugar, debe asociar su nombre de host al punto de conexión del servidor y, a continuación, añadir los usuarios y otorgarles el nivel de acceso necesario. Una vez hecho esto, las solicitudes de

transferencia de los usuarios se atenderán directamente desde el punto de conexión del servidor de Transfer Family.

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 finales de los AWS Transfer Family servidores

¿Cómo funciona AWS Transfer Family

AWS Transfer Family es un AWS servicio totalmente gestionado que puede utilizar para transferir archivos al almacenamiento de Amazon Simple Storage Service (Amazon S3) o a los sistemas de archivos Amazon Elastic File System (Amazon EFS) mediante los siguientes protocolos:

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

  El documento oficial del IETF está aquí: SSH File Transfer Protocol -02.txt. draft-ietf-secsh-filexfer
- Protocolo seguro de File Transfer (FTPS)
- Protocolo de File Transfer (FTP)
- Declaración de aplicabilidad 2 (AS2)

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 enrutamiento basado en la latencia, consulte la entrada del blog Minimice la latencia de la red con la transferencia para servidores SFTP. AWS

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, filtrar, comprimir/descomprimir y cifrar/descifrar 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: un cliente gráfico exclusivo para Windows.
- 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 AWS Transfer Family puntos de conexión SFTP/FTPS 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 del servidor. 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
Diseñamos transferencias de archivos gestionadas seguras y compatibles con conectores AWS Transfer Family SFTP y cifrado PGP	16 de mayo de 2024
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

Título y enlace de la entrada del blog	Date
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
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

Título y enlace de la entrada del blog	Date
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.

Temas

- AWS Regiones, puntos de enlace y cuotas compatibles
- Inscríbase en AWS
- Configure el almacenamiento para usarlo con AWS Transfer Family
- Creación de una política y un rol de IAM

AWS Regiones, puntos de enlace y cuotas compatibles

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` Service Quotas, también denominadas límites, establecen el número máximo de recursos u operaciones de servicio para su cuenta de Cuenta de AWS. En esta guía, puedes encontrar las cuotas en Cuotas de AS2 yCuotas 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

Inscríbase 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 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 AWSse 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 AWS Pricing Calculator 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

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 acceso multirregionales de 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 diagonal (/), tratando el último elemento como el nombre del archivo y agrupando los nombres de los archivos que tienen el mismo prefijo en la misma ruta. Los objetos de cero bits 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 HeadObjectla 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, *`DOC-EXAMPLE-BUCKET`* sustitúyala por el nombre de tu bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListing",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
```

```
        },
        {
            "Sid": "AllowReadWrite",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
         },
      {
            "Sid": "DenyIfNotFolder",
            "Effect": "Deny",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "NotResource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/"
            ]
         }
      ]
}
```

> **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 habilitar 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, tiene 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 sistema de archivos de Amazon EFS tienen un modo de estilo Unix asociado a ellos. Este valor de modo define los permisos para realizar acciones en ese objeto.

Además, en los sistemas de estilo Unix, los usuarios y los grupos se asignan a identificadores numéricos, que Amazon EFS utiliza para representar la propiedad del archivo. 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 al UID/GID y a los directorios que especifique. Si el UID/GID/ los directorios aún 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 del usuario raíz mediante SFTP/FTPS para 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 gestionados por el servicio Amazon EFS y, tanto para el ID de usuario como para el ID de grupo, introduzca 0 (cero).

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 administrado por el servicio, puede seleccionar la política de generación automática basada en 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 una política de acceso de lectura y escritura

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, debes crear una política y un rol basados en la identidad AWS Identity and Access Management (IAM) que proporcionan 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, consulte Ejemplo de una política de acceso de lectura y escritura.
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 Policies (Políticas) y, a continuación, seleccione Create policy (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 acceso de lectura/escritura o restringir a los usuarios a su directorio de inicio. Para obtener más información, consulte Ejemplo de una política de acceso de lectura y escritura.
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 asóciele 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 (Siguiente: 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 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).

Luego, estableces 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 siguientes, reemplace cada *marcador de posición del usuario* con su propia información.

Para obtener más información sobre el confuso problema del diputado y otros ejemplos, consulte Prevención de la sustitución confusa entre servicios.

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 finales de los AWS Transfer Family servidores se asignan este rol y esta política al usuario o usuarios.

Véase también

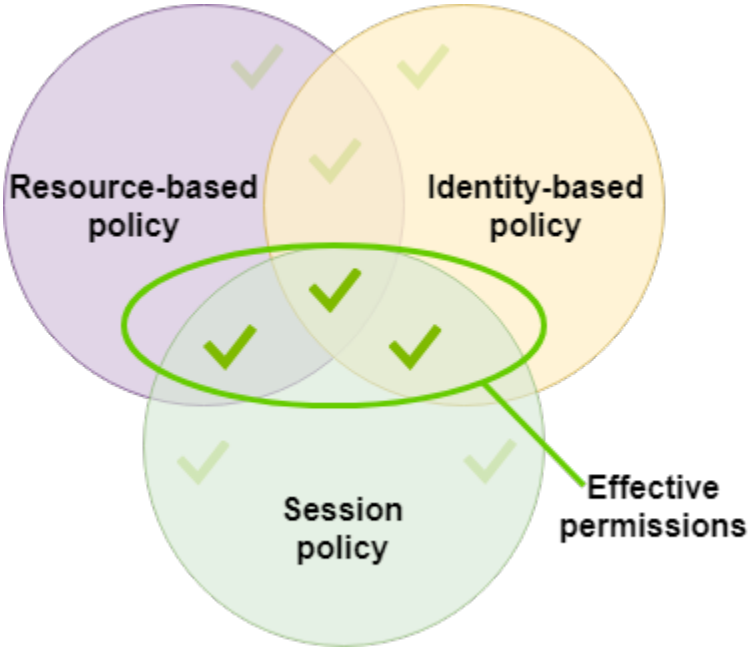
- Para obtener más información general sobre las funciones de IAM, consulte Crear una función para delegar permisos a un AWS servicio en la Guía del usuario de IAM.
- Para obtener más información acerca de las políticas basadas en identidades para los recursos de Amazon S3, consulte Identity and Access 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 acceso de lectura y escritura, 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 detalles, consulte Cifrado de datos en Amazon S3.

```
{
    "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 una política de acceso de lectura y escritura

Conceder acceso de lectura/escritura al bucket de Amazon S3

El siguiente ejemplo de política AWS Transfer Family otorga acceso de lectura y escritura a los objetos de su bucket de Amazon S3.

Tenga en cuenta lo siguiente:

- Sustituya *`DOC-EXAMPLE-BUCKET`* por el nombre del 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:::DOC-EXAMPLE-BUCKET"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObjectVersion",
                "s3:GetObjectACL",
                "s3:PutObjectACL"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-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, sustituya *region* por su región, *account-id* por la cuenta en la que se encuentra el archivo y *file-system-id*por el ID de su 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:region:account-id: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:region:account-id:file-system/file-
system-id"
        }
    ]
}
```

Tutoriales de Transfer Family

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

- Cómo empezar con los puntos finales de los AWS Transfer Family servidores: este tutorial explica cómo crear un servidor SFTP Transfer Family y un usuario gestionado por el servicio y, a continuación, muestra cómo transferir un archivo mediante un cliente.
- Configuración y uso de conectores SFTP: este tutorial muestra cómo configurar un conector SFTP y, a continuación, 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 : 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.
- Configuración de un flujo de trabajo gestionado para descifrar un archivo: en este tutorial se muestra cómo configurar un flujo de trabajo gestionado que contenga un paso de descifrado y cómo cargar un archivo cifrado en un bucket de Amazon S3 y, a continuación, ver el archivo descifrado.
- Configuración de una configuración AS2: este tutorial explica los pasos necesarios para configurar un servidor AS2 Transfer Family. Hay instrucciones para importar certificados, crear perfiles y acuerdos y, opcionalmente, crear un conector AS2 y, a continuación, probar la configuración.

Temas

- Cómo empezar con los puntos finales 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

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

Usa este tutorial para empezar con AWS Transfer Family (Transfer Family). Aprenderá a crear un servidor compatible con SFTP con punto de conexión de acceso público mediante el

almacenamiento de Amazon S3, a añadir un usuario con autenticación administrada por el servicio y a transferir un archivo con Cyberduck.

Temas

- Requisitos previos
- Paso 1: Iniciar sesión en la consola de AWS Transfer Family
- Paso 2: creación de un servidor compatible con SFTP
- 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, para los usuarios que transfieren archivos dentro y fuera de AWS Transfer Family, AmazonS3 FullAccess concede 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:

- AWSTransferConsoleFullAccessconcede permisos a su usuario de SFTP para crear recursos de Transfer Family.
- La IAM FullAccess (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: CreateVpc Endpoint y ec2: DeleteVpc Endpoints a su política.

> **Note**
>
> Las FullAccess políticas de Amazon S3 FullAccess e IAM no son, en sí mismas, 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. AWS Puede ver los permisos individuales de estas políticas y determinar el conjunto mínimo que necesita para sus fines.

Paso 1: Iniciar sesión en la consola de AWS Transfer Family

Inicio de sesión en Transfer Family

1. Inicie sesión en la AWS Transfer Family consola AWS Management Console y ábrala 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: creación de un servidor compatible con SFTP

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.

Creación de un servidor compatible con SFTP

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 servidores AWS Transfer Family

   > **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, consulteAdministración de usuarios para puntos finales de servidor.

Paso 3: agregar un usuario de servicio administradas

Cómo agregar un usuario al servidor con SFTP

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, A-Z, 0—9, subrayado '_', guión

'-', punto ' . ', y en el signo (@). El nombre de usuario no puede comenzar por un guion, un punto ni una arroba.

4. En Access, elige el rol de IAM en Creación de una política y un rol de IAM el que lo creaste. 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 deseas 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, consulteFuncionamiento 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 que esté fuera de 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, consulteGenere 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 servidor habilitado para SFTP.

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` se muestra 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 /mybucket/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 /my-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: guardar 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. `DOC-EXAMPLE-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:::DOC-EXAMPLE-BUCKET/*",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET"]
            "Condition": {
                "StringEquals": {
                    "s3:RequestObjectTag/Archive": "yes"
                }
            }
        },
        {
```

```
            "Sid": "DecryptSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:region:account-id: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 `DOC-EXAMPLE-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. Abre 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, `DOC-EXAMPLE-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 detalles, 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). Sin embargo, si elige ECC, asegúrese de seleccionar una NIST o BrainPool para la curva elíptica. No seleccione Curve 25519.

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: guardar 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 Precios de AWS Secrets Manager.

Almacenamiento de una clave privada PGP en Secrets Manager

1. Inicia sesión en la AWS Secrets Manager consola AWS Management Console y ábrela 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 Pares clave-valor, seleccione la pestaña Clave/valor.
   - Clave: introduzca **`PGPPrivateKey`**.
   - valor: pegue el texto de su clave privada en el campo valor.
6. Seleccione Añadir fila y, en la sección de Pares clave/valor, seleccione la pestaña Clave/valor.
   - 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`**.

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: /DOC-EXAMPLE-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
```

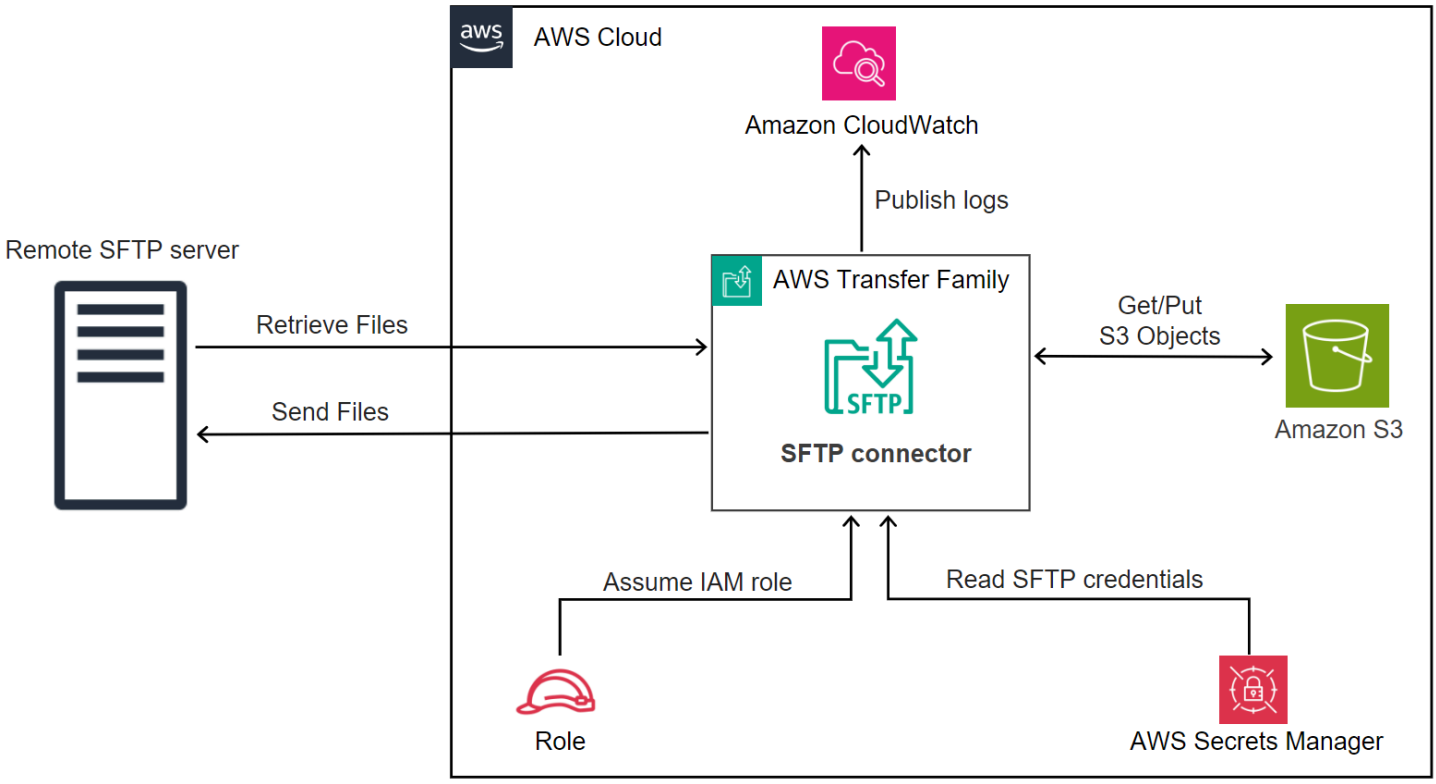
   Si tiene éxito, el comando `ls` muestra el archivo `testfile.txt`. Puede descargar este archivo y comprobar que es el mismo que el archivo original que cifró anteriormente.

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 y, a continuación, transferir archivos entre el almacenamiento de Amazon S3 y un servidor SFTP.

Un conector SFTP recupera las credenciales de SFTP para AWS Secrets Manager autenticarse en un servidor SFTP remoto y establecer una conexión. El conector envía o recupera archivos del servidor remoto y los almacena en Amazon S3. 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.



Las siguientes entradas del blog proporcionan 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

Temas

- Paso 1: Crear los recursos de apoyo necesarios
- Paso 2: Crear y probar un conector SFTP
- Paso 3: Enviar y recuperar archivos mediante el conector SFTP
- Procedimientos para crear un servidor Transfer Family para usarlo como servidor SFTP remoto

Paso 1: Crear 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 para 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

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 es**`sftp-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.

El siguiente ejemplo concede los permisos necesarios para acceder al *`DOC-EXAMPLE-BUCKET en Amazon`* S3 y al secreto especificado almacenado en Secrets Manager.

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

```
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

Sustituya los elementos de la siguiente manera:

- Para *DOC-EXAMPLE-BUCKET, el tutorial* usa. **s3-storage-east**
- Para la *región*, el tutorial usa. **us-east-1**
- Para el *ID de cuenta*, usa tu Cuenta de AWS ID.
- Para *SecretName-6 RandomCharacters*, nos **using sftp-connector1** quedamos con el 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, consulteFunción 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 Precios de AWS Secrets Manager.

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 el 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 la AWS Secrets Manager consola AWS Management Console y ábrala 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 Pares clave-valor, seleccione la pestaña Clave/valor.
   - Clave: introduzca **`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).

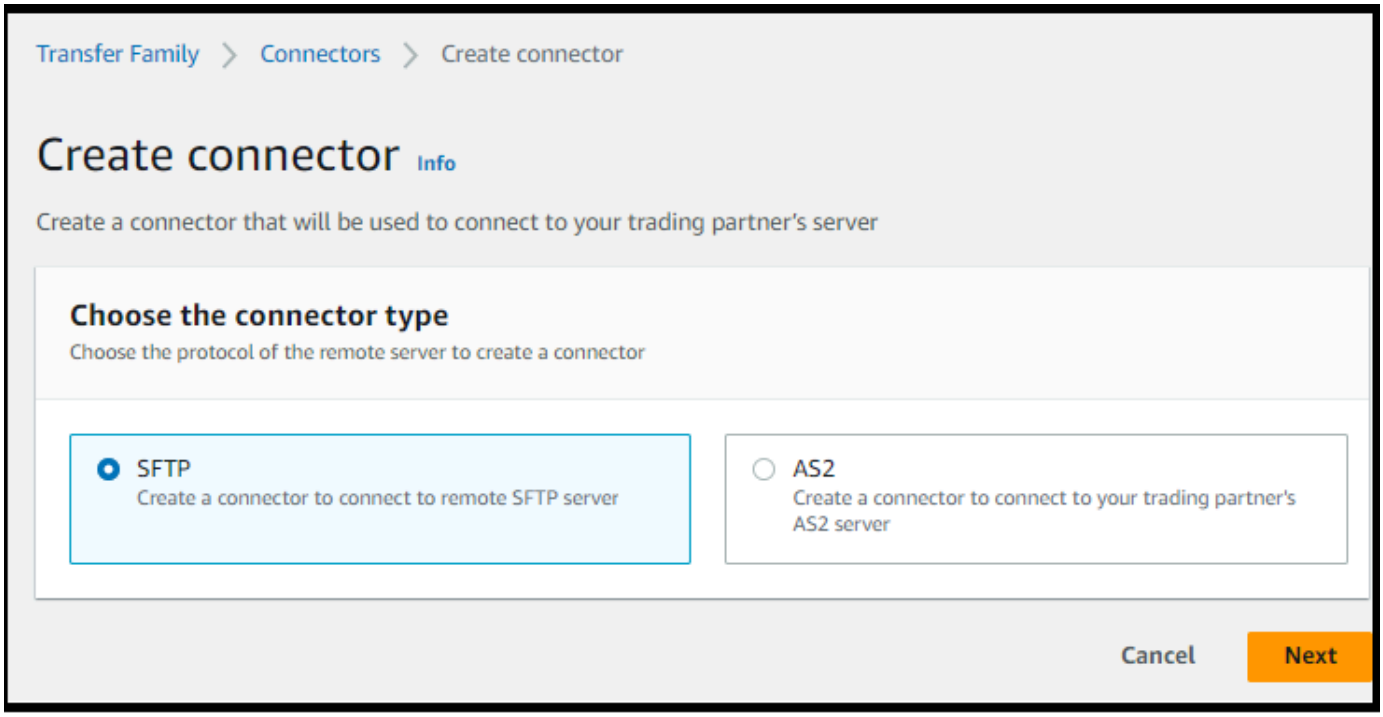
7. Elija Siguiente.
8. En la página Configurar el secreto, introduzca un nombre para el secreto. En este tutorial, asignamos un nombre al secreto**`aws/transfer/sftp-connector1`**.
9. Seleccione Siguiente y, a continuación, acepte los valores predeterminados de la página Configurar rotación. A continuación,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

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 Configure los conectores SFTP.

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 y, a continuación, seleccione Crear conector.
3. Elija SFTP como tipo de conector para crear un conector SFTP y, a continuación, elija Siguiente.



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

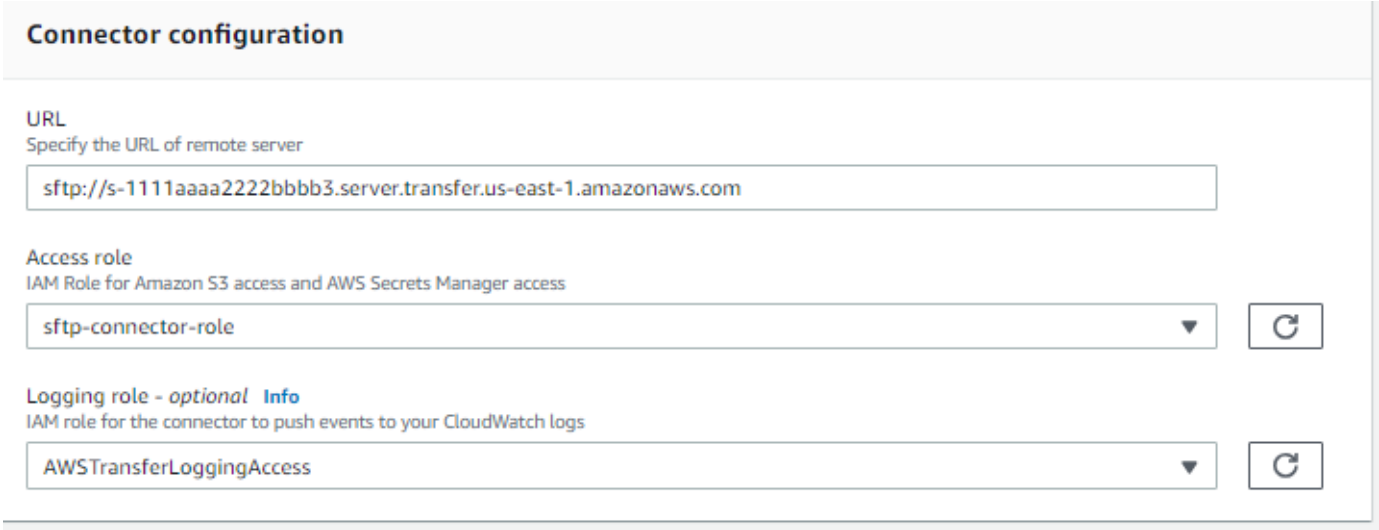
- Para la URL, introduzca la URL del servidor SFTP remoto. Para el tutorial, introducimos la URL del servidor Transfer Family que estamos utilizando como servidor SFTP remoto.

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

  Sustituye *1111aaaa2222bbbb3 por tu ID de servidor* de Transfer Family.

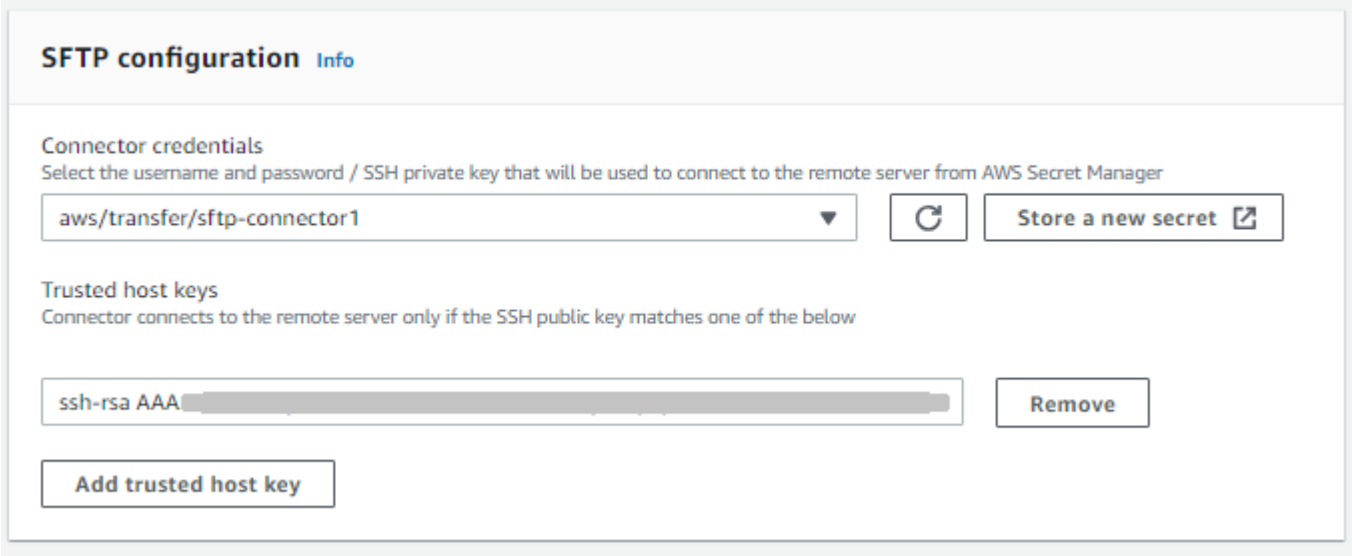
- Para el rol de acceso, ingresa el rol que creamos anteriormente. **sftp-connector-role**
- Para la función de registro, elija**AWSTransferLoggingAccess**.

> **Note**
>
> AWSTransferLoggingAccess es una política AWS gestionada. Esta política se describe en detalle enAWS política gestionada: AWSTransferLoggingAccess.



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 de confianza, 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 SftpConnectorConfigsobre los tipos de datos.



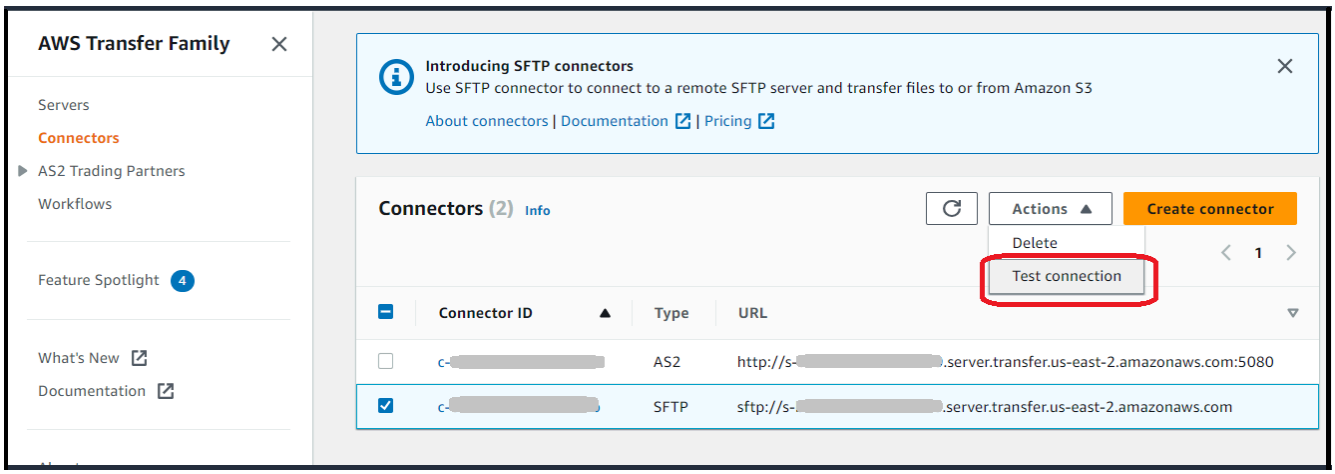
6. Una vez que haya confirmado todos los ajustes, elija Crear conector para crear el conector SFTP.

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

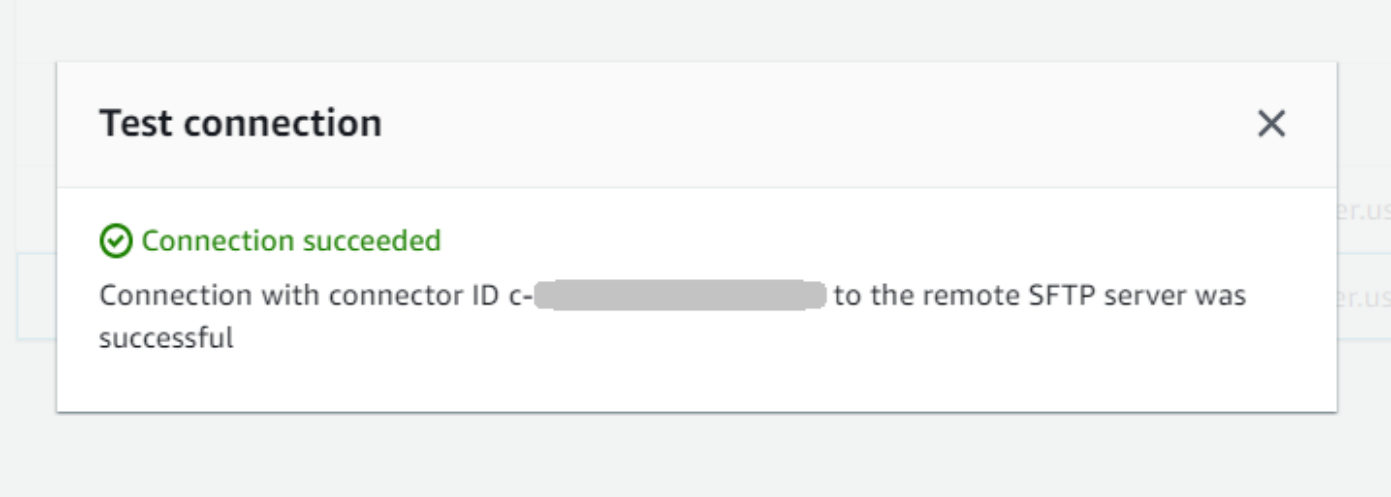
Test a connector using the console

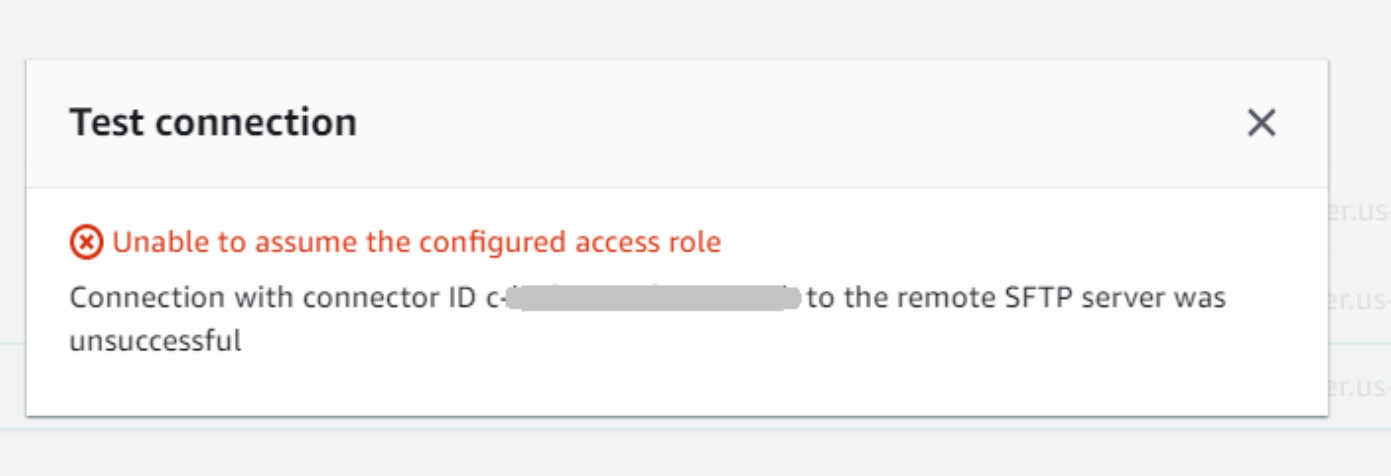
Prueba de un conector SFTP

1. Abra la AWS Transfer Family consola en https://console.aws.amazon.com/transfer/.
2. En el panel de navegación izquierdo, seleccione Conectores 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 (sustituya el identificador del *conector por el identificador* del 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"
}
```

Paso 3: Enviar y recuperar 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.

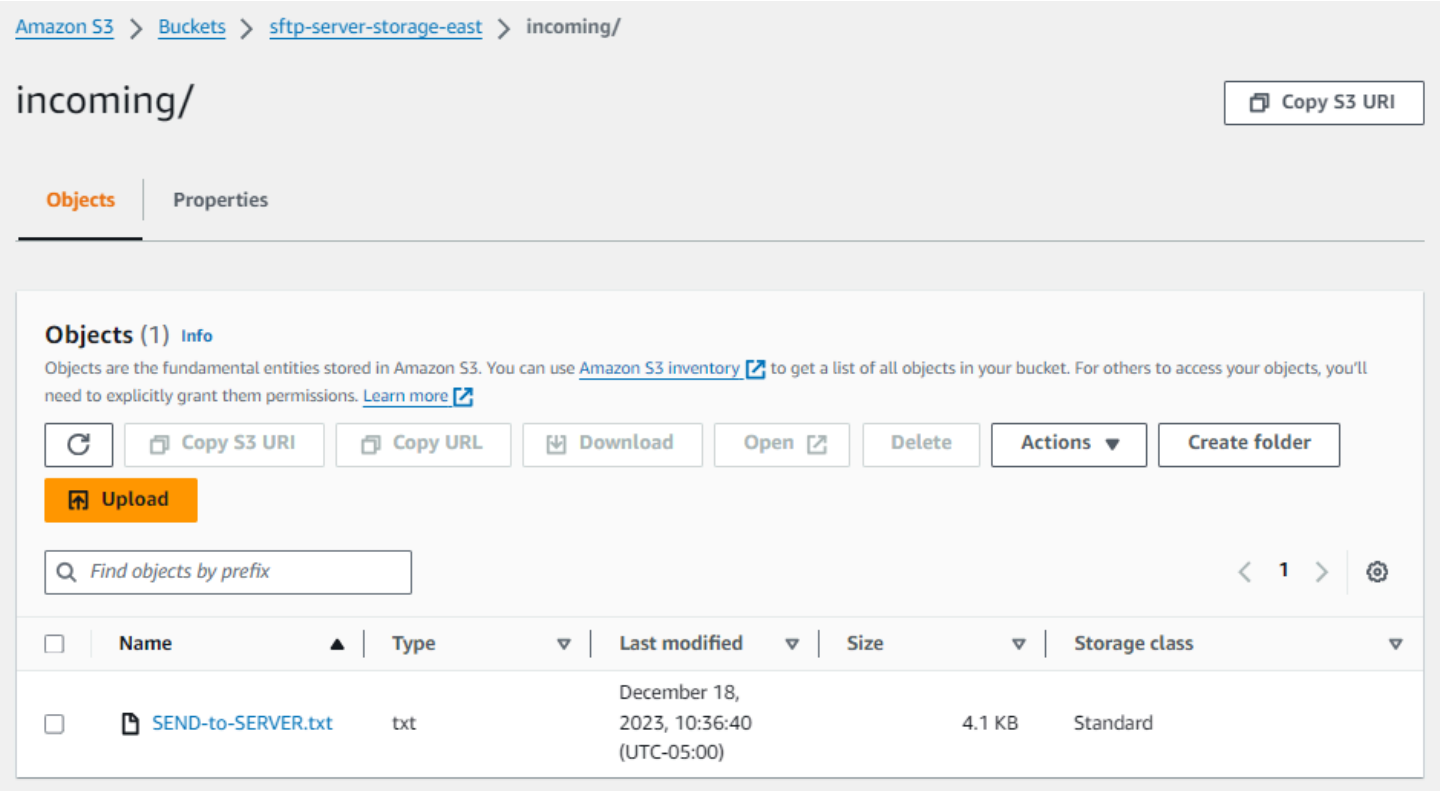
- Enviamos un archivo con el nombre `SEND-to-SERVER.txt` del almacenamiento de Amazon S3 al servidor SFTP.
- Recuperamos un archivo con el nombre `RETRIEVE-to-S3.txt` del servidor SFTP al almacenamiento de Amazon S3.

> **Note**
>
> En los siguientes comandos, sustituya el *`connector-id por el ID del`* 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 "/s3-
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.



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",
```

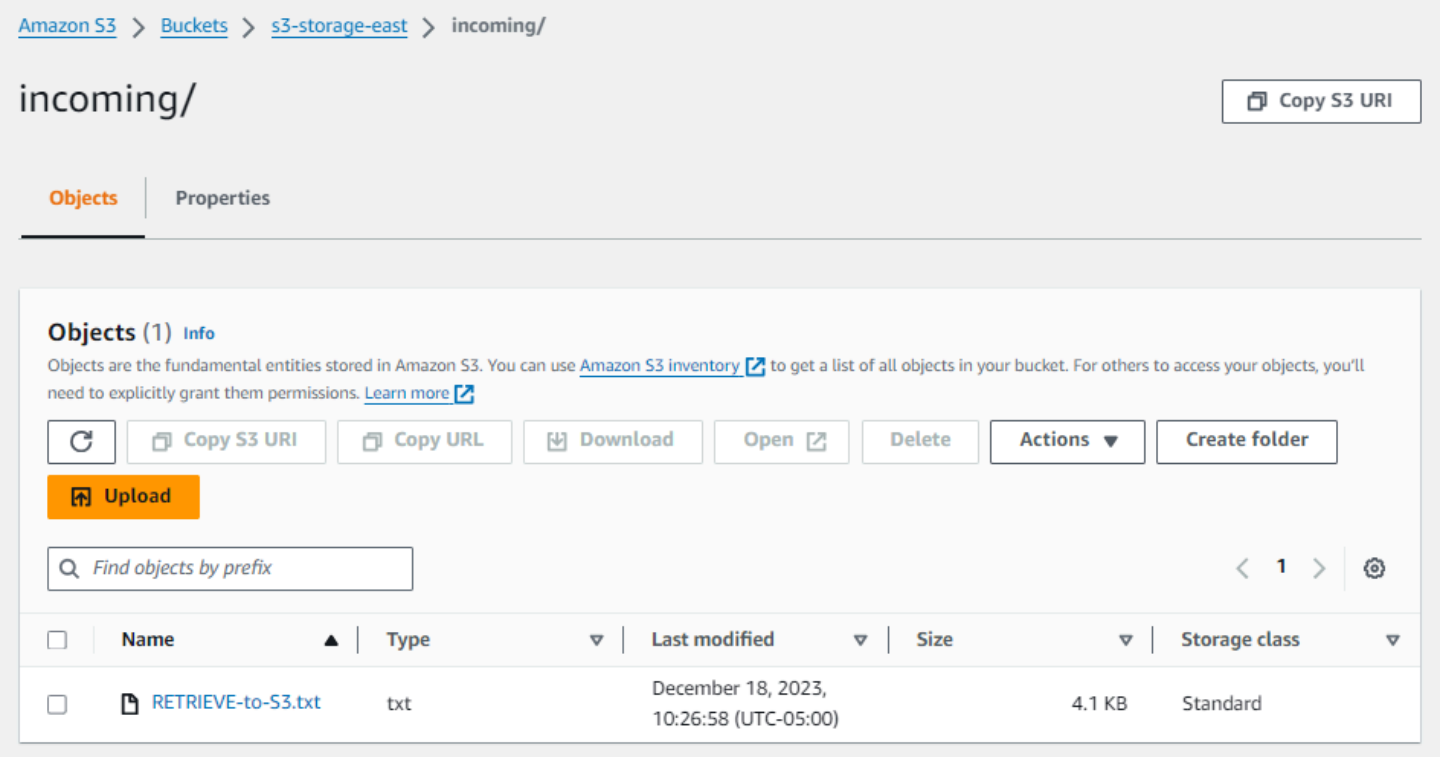
```
    "file-path": "/s3-storage-east/SEND-to-SERVER.txt",
    "status-code": "COMPLETED",
    "start-time": "2023-12-18T15:26:56.915864Z",
    "end-time": "2023-12-18T15:26:57.298122Z",
    "account-id": "500655546075",
    "connector-arn": "arn:aws:transfer:us-east-1:500655546075:connector/connector-id",
    "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 "/s3-storage-east/
incoming"
```

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



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": "500655546075",
    "connector-arn": "arn:aws:transfer:us-east-1:500655546075:connector/c-connector-
id",
    "local-directory-path": "/s3-storage-east/incoming"
}
```

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. **`s3-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 Cree un servidor compatible con SFTP 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:::s3-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:::s3-storage-east/*"
            ]
        },
        {
            "Sid": "GetConnectorSecretValue",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:us-east-1:500655546075: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 AWS 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, consulteConfiguración 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 AWS CloudFormation en la siguiente sección.

Paso 1: Crear una CloudFormation pila

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

1. Abre la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
2. Seleccione Crear pila y seleccione Con recursos nuevos (estándar).
3. En Requisito previo: preparar plantilla, elija La plantilla está lista.
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 UserNamey UserPassword.
   - Para UserHomeDirectoryello, 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 UserRoleArnde 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 campo UserPublicKey1. 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 AWS 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 detalles, consulte Agregue un cortafuegos de aplicaciones web.

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 AWS 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.

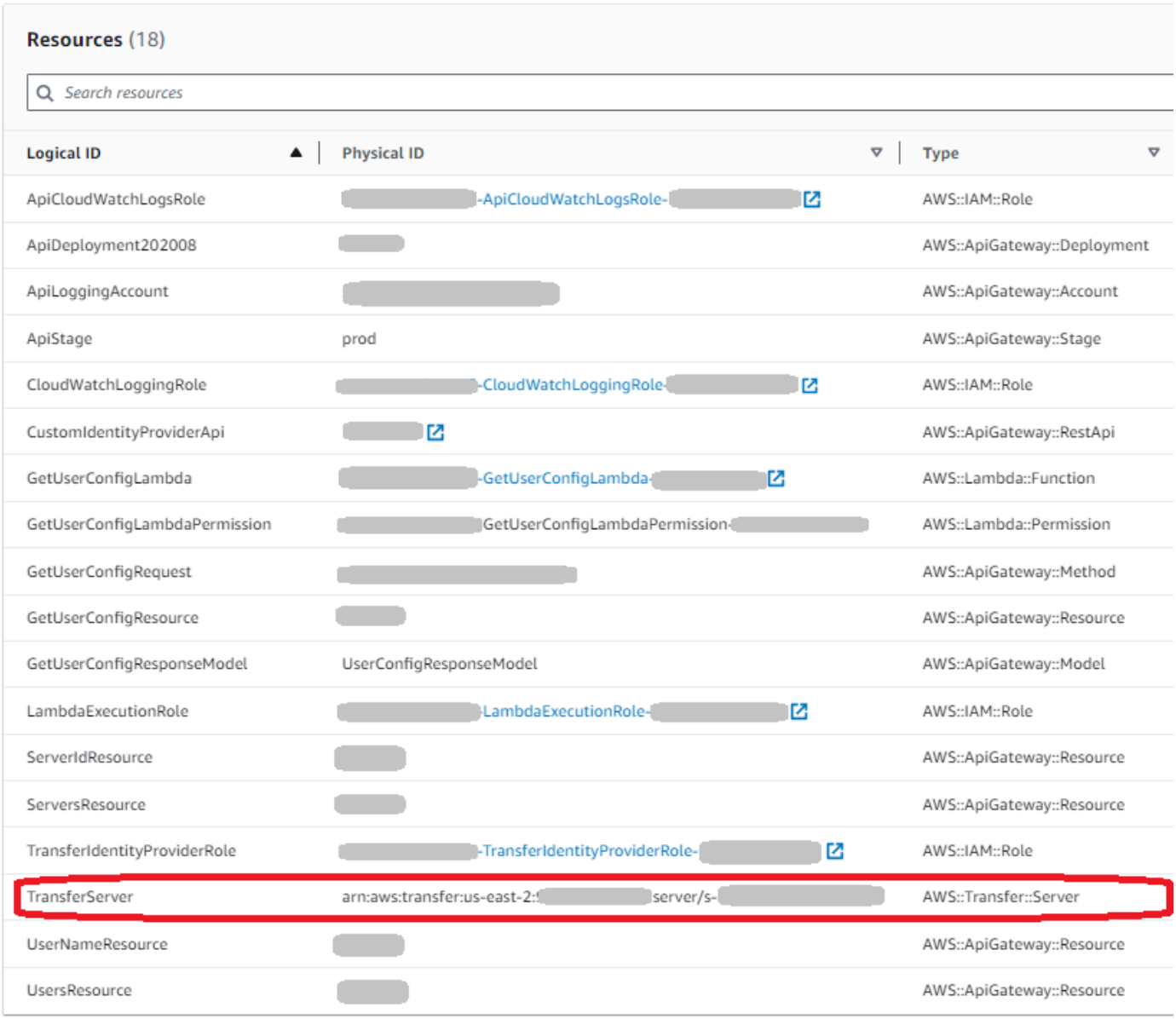
Paso 3: visualización de los detalles del servidor de Transfer Family

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

Visualización de los detalles del servidor de Transfer Family

1. Abra la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.

2. Elija la pila que ha creado.
3. Elija la pestaña Recursos.



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

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

   El ID del servidor coincide con el ID que se muestra para el TransferServerrecurso en AWS 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 AWS 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 `StatusCode: 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 AWS CloudFormation pila:

- CreateServer: `true`
- UserHomeDirectory: `/myuser-bucket`
- 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`

El UserPublicKey1 es una clave pública que ha generado como parte de un par de claves pública/privada.

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:::myuser-bucket"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObjectAcl",
                "s3:GetObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:PutObjectAcl",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::myuser-bucket/*"
        }
    ]
}
```

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: /myuser-bucket
```

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

```
sftp> pwd
Remote working directory: /myuser-bucket
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 pila y lambda-identifier** es el identificador de la CloudFormation 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 aquí descritos, dispondrá de un servidor compatible con AS2 preparado para aceptar mensajes de 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 del ejemplo de configuración 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. 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 2: creación de un servidor de 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.

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

   Este proceso se describe en Paso 3: importación de certificados como recursos de certificados de Transfer Family.

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

   Este proceso se describe en Paso 4: creación de perfiles para usted y su socio comercial.

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

Paso 1: creación de los certificados para AS2

En un intercambio AS2, ambas partes 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=ROOTCA" \
-key root-ca-key.pem \
-out root-ca.pem
```

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

	Nombre	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, región no se refiere a su Región de AWS.)
L	Nombre de la localidad	Nombre de la ciudad donde se ubica su empresa.
0	Nombre de la organización	El nombre legal completo de su empresa, incluidos los sufijos, como LLC, Corp, etc.
0U	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 servidores compatibles con AS2, como OpenAS2, requieren que se utilice el mismo certificado para la firma y 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: creación de un servidor de Transfer Family que utilice el protocolo AS2

Este procedimiento explica cómo crear un servidor compatible con AS2 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 servidor SFTP o FTPS, se crea un AWS Transfer Family servidor compatible con AS2 mediante el parámetro del comando. `--protocols AS2` `create-server` AWS CLI 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 un servidor compatible con AS2 para Transfer Family mediante el comando `create-server`, se crea automáticamente un punto de conexión 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.

Creación de un servidor compatible con AS2

1. Ejecute el siguiente comando de la . 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 su servidor compatible con AS2 es accesible, 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 ejecute 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` gestionada. Para 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 3: importación de 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`).

```
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 4: creación de perfiles para usted y su socio comercial

En este procedimiento se explica cómo crear perfiles AS2 mediante. AWS CLI 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, sustituya *MYCORP* por el nombre de su empresa y *PARTNER-COMPANY* por el nombre de la empresa de su socio comercial.

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 “Creación de acuerdos 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 acceso de lectura/escritura hacia y desde el bucket. 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)
- 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

Ejecute el siguiente comando para crear el panel.

```
aws transfer create-agreement --description "ExampleAgreementName" --server-id your-
server-id \
--local-profile-id your-profile-id --partner-profile-id your-partner-profile-id --base-
directory /DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox \
--access-role arn:aws:iam::111111111111:role/TransferAS2AccessRole
```

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 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",
"SigningAlgorithm": "SHA256"
}
```

> **Note**
>
> Por `EncryptionAlgorithm` ejemplo, no especifique el `DES_EDE3_CBC` algoritmo a menos que deba admitir 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 formato`s-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 `/DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox/processed/myfile1.`*`messageId`*`.txt` y `/DOC-EXAMPLE-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 "/DOC-EXAMPLE-SOURCE-BUCKET/myfile1.txt" "/DOC-EXAMPLE-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.

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
- 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

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.

Acción	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
Autenticación basada en clave	Sí	No	Sí	Sí
Autenticación de contraseña	No	Sí	Sí	Sí
AWS Identity and Access	Sí	Sí	Sí	Sí

Acción	AWS Transfer Family servicio gestionado	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
Management (IAM) y POSIX				
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
- Existe una entrada de blog que describe el uso de una función de Lambda integrada con Microsoft Azure AD como proveedor de identidad de Transfer Family. Para obtener más información, consulte Autenticarse AWS Transfer Family con Azure Active Directory y AWS Lambda.
- Proporcionamos varias AWS CloudFormation plantillas para ayudarlo a implementar rápidamente un servidor Transfer Family que utilice un proveedor de identidad personalizado. Para obtener más detalles, consulte Plantillas de función de Lambda.

En los siguientes procedimientos, puede crear un servidor compatible con SFTP, un servidor compatible con FTPS, un servidor compatible con FTP o un servidor compatible con AS2.

Paso siguiente

- Cree un servidor compatible con SFTP
- Cree un servidor compatible con FTPS
- Cree un servidor compatible con FTP
- 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 entornos de VPC o conectados a VPC, como un centro de datos local a través de una VPN. AWS Direct Connect	Desde entornos de VPC o conectados a VPC, como un centro de datos local a través de una VPN. AWS Direct Connect	Desde entornos de VPC o conectados a VPC, como un centro de datos local a través de una VPN. AWS Direct Connect
Direcciones IP estáticas	No puedes adjuntar una dirección IP estática. AWS proporciona	Puede adjuntar direcciones IP elásticas al punto de conexión.	Las direccion es IP privadas adjuntas al punto de conexión no cambian.	Las direccion es IP privadas adjuntas al punto de conexión no cambian.

Característica	Público	VPC: internet	VPC: interna	VPC_Endpoint (obsoleta)
	direcciones IP que están sujetas a cambios.	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.		

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 los puntos finales alojados en VPC, los servidores SFTP Transfer Family pueden funcionar a través del puerto 22 (el predeterm	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)
	inado), el puerto 2222 o el puerto 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 direccion es IP permitidas por el firewall de su cliente.	Puede permitir el nombre DNS del servidor o las direccion es 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.

> **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 usar `EndpointType=VPC_ENDPOINT`, utilice el nuevo tipo de punto de conexión de VPC (`EndpointType=VPC`), que puede utilizar como interno u orientado a Internet, como se describe en la tabla anterior. Para obtener más detalles, consulte Suspender el uso de VPC_ENDPOINT.

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

- Utilice un punto de conexión de VPC con acceso interno, de modo que solo puedan acceder al servidor los clientes de su VPC o entornos conectados a VPC, como un centro de datos local a través de una VPN. AWS 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 detalles, consulte the section called “Cree un servidor compatible con SFTP”.

> **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 detalles, consulte the section called “Cree un servidor compatible con FTPS”.
- Protocolo de File Transfer (FTP): File Transfer sin cifrar. Para obtener más detalles, consulte the section called “Cree un servidor compatible con FTP”.
- Declaración de aplicabilidad 2 (AS2): transferencia de archivos para transportar datos estructurados business-to-business . Para obtener más detalles, consulte the section called “Configurar AS2”. En el caso de AS2, puede crear rápidamente una AWS 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 detalles, 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 detalles, consulte Uso del proveedor de identidad de AWS Directory Service.
- Un método personalizado. El método de proveedor de identidad personalizado utiliza AWS Lambda o Amazon API Gateway y le permite integrar su servicio de directorio para autenticar y autorizar a sus usuarios. El servicio asigna automáticamente un identificador que designa cada servidor de forma unívoca. Para obtener más detalles, consulte Uso de proveedores de identidad personalizados. Transfer Family proporciona AWS CloudFormation plantillas que puede usar para implementar rápidamente servidores que usen un proveedor de identidad personalizado.
  - funciones de Lambda para autenticacióndescribe CloudFormation las plantillas que utilizan una función Lambda para la autenticación.
  - Autenticación mediante un método de API Gatewaydescribe CloudFormation las plantillas que utilizan un método de Amazon API Gateway para la autenticación.

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 AWS Pricing Calculator para obtener una estimación del costo de usar Transfer Family, consulta AWS Transfer Family los precios.

Cree un servidor compatible con SFTP

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.

> **Note**
>
> Los servidores SFTP de Transfer Family funcionan a través del puerto 22. Para los puntos finales alojados en VPC, los servidores SFTP Transfer Family también pueden funcionar a través del puerto 2222 o el puerto 22000. Para obtener más detalles, consulte 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.

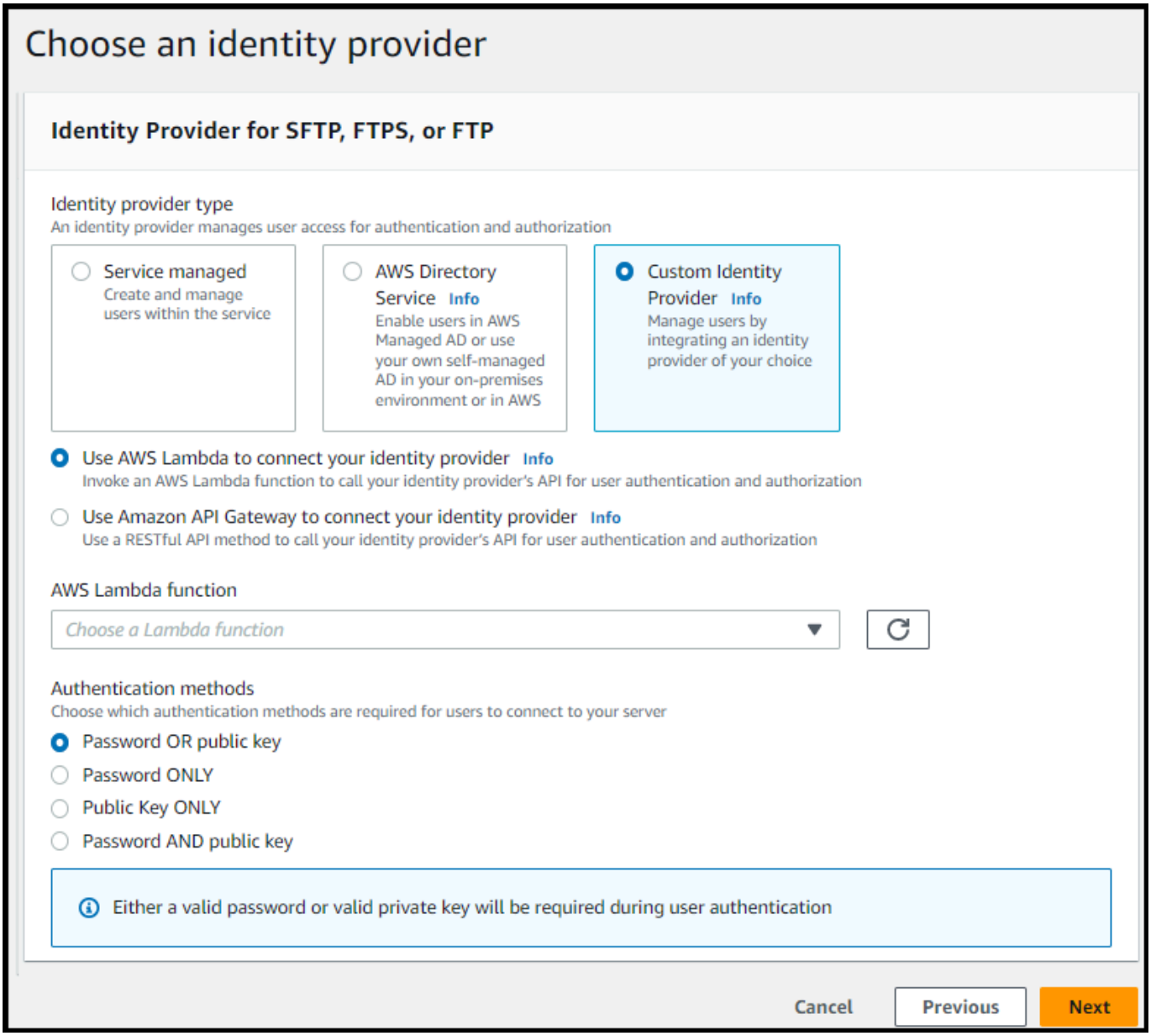
Creación de un servidor compatible con SFTP

1. Abre la AWS Transfer Family consola en https://console.aws.amazon.com/transfer/, selecciona Servidores en el panel de navegación y, a continuación, selecciona 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— Usted proporciona un AWS 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, consulteUso del proveedor de identidad de AWS Directory Service.

> **Note**
>
> - No se admiten los directorios multicuenta y compartidos. AWS Managed Microsoft AD
> - Para configurar un servidor con Directory Service como proveedor de identidad, debe añadir algunos AWS Directory Service permisos. Para obtener más detalles, 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.

  Para cualquiera de las opciones, también puede especificar cómo se va a autenticar.
  - Contraseña o clave: los usuarios pueden autenticarse con su contraseña o su clave. Este es el valor predeterminado.
  - 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.



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. (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.

c. (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**
>
> Los puntos de conexión con FIPS solo están disponibles en las regiones de Norteamérica 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 obtener más información acerca del FIPS, consulte Estándar federal de procesamiento de la información (FIPS) 140-2 .

d. Elija Siguiente.

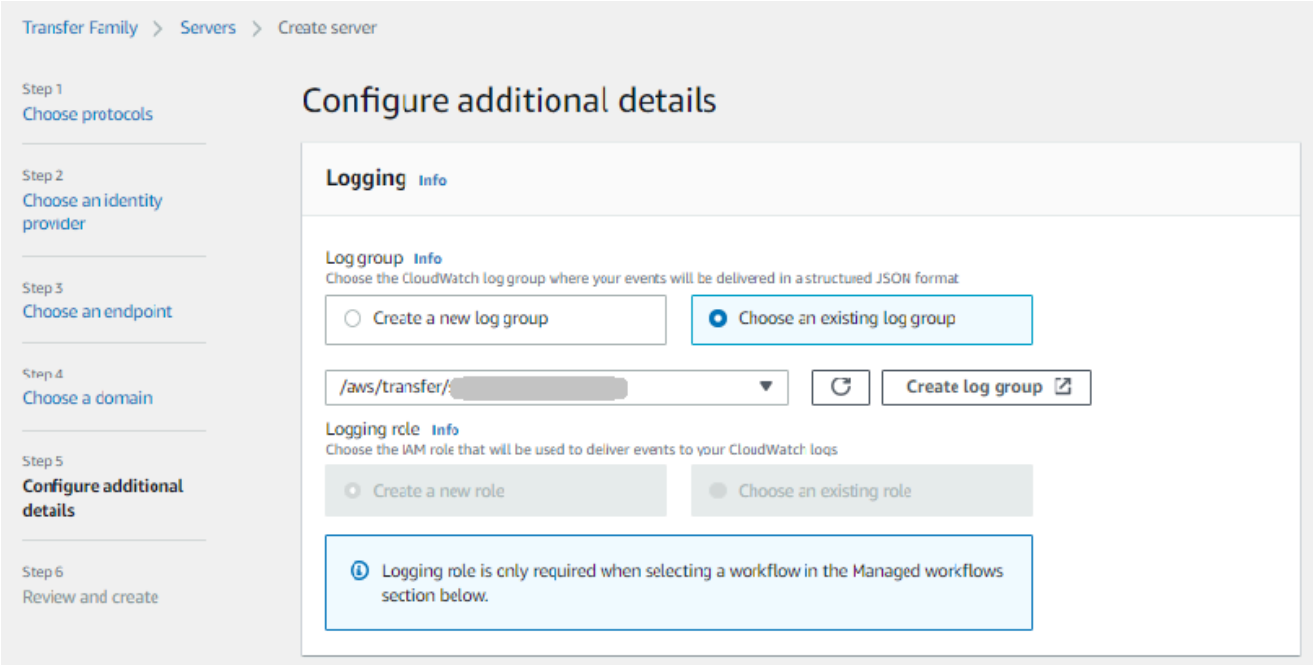
6. En la página Elegir dominio, elige el servicio AWS de almacenamiento que deseas usar para almacenar tus datos y acceder a ellos a través del protocolo seleccionado:

   - 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.

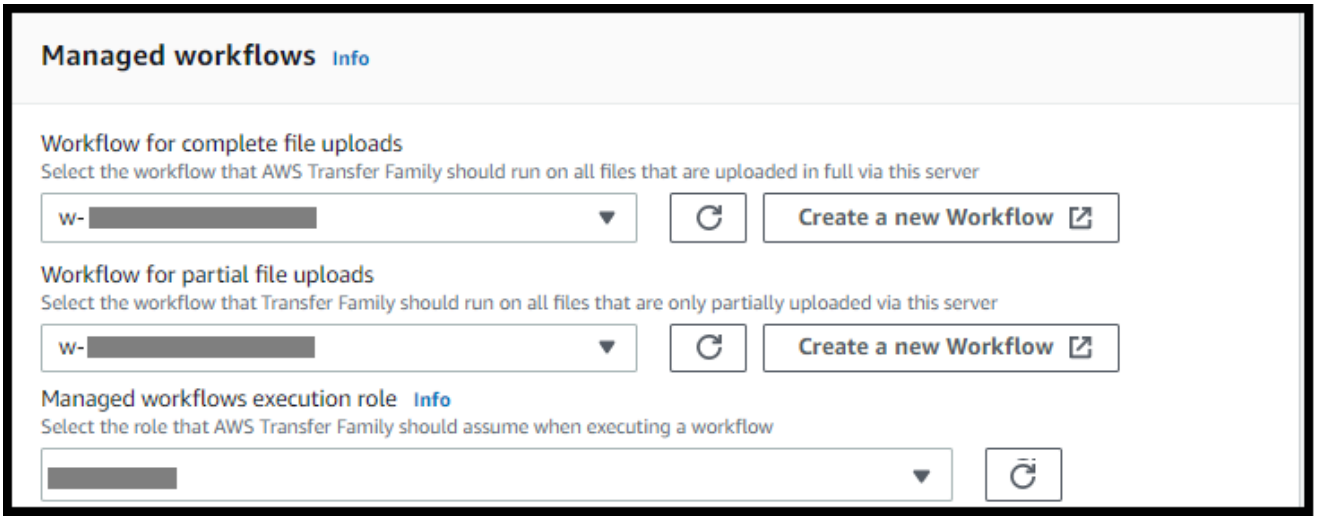
7. En Configurar detalles adicionales, haga lo siguiente:

   a. Para el registro, especifique un grupo de registro de ya existente o cree uno nuevo (la opción predeterminada). 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.



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 servidores AWS Transfer Family](#).

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.

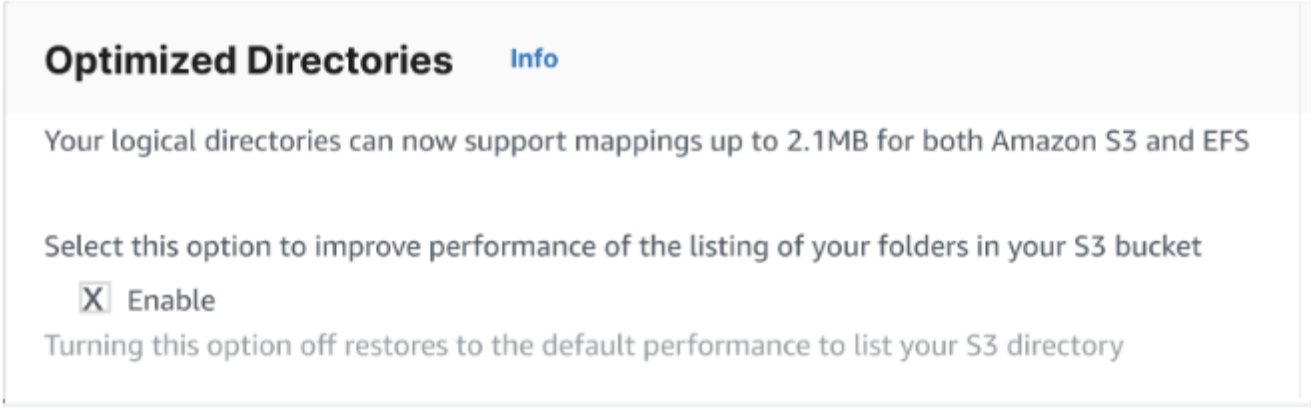
   > **Note**
   >
   > La sección Clave de host del servidor se usa solo para migrar usuarios desde un servidor existente habilitado para SFTP.

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. Seleccione Next (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.

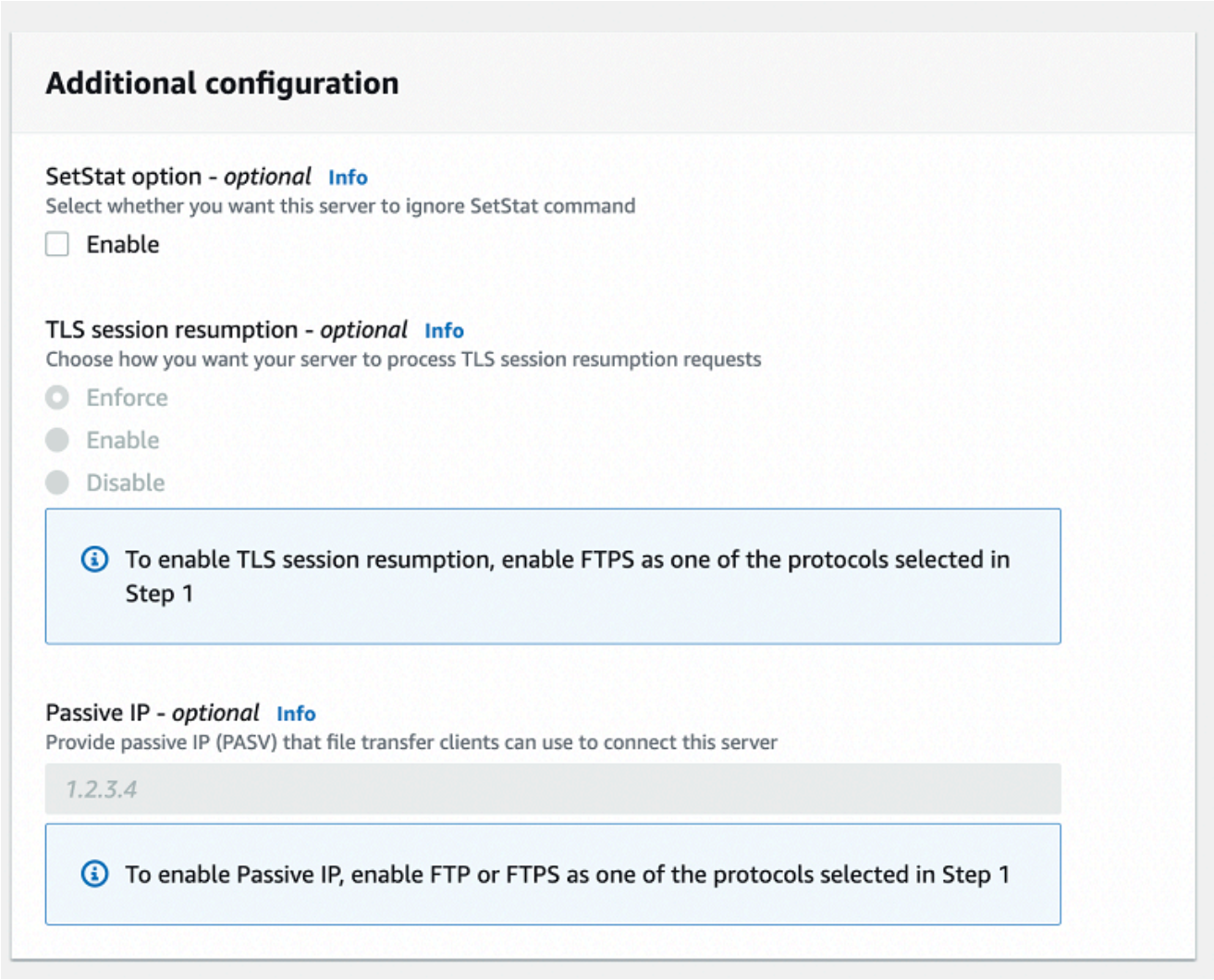
   Al crear el servidor mediante la consola, los directorios optimizados están habilitados de forma predeterminada. Si crea el servidor mediante la API, este comportamiento no está habilitado de forma predeterminada.



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 encabezado de visualización previa a la autenticación, introduzca el mensaje de texto que desee mostrar a los usuarios antes de que se autentiquen.

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.



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, consulteAdministración de usuarios para puntos finales de servidor.

Cree un servidor compatible con FTPS

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.

Creación de un servidor compatible con FTPS

1. Abra la AWS Transfer Family consola en https://console.aws.amazon.com/transfer/, seleccione Servidores en el panel de navegación y, a continuación, elija Crear servidor.
2. En Elegir protocolos, seleccione FTPS.

   Para el certificado del servidor, seleccione un certificado almacenado en AWS Certificate Manager (ACM) que se utilizará para identificar su servidor cuando los clientes se conecten a través de FTPS y luego, 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)

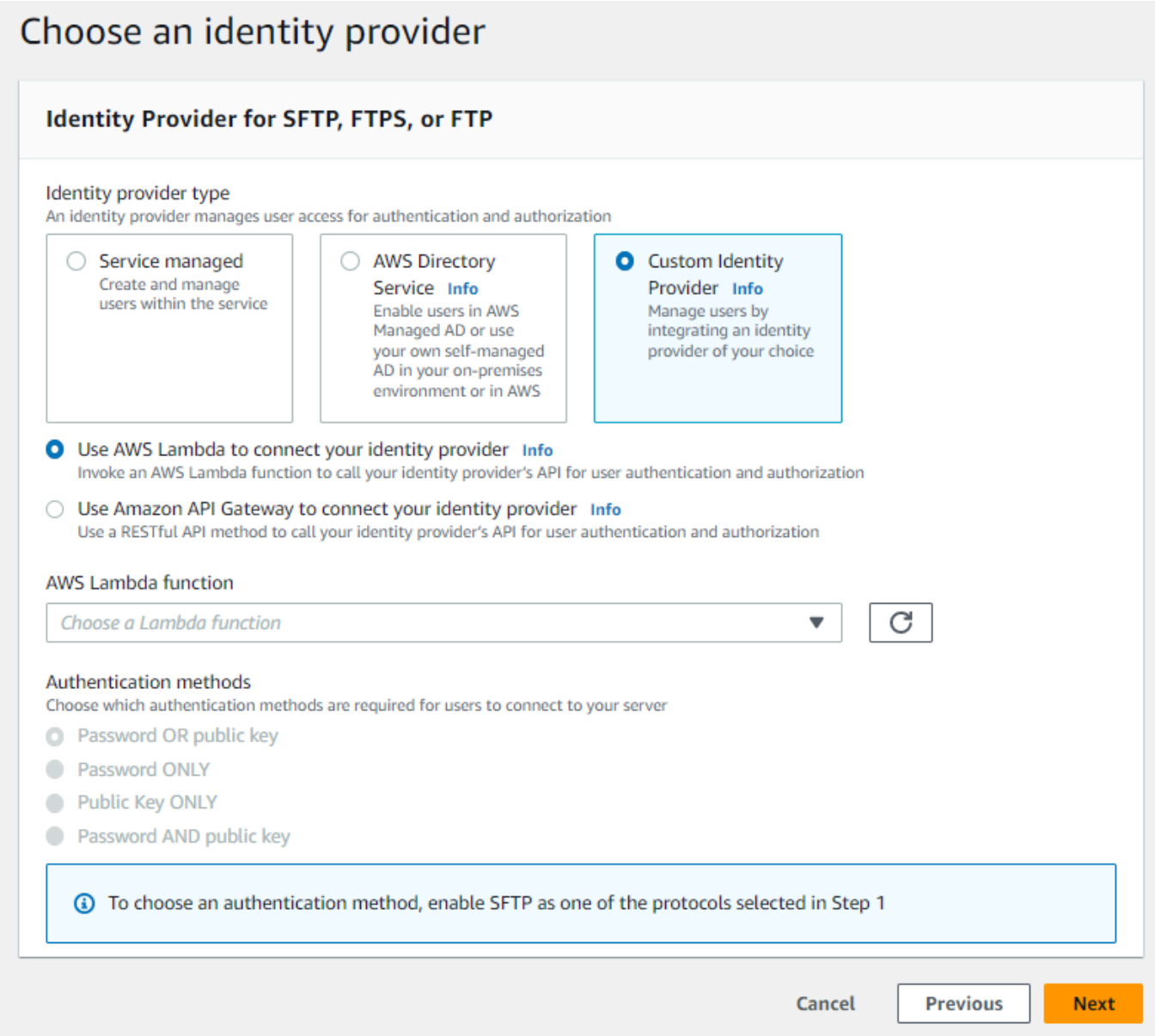
> **Note**
>
> El certificado debe ser un certificado SSL/TLS X.509 versión 3 válido con el FQDN o la dirección IP especificados y contener información sobre el emisor.

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 directorio para acceder al punto final. AWS Directory Service 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, consulteUso del proveedor de identidad de AWS Directory Service.

     > **Note**
     >
     > - No se admiten los directorios multicuenta y compartidos. AWS Managed Microsoft AD
     > - Para configurar un servidor con Directory Service como proveedor de identidad, debe añadir algunos AWS Directory Service permisos. Para obtener más detalles, 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.



4. Elija Siguiente.
5. En Elegir punto de conexión, haga lo siguiente:

> **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

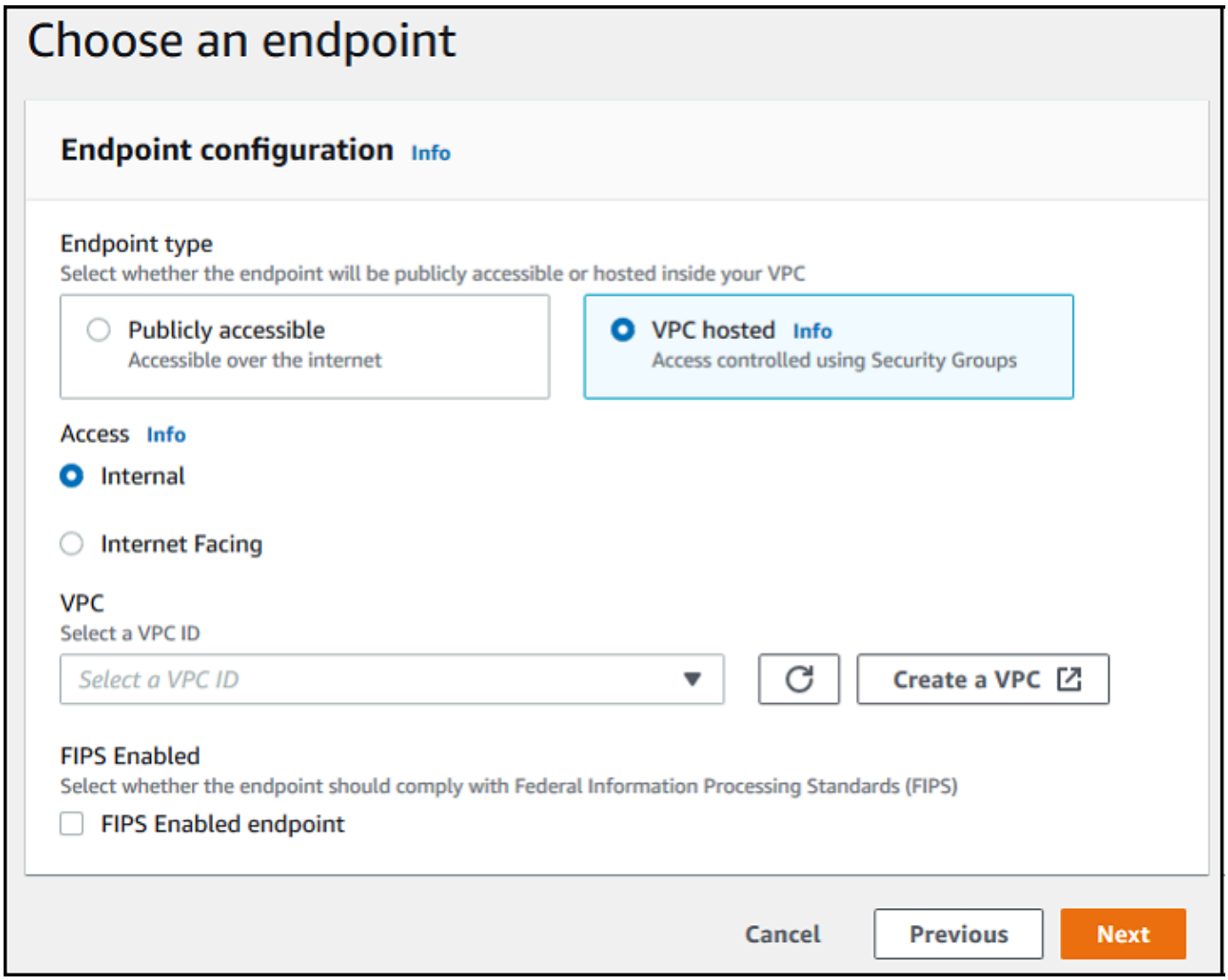
cómo configurar un punto de conexión de la VPC, consulte Creación de un servidor en una nube privada virtual (VPC).

> **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**
>
> Los puntos de conexión con FIPS solo están disponibles en las regiones de Norteamérica 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 obtener más información acerca del FIPS, consulte Estándar federal de procesamiento de la información (FIPS) 140-2 .

c. Elija Siguiente.



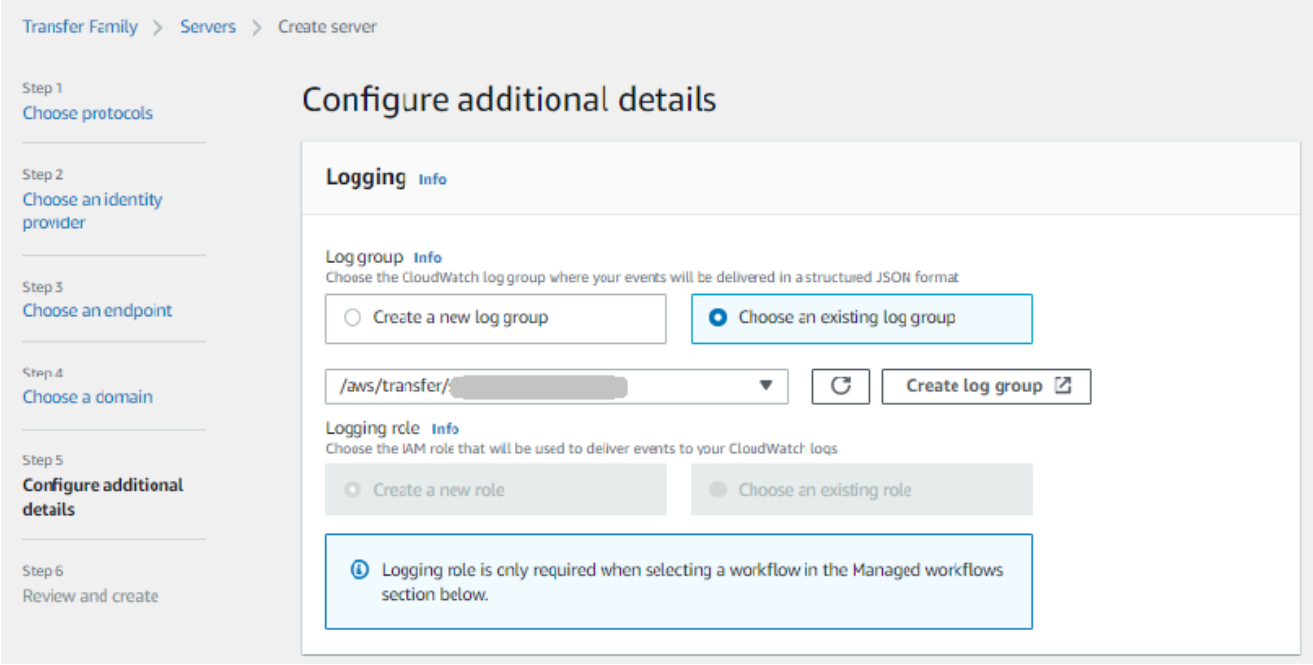
6. En la página Elegir dominio, elija el servicio AWS de almacenamiento que desee utilizar para almacenar sus datos y acceder a ellos mediante el protocolo seleccionado:

   - 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.

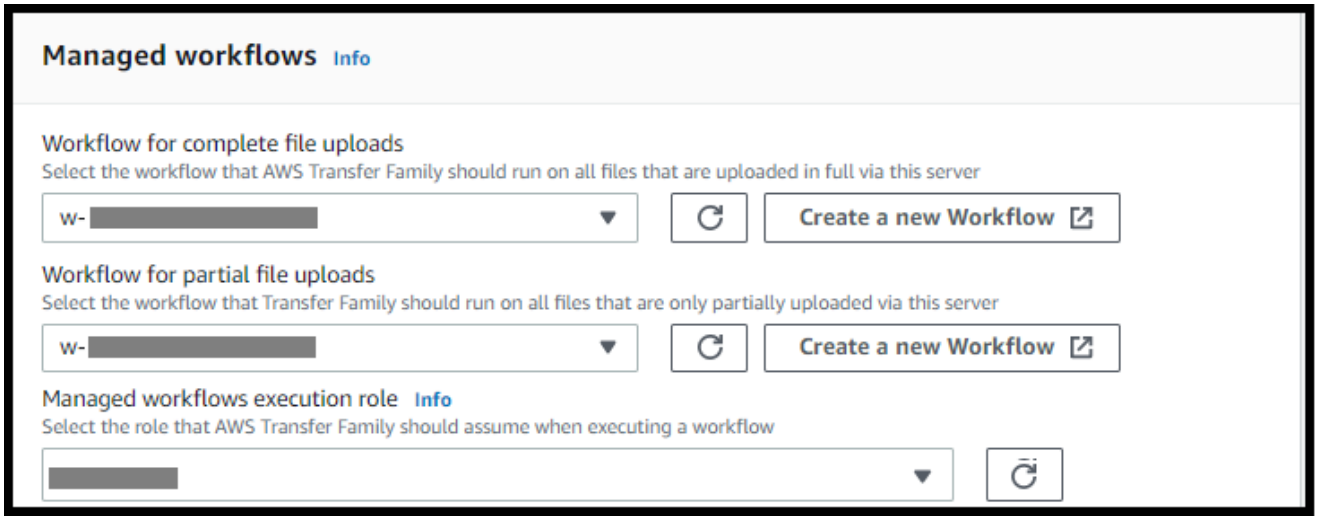
7. En Configurar detalles adicionales, haga lo siguiente:

a. Para el registro, especifique un grupo de registro de ya existente o cree uno nuevo (la opción predeterminada).



Si 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.



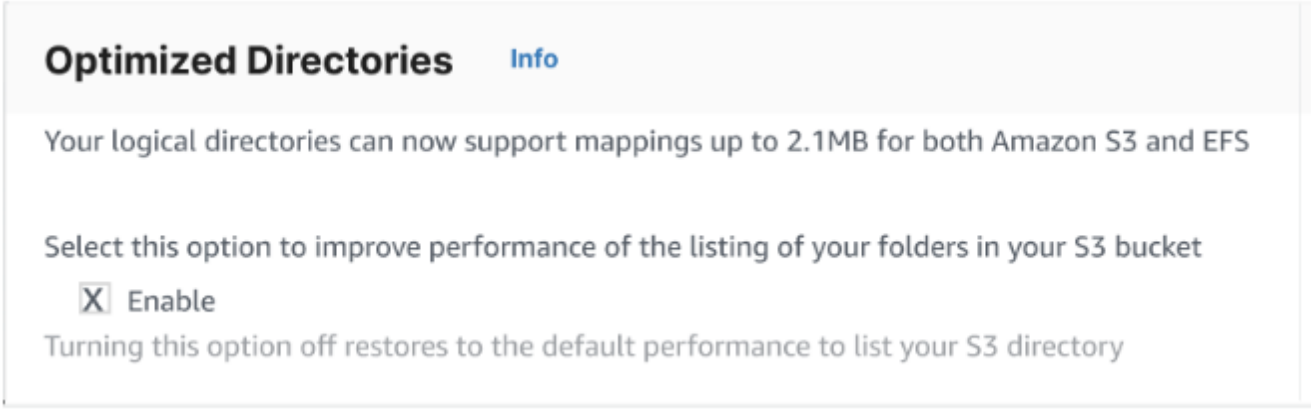
c. Para ver las opciones de algoritmos criptográficos, elija una política de seguridad que contenga los algoritmos criptográficos habilitados para su uso en el servidor. Nuestra política de seguridad más reciente es la predeterminada: para obtener más información, consulte[Políticas de seguridad para servidores AWS Transfer Family](#).

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.



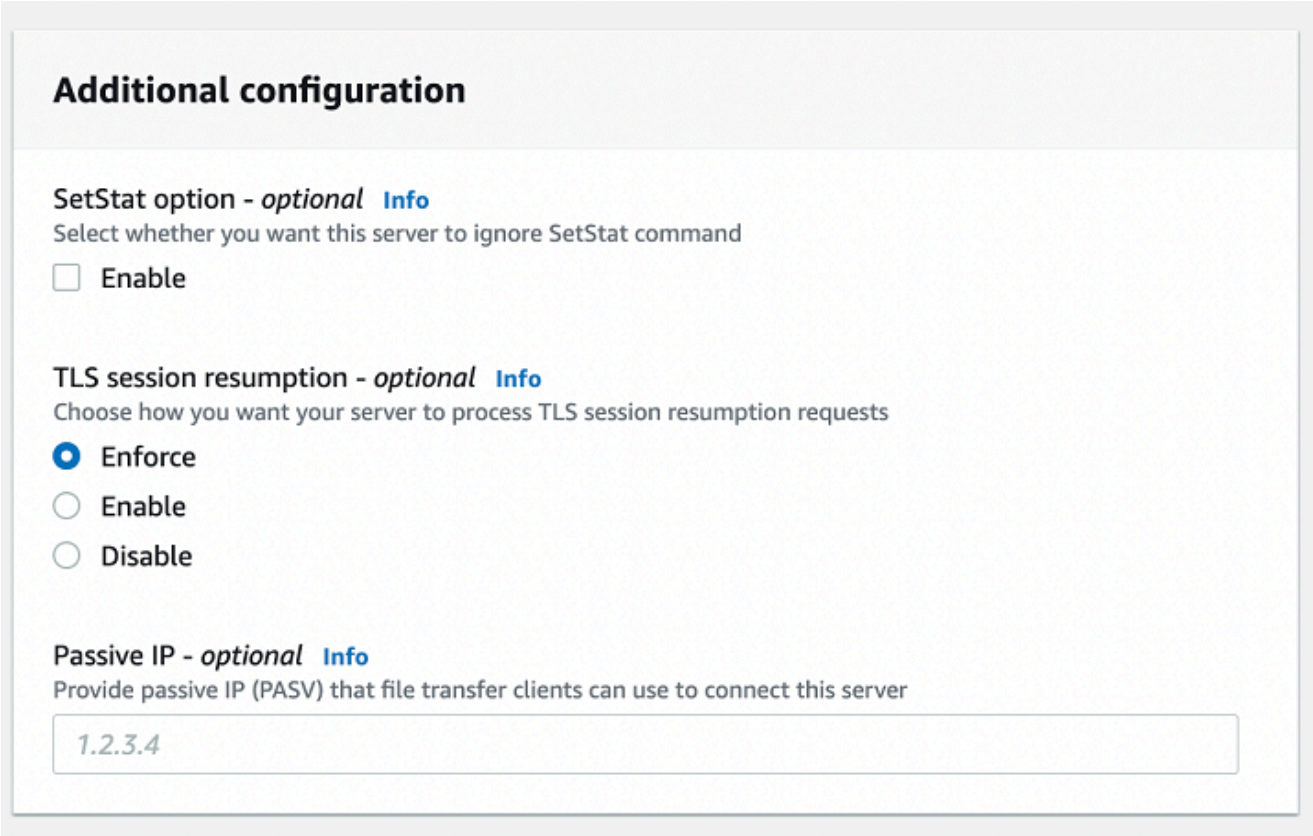
g. Elija Siguiente.

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.

   Para Mostrar banner, en el cuadro de texto Texto del banner de preautenticación, ingrese el mensaje de texto que desee mostrar a sus usuarios antes de que se autentiquen. En el cuadro de texto Texto del banner de postautenticación, ingrese el texto que desee mostrar a sus usuarios después de que se autentiquen 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 ProtocolDetailstema.
   - 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 ProtocolDetailstema.
   - 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 ProtocolDetailstema.



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 compatible con FTP

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 punto final alojado en VPC. Si necesita que su servidor haga que los datos atraviesen la red pública, debe utilizar protocolos seguros, como SFTP o FTPS.

Creación de un servidor compatible con FTP

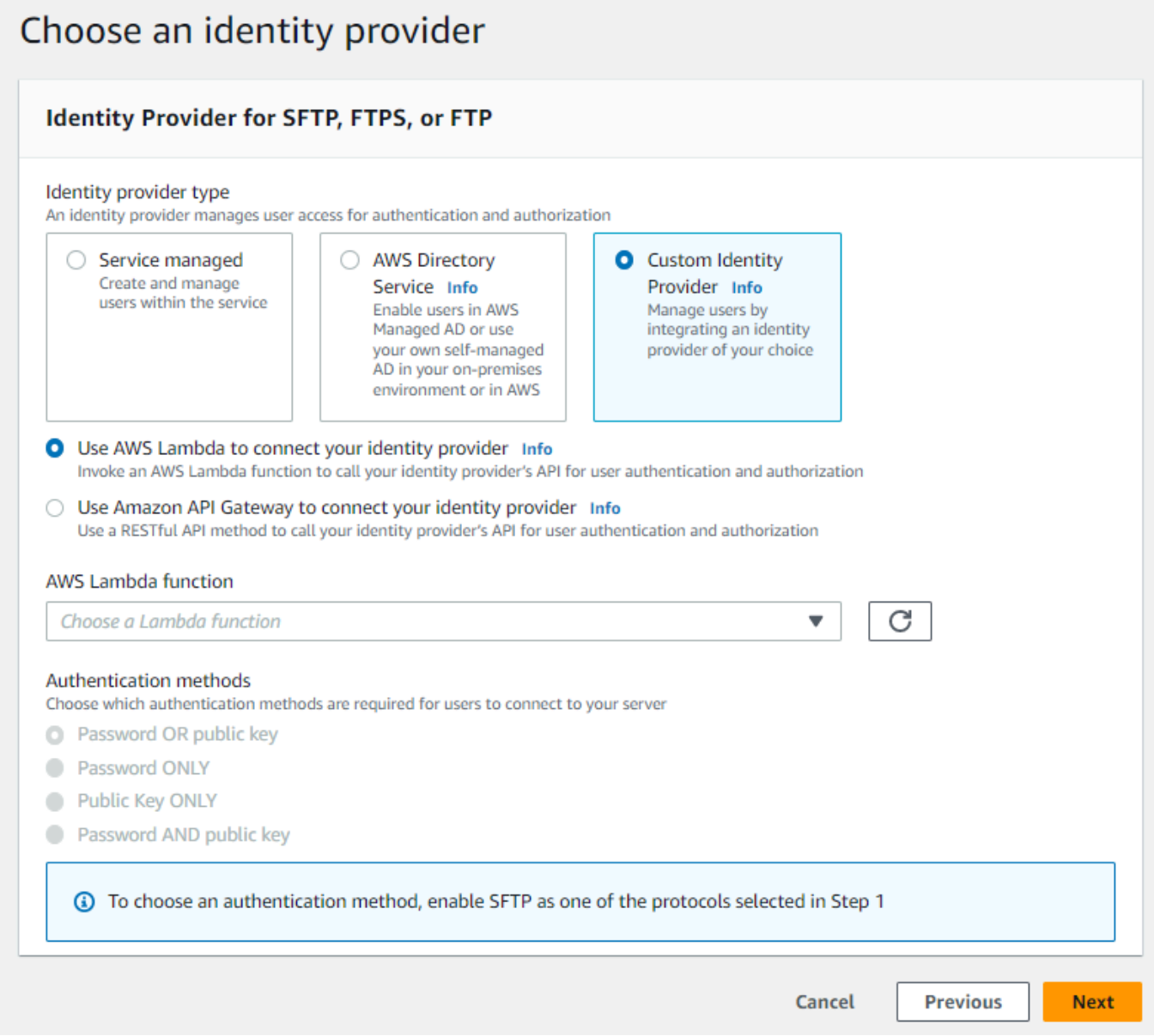
1. Abra la AWS Transfer Family consola en https://console.aws.amazon.com/transfer/ y seleccione Servidores en el panel de navegación y, a continuación, elija Crear servidor.
2. En Elegir protocolos, seleccione FTP y, a continuación, Siguiente.
3. En Elegir un proveedor de identidad, seleccione el proveedor 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 AWS 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, consulteUso del proveedor de identidad de AWS Directory Service.

     > **Note**
     >
     > - No se admiten los directorios multicuenta y compartidos. AWS Managed Microsoft AD
     > - Para configurar un servidor con Directory Service como proveedor de identidad, debe añadir algunos AWS Directory Service permisos. Para obtener más detalles, 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.



4. Elija Siguiente.

5. En Elegir punto de conexión, haga lo siguiente:

> **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).

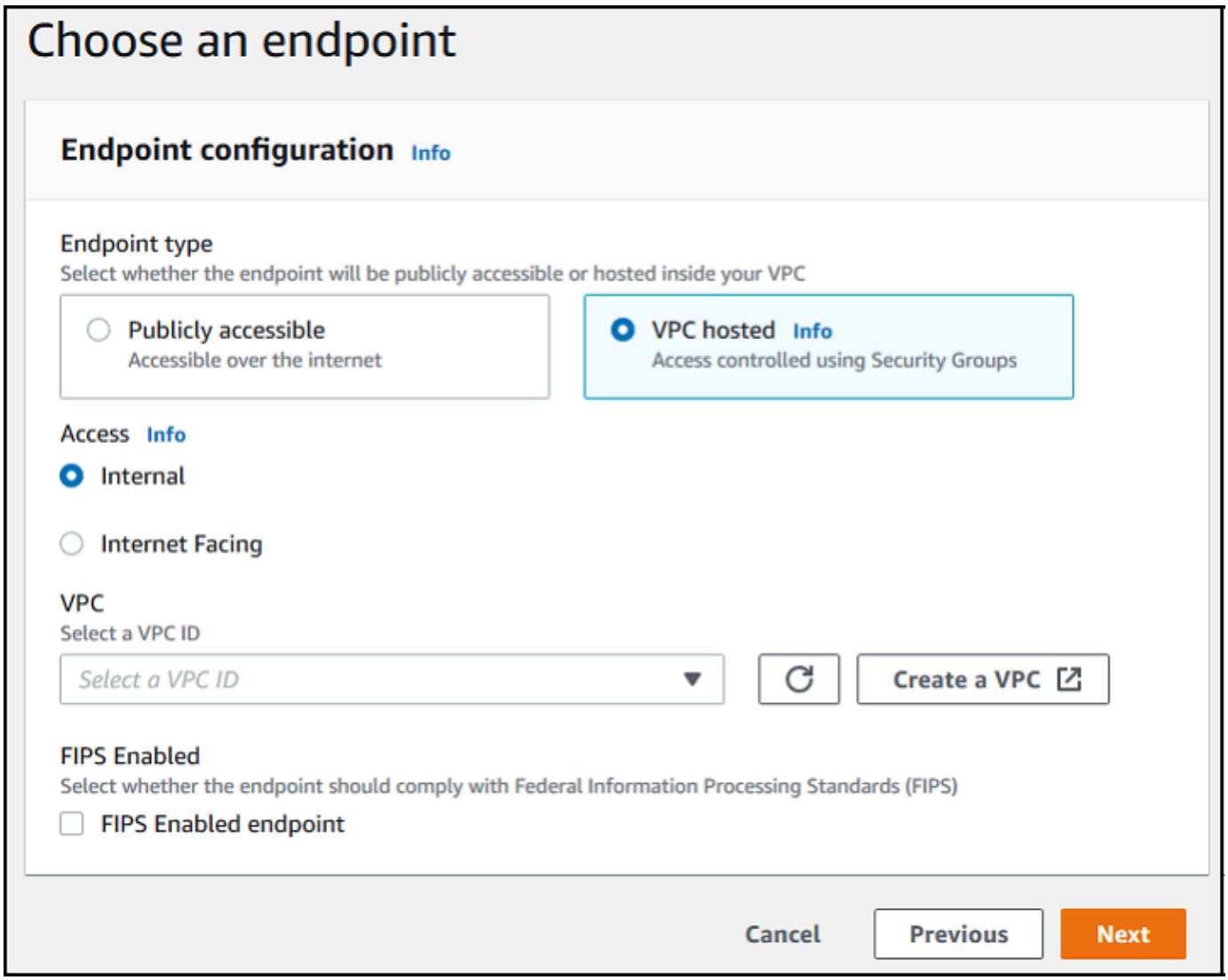
a. En el tipo de punto de conexión, seleccione el punto de conexión alojado en la VPC para alojar el punto de conexión de su servidor. Para obtener más información acerca de cómo configurar un punto de conexión de la VPC, consulte Creación de un servidor en una nube privada virtual (VPC).

> **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**
>
> Los servidores FTP no admiten puntos de conexión con FIPS.

c. Elija Siguiente.



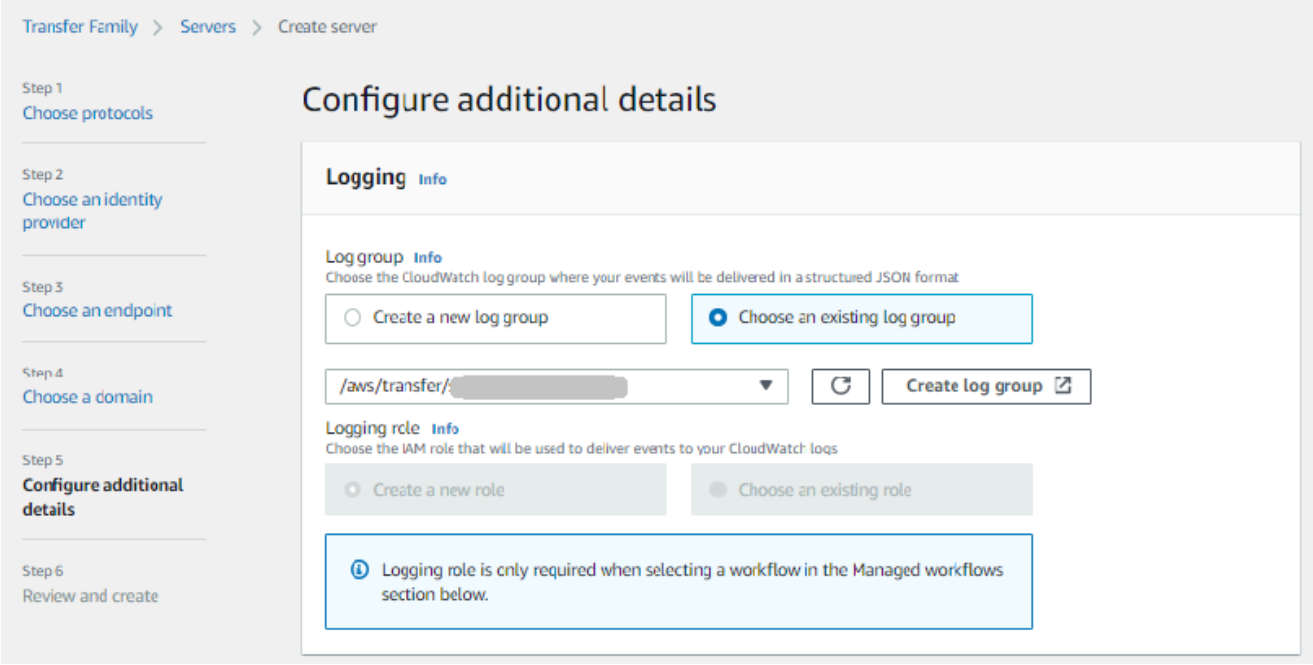
6. En la página Elegir dominio, elija el servicio AWS de almacenamiento que desee usar para almacenar sus datos y acceder a ellos a través del protocolo seleccionado.

   - 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.

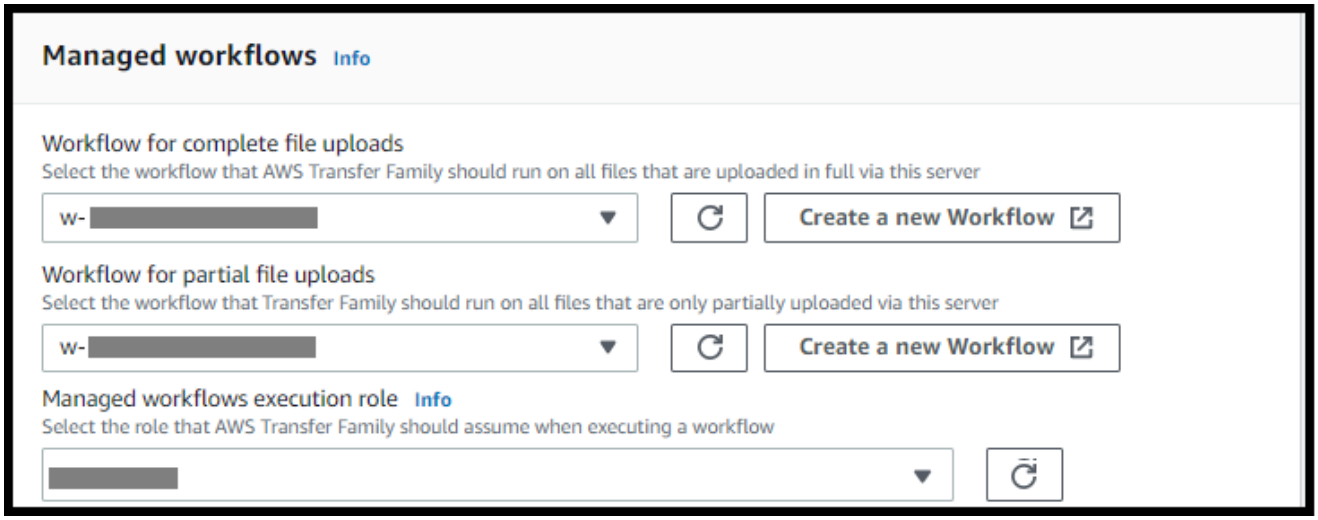
7. En Configurar detalles adicionales, haga lo siguiente:

a. Para el registro, especifique un grupo de registro de ya existente o cree uno nuevo (la opción predeterminada).



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.



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.

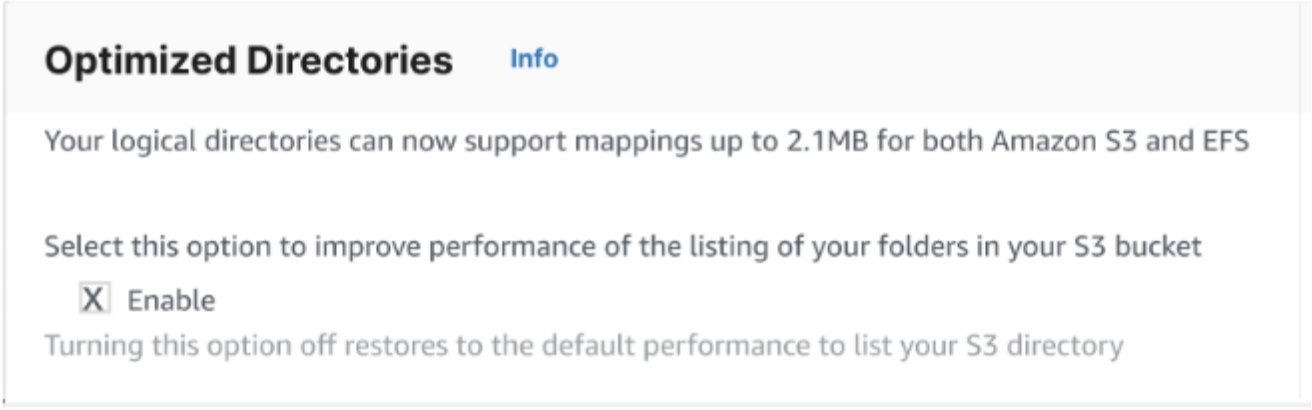
> **Note**
>
> Transfer Family asigna la política de seguridad más reciente a su servidor FTP. Sin embargo, dado que el protocolo FTP no utiliza ningún tipo de cifrado, los servidores FTP no utilizan ninguno de los algoritmos de política de seguridad. A menos que su servidor también utilice el protocolo 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.



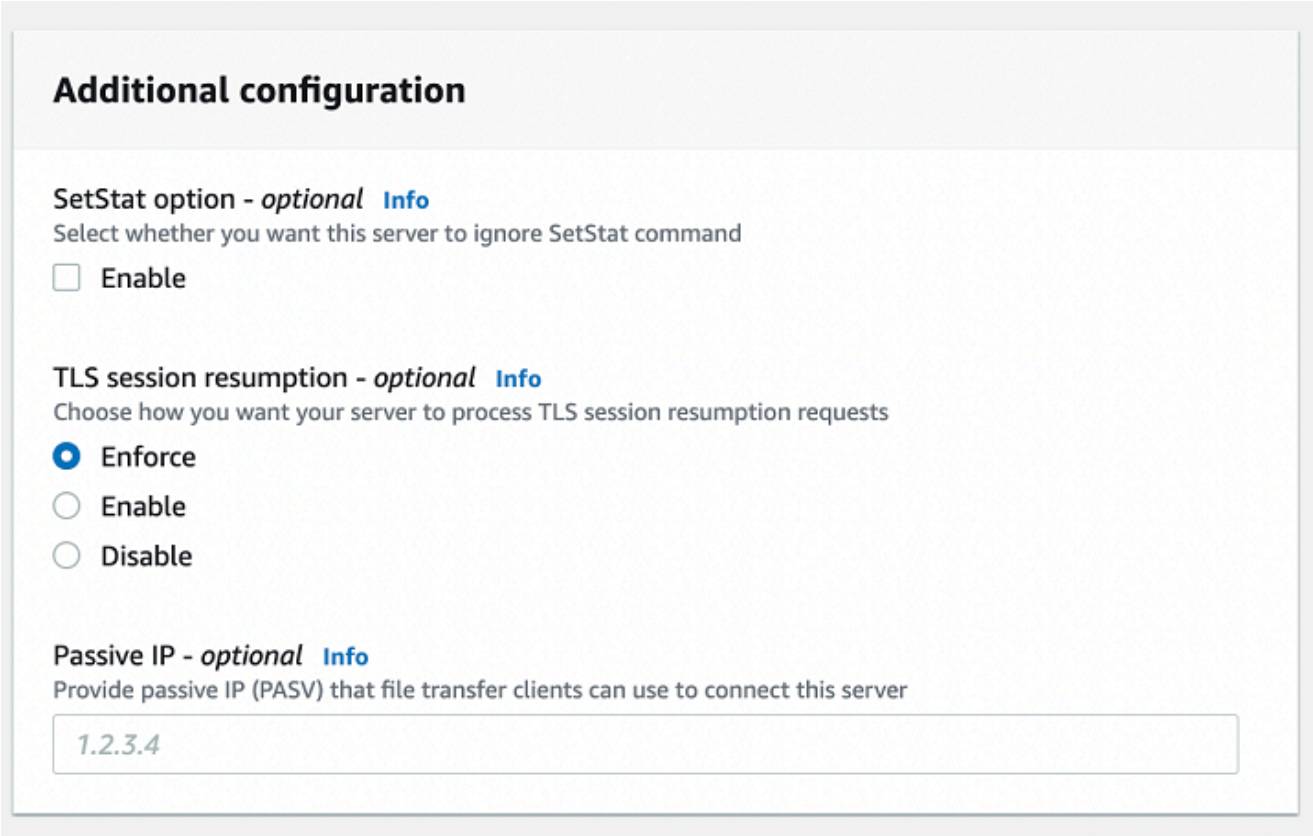
g. Elija Siguiente.

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.

   Para Mostrar banner, en el cuadro de texto Texto del banner de preautenticación, ingrese el mensaje de texto que desee mostrar a sus usuarios antes de que se autentiquen. En el cuadro de texto Texto del banner de postautenticación, ingrese el texto que desee mostrar a sus usuarios después de que se autentiquen 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 ProtocolDetailstema.
   - 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 ProtocolDetailstema.
   - 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 ProtocolDetailstema.



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 “Suspender el uso de 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.

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
- 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: creación de un servidor compatible con SFTP.
4. En Elegir un proveedor de identidad, selecciona Servicio gestionado para almacenar las identidades y claves de los usuarios y AWS Transfer Family, a continuación, selecciona Siguiente.

   > **Note**
   >
   > 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:

> **Note**
>
> Los servidores FTP y FTPS de 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.

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.

> **Note**
>
> 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.

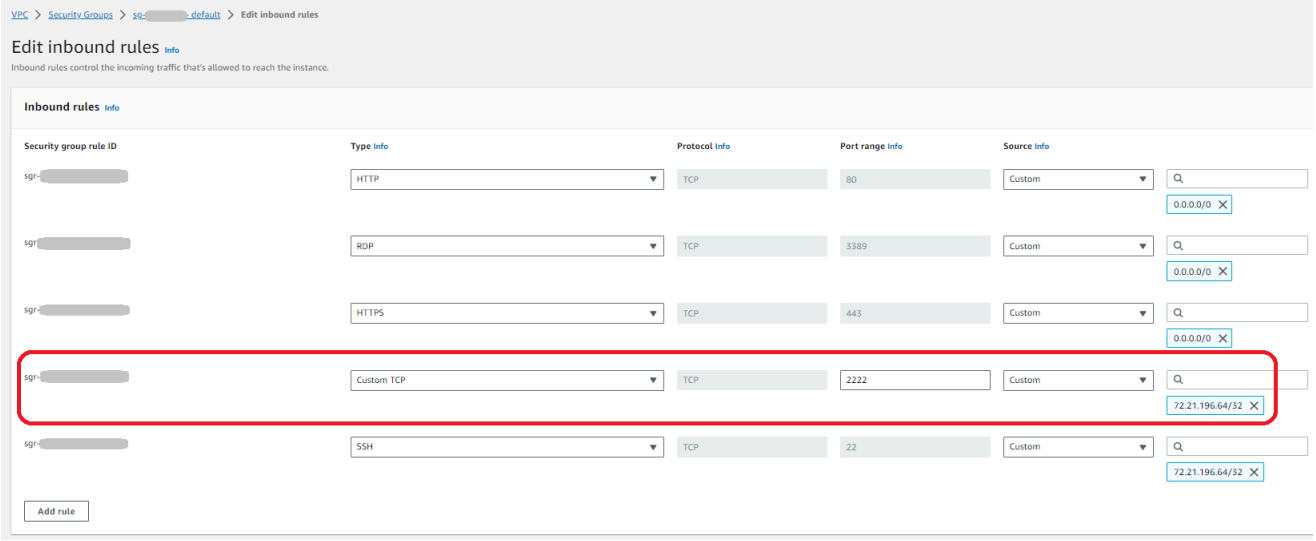
e. En la sección Grupos de seguridad, elija uno o varios ID de grupo de seguridad existentes o elija Crear un grupo de seguridad para crear un grupo de seguridad nuevo. Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad para su VPC en la Guía del usuario de Amazon 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.

> **Note**
>
> También puedes 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.



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**
>
> Los puntos de conexión con FIPS solo están disponibles en las regiones de Norteamérica 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 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, consulteConfigura 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-2020-06` 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 servidores AWS Transfer Family.

c. (Opcional: esta sección es solo para migrar usuarios desde un servidor existente habilitado para SFTP). Para 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. Seleccione Next (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: creación de un servidor compatible con SFTP.
4. En Elegir un proveedor de identidad, selecciona Servicio gestionado para almacenar las identidades y claves de los usuarios y AWS Transfer Family, a continuación, selecciona Siguiente.

   > **Note**
   >
   > 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.

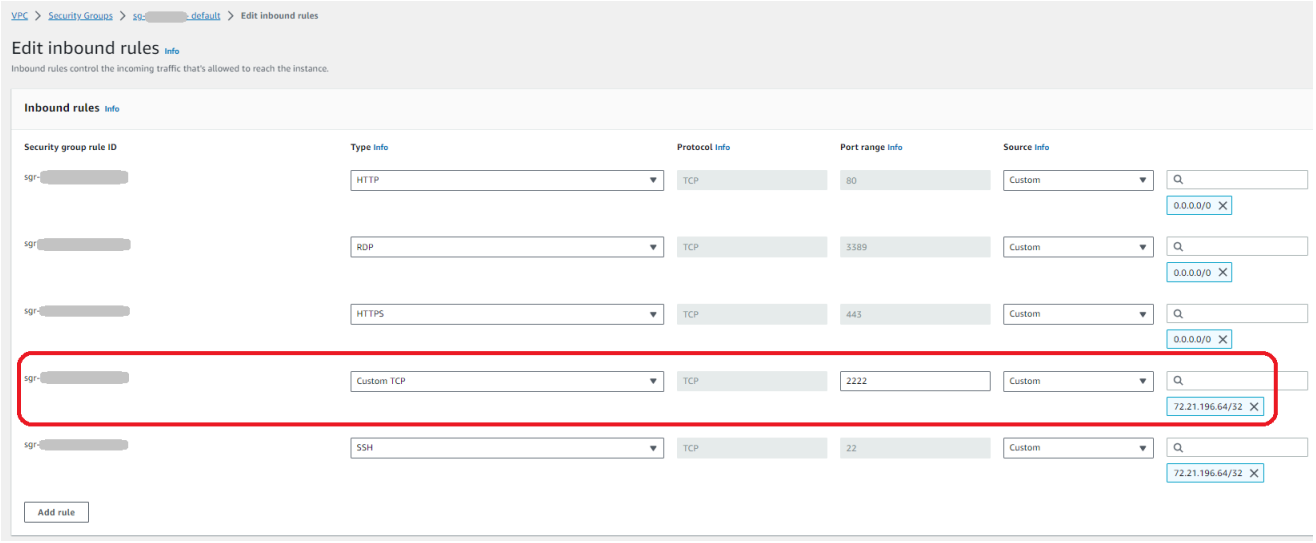
f. En la sección Grupos de seguridad, elija uno o varios ID de grupo de seguridad existentes o elija Crear un grupo de seguridad para crear un grupo de seguridad nuevo. Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad para su VPC en la Guía del usuario de Amazon 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.

> **Note**
>
> También puedes 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.



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**
>
> Los puntos de conexión con FIPS solo están disponibles en las regiones de Norteamérica 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 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, consulteConfigura 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-2020-06` seguridad se adjunta a su servidor a menos que elija una diferente.

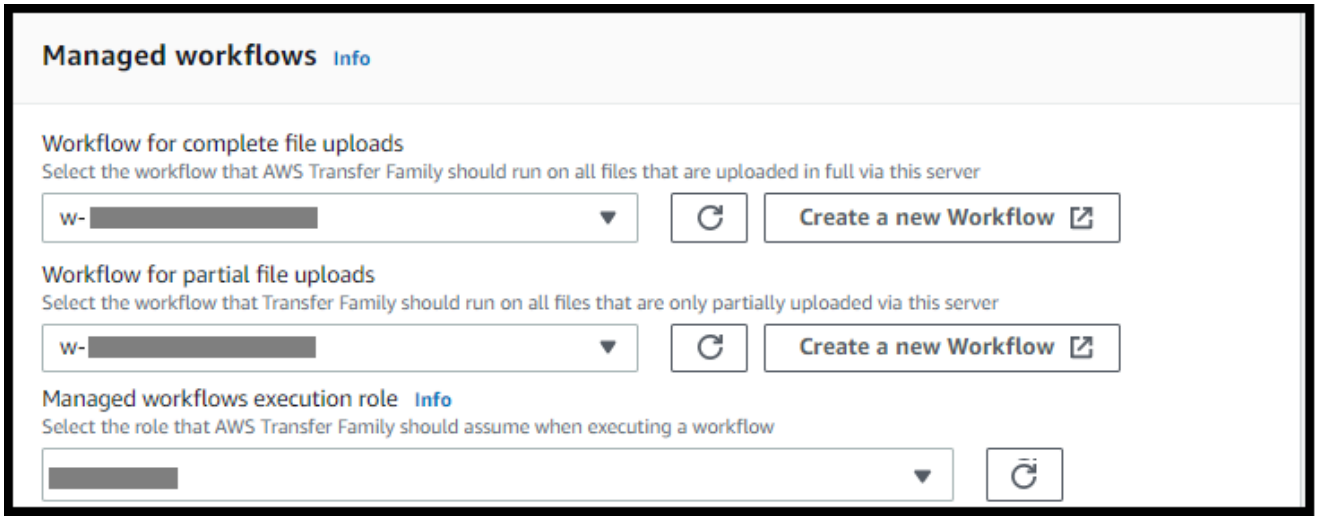
Para obtener más información sobre las políticas de seguridad, consulte Políticas de seguridad para servidores AWS Transfer Family.

c. (Opcional: esta sección es solo para migrar usuarios desde un servidor existente habilitado para SFTP). Para 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. Seleccione Next (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.



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 rellenada 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 Guardar.

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 va a dejar 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 `EndpointType=VPC_ENDPOINT` ellos. 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 AWS PrivateLink los precios.

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, consulta la entrada de blog sobre el uso de direcciones IP permitidas AWS Transfer Family para proteger tus 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 características y la compatibilidad con FTPS/FTP 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 AWS 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 tienes más preguntas, puedes ponerte en contacto con nosotros AWS Support o con tu equipo de cuentas.

Actualización del tipo de punto final AWS Transfer Family del servidor de VPC_ENDPOINT a VPC

Puedes usar la AWS Management Console API Transfer Family o la API Transfer Family para actualizar el servidor `EndpointType` de `VPC_ENDPOINT` a`VPC`. AWS 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
- Actualizar el tipo de punto final del servidor mediante el AWS Management Console
- Actualización del tipo de punto final del servidor mediante AWS 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 AWS Management Console.

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 llamadas a la ListServers API Amazon EC2 DescribeRegionsy Transfer Family para obtener una lista de los ID de servidor y las regiones de todos los servidores que utiliza. `VPC_ENDPOINT` Si tiene varias AWS cuentas, 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`.

Actualizar el tipo de punto final del servidor mediante el AWS Management Console

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 AWS CloudFormation

En esta sección se describe AWS CloudFormation cómo actualizar el servidor `EndpointType` aVPC. Utilice este procedimiento para los servidores Transfer Family que haya desplegado mediante AWS CloudFormation. En este ejemplo, la AWS CloudFormation plantilla original utilizada para implementar el servidor Transfer Family se muestra de la siguiente manera:

```
AWS TemplateFormatVersion: '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 AWS 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. Actualice la CloudFormation pila

   a. Abre la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.

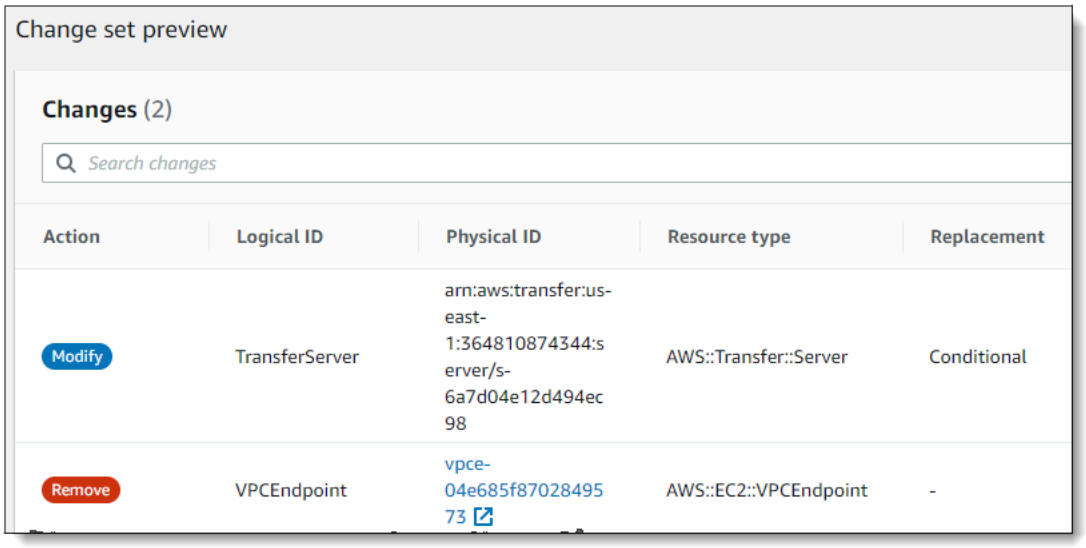
   b. Seleccione la pila de que se va a utilizar para crear el servidor de Transfer Family.

   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:



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. Seleccione el servidor en el que ha realizado la actualización y AWS 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: creación de un servidor compatible con SFTP. 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 la consola, el nombre de host de un punto de conexión tiene este aspecto:

serverid.server.transfer.*region*.amazonaws.com

> **Note**
>
> Si su servidor tiene un punto de conexión 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) AWS 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 AWS Management Console y ábrala en https://console.aws.amazon.com/route53/.

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 número máximo de sesiones SFTP simultáneas y multiplexadas por conexión es de 10.
- Hay dos valores de tiempo de espera para las conexiones SFTP/FTP/FTPS. Para las conexiones inactivas, el valor de tiempo de espera es de 1800 segundos (30 minutos). Si no hay actividad una vez transcurrido el período, es posible que el cliente se desconecte. También hay un tiempo de espera de 300 segundos (5 minutos) cuando un cliente deja de responder por completo.

- Amazon S3 y Amazon EFS (debido al protocolo NFSv4) requieren que los nombres de archivo estén codificados en 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 imagen/binario.
- Para FTP y FTPS, TLS: PROT C (desprotegido) El TLS para la conexión de datos es el valor predeterminado, pero PROT C no es compatible con el protocolo FTPS. 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_READLINK	SSH_FXP_SYMLINK	SSH_FXP_STAT cuando el archivo solicitado es un enlace simbólico	SSH_FXP_REALPATH cuando la ruta solicitada 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 SFTP/FTPS/FTP disponibles
- Encuentre su punto de conexión de Amazon VPC
- Evite errores setstat
- Uso de OpenSSH
- Utilice WinSCP
- Uso de Cyberduck
- Usa FileZilla
- Utilice un cliente Perl
- Procesamiento de carga posterior

Comandos SFTP/FTPS/FTP disponibles

En la siguiente tabla se describen los comandos disponibles para los protocolos SFTP AWS Transfer Family, FTPS y FTP.

> **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.

Comandos SFTP/FTPS/FTP

Comando	Amazon S3	Amazon EFS
`cd`	Soportado	Soportado
`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

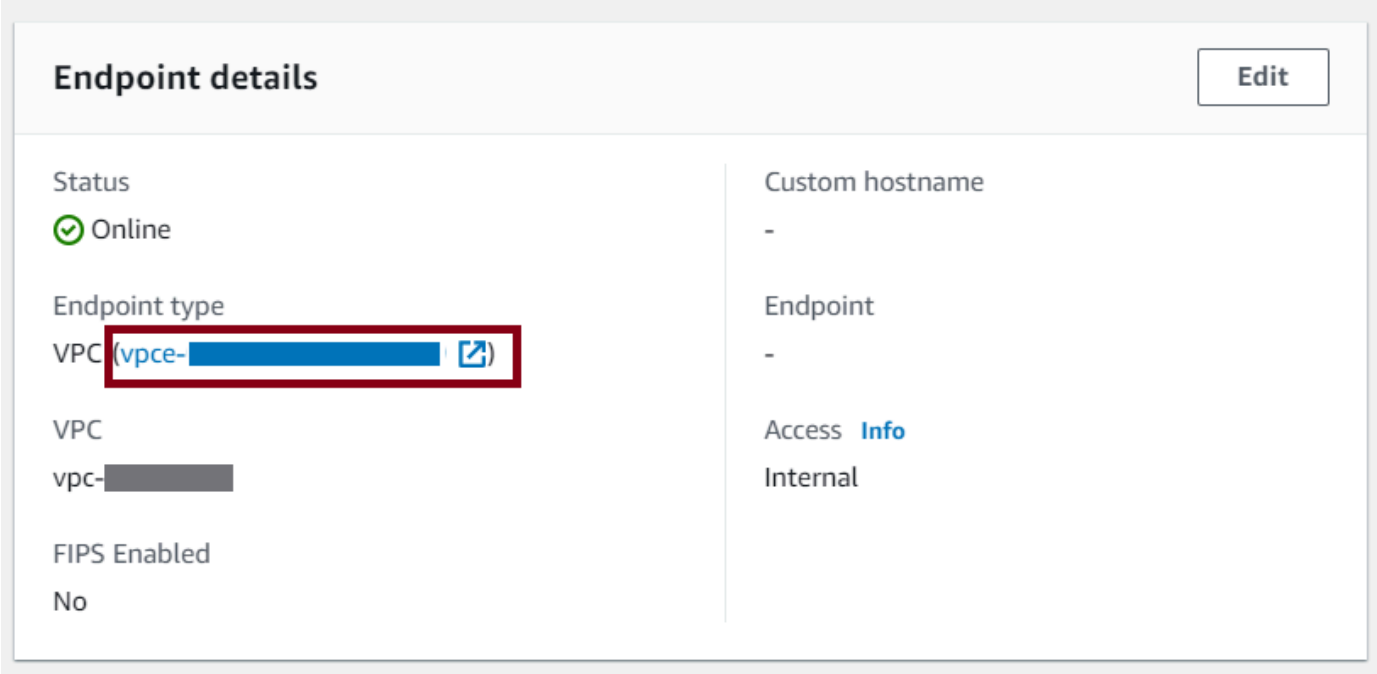
Comando	Amazon S3	Amazon EFS
`pwd`	Soportado	Soportado
`rename`	Solo se admite para archivos	Compatible **Note** No se admite el cambio de nombre que sobrescriba un archivo o directorio existente.
`rm`	Soportado	Soportado
`rmdir`	Compatible (solo directorios vacíos)	Soportado
`version`	Soportado	Soportado

Encuentre su punto de conexión de Amazon VPC

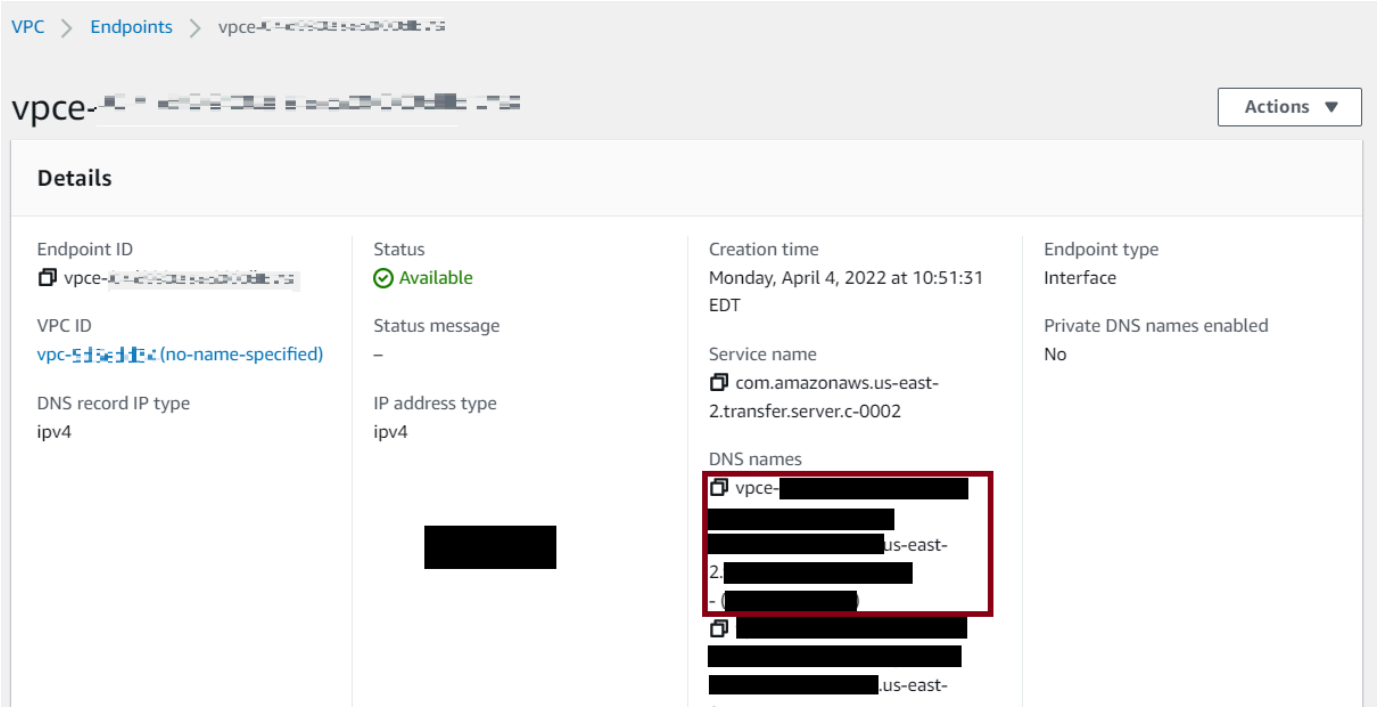
Si el tipo de punto de conexión de su servidor de Transfer Family es VPC, no es fácil identificar el punto de conexión que se va a utilizar para transferir archivos. En este caso, utilice el siguiente procedimiento para encontrar su punto de conexión de Amazon VPC.

Encuentre 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.



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.



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

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

> **Note**
>
> Este cliente solo funciona con un servidor habilitado para SFTP.

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* está 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 /my-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.

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 AWS sus credenciales y cargar/descargar archivos. 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.

   > **Note**
   >
   > 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.

> **Note**
>
> 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 del proveedor de identidad de AWS Directory Service
> - 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.

> **Note**
>
> 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 reanudación de la transferencia o la transferencia a un nombre de archivo temporal, seleccione Desactivar.

> **Note**
>
> 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.

> **Note**
>
> 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 drag-and-drop métodos para copiar archivos entre la ventana de destino y la de 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 File Transfer SSH), FTP-SSL (TLS de autenticación explícita) o FTP (protocolo de File Transfer).
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.

   > **Note**
   >
   > 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).

Usa FileZilla

Siga las instrucciones que aparecen a continuación para transferir archivos utilizando FileZilla.

FileZilla Para configurar una transferencia de archivos

1. Abre 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.

   > **Note**
   >
   > Si el servidor usa un punto de conexión de VPC, consulte Encuentre su punto de conexión de Amazon VPC.

   - Si utiliza SFTP, introduzca: `sftp://`*`hostname`*
   - Si utiliza FTPS, introduzca: `ftps://`*`hostname`*

   Asegúrese de reemplazar el *`nombre de host`* por el punto de conexión de su servidor actual.
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 el`queue_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.

Procesamiento de carga posterior

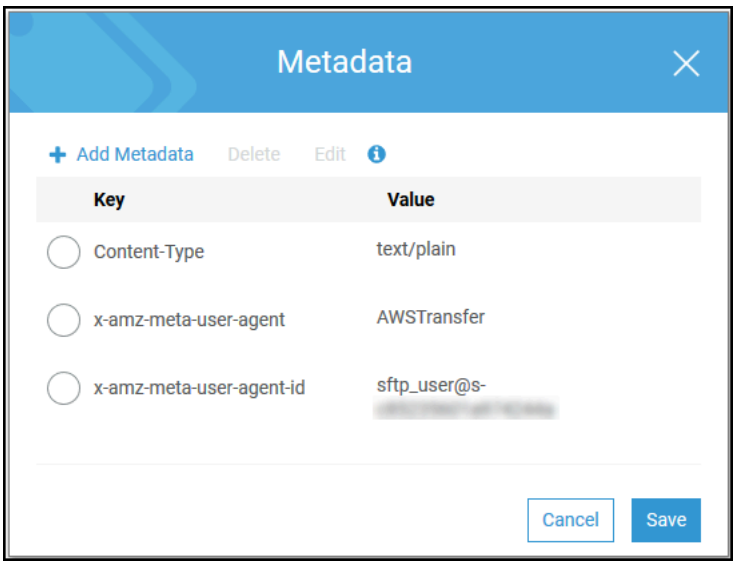
Puede ver la información de procesamiento posterior a la carga, incluidos los metadatos de los objetos de Amazon S3 y las notificaciones de eventos.

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 HeadObjectoperación en el objeto S3 dentro de la función Lambda.



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.

Administración de usuarios para puntos finales de servidor

En las secciones siguientes encontrará información sobre cómo agregar usuarios usando AWS Transfer Family, AWS Directory Service for Microsoft Active Directory o un proveedor de identidad personalizado.

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.

Como parte de las propiedades de cada usuario se almacena también su clave pública de Secure Shell (SSH). Esto es necesario para la autenticación basada en claves, que es la que emplea este ejercicio de introducción. 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.

Además debe especificar el directorio principal 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 principal del bucket de Amazon S3.

> **Important**
>
> AWS Transfer Family impide que los nombres de usuario que tengan 1 o 2 caracteres se autentiquen 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 admiten claves públicas y privadas

- 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 principal, 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 gestionados 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`.

Temas

- Trabajar con usuarios de servicios administrados
- Uso del proveedor de identidad de AWS Directory Service
- Uso de proveedores de identidad personalizados

Trabajar con usuarios de servicios administrados

Puede añadir usuarios gestionados 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.

Para añadir un usuario gestionado por un 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 gestionados por el servicio Amazon S3
- Añadir usuarios gestionados por el servicio Amazon EFS
- Administración de usuarios administrados por servicios

Añadir usuarios gestionados por el servicio Amazon S3

> **Note**
>
> Si desea configurar un bucket de Amazon S3 multicuenta, siga los pasos que se mencionan en este artículo del Centro de conocimiento: ¿Cómo configuro mi servidor de AWS Transfer Family para que utilice un bucket de Amazon Simple Storage Service que está en otra cuenta de AWS? .

Añadir un usuario gestionado por el servicio Amazon S3 a su servidor

1. Abra la consola de AWS Transfer Family en https://console.aws.amazon.com/transfer/ y, 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. El nombre de usuario debe tener un mínimo de 3 y un máximo de 100 caracteres. El nombre de usuario puede contener los siguientes caracteres: a-z, A-Z, 0-9, guion bajo '_', guion '-', punto '.', y el signo arroba "@". El nombre de usuario no puede comenzar por un guion '-', un punto '.', ni una arroba "@".
5. En Acceso, seleccione el rol de IAM que ha creado anteriormente para proporcionar acceso al 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 servicio AWS Transfer Family 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 AWS Transfer Family y Amazon 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.
   - Generar automáticamente una 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 Generar automáticamente una política basada en la carpeta principal, no seleccione Restringido para este usuario.

   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.

7. En Directorio principal, seleccione el bucket de Amazon S3 donde almacenar los datos transferidos con 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 principal y restringirlo a ese directorio principal 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 política de generación automática basada en 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 etiquetas.
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 Servidores.

Próximos pasos: para el siguiente paso, continúe con Transferencia de archivos a través de un punto de conexión mediante un cliente.

Añadir usuarios gestionados 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.

Para añadir un usuario gestionado por el servicio Amazon EFS a su servidor

1. Abra la consola de AWS Transfer Family en https://console.aws.amazon.com/transfer/ y, 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. El nombre de usuario puede contener los siguientes caracteres: a-z, A-Z, 0-9, guion bajo '_', guion '-', punto '.', y el signo arroba "@". 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 identificador 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 de Amazon EFS con acceso al montaje y permisos de lectura/escritura. Por ejemplo, la combinación de las dos políticas administradas de AWS 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 principal, 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 principal como Restringido. Si se establece el directorio principal 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 principal en el que desea que estén los usuarios cuando inicien sesión con su cliente.

Si no especifica un directorio principal, 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 etiquetas.
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 Servidores.

Problemas que pueden surgir al usar SFTP por primera vez en su servidor 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 cwd
  ```

  En este caso, debe aumentar los permisos de política de la función de usuario. Puede añadir una política de AWS gestionada, como `AmazonElasticFileSystemClientFullAccess`.
- Si introduce pwd en el indicador `sftp` para ver el directorio personal del usuario, puede que vea el siguiente mensaje, donde *`USER-HOME-DIRECTORY`* es el directorio personal del usuario SFTP:

  ```
  remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
  ```

  En este caso, debería poder navegar hasta el directorio principal (`cd ..`) y crear el directorio principal 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
- Agregar clave pública SSH
- Eliminar la clave pública SSH

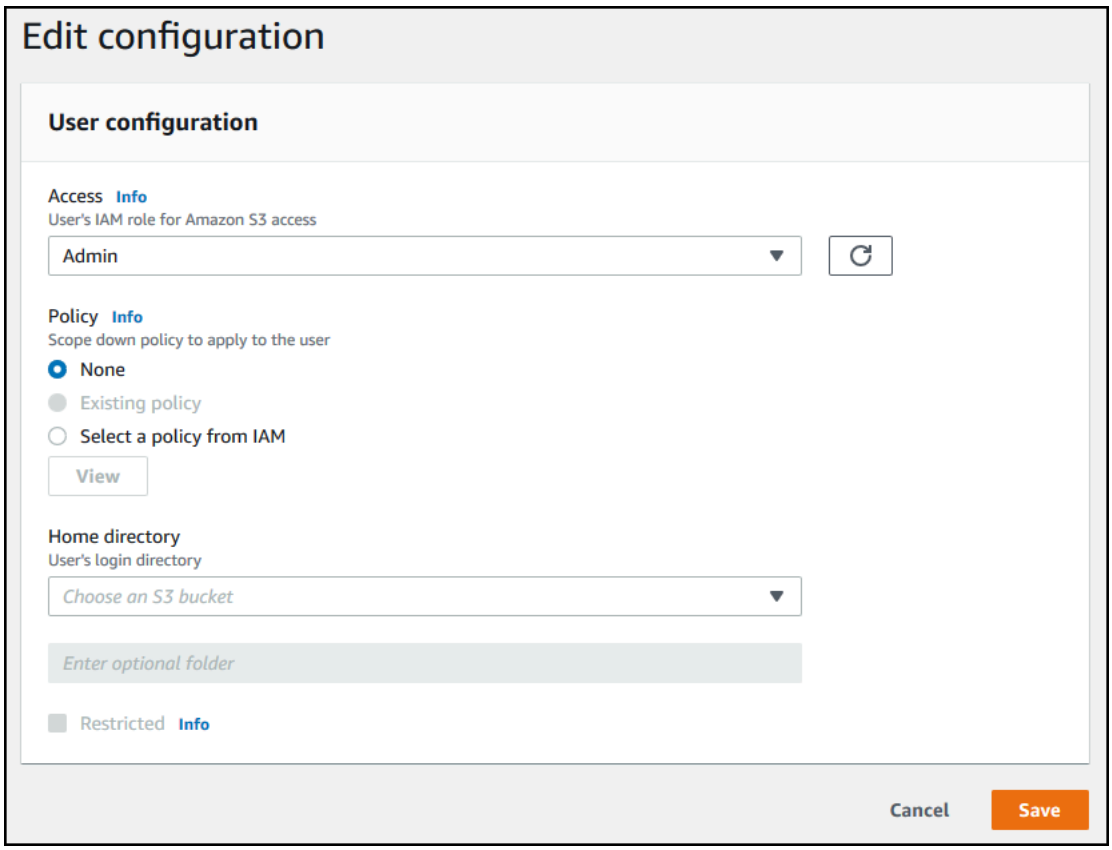
Encontrar una lista de sus usuarios

1. Abra la consola AWS Transfer Family 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 Configuración de servidor.
4. En Usuarios, consulte una lista de usuarios.

Ver o editar los detalles del usuario

1. Abra la consola AWS Transfer Family 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 Configuración de 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 servicio AWS Transfer Family 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 Directorio principal, seleccione el bucket de Amazon S3 donde almacenar los datos transferidos con 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 principal y restringirlo a ese directorio principal, 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.

Para eliminar un usuario

1. Abra la consola AWS Transfer Family 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 Configuración de 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, selecciona 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 y se quita de la lista de usuarios.

Para añadir una clave pública SSH para un usuario

1. Abra la consola AWS Transfer Family 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 Configuración de 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 de SSH para un usuario

1. Abra la consola AWS Transfer Family 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 Configuración de 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 del proveedor de identidad de AWS Directory Service

En este tema se describe cómo utilizar el proveedor de identidad de AWS Directory Service para AWS Transfer Family.

Temas

- Usando AWS Directory Service for Microsoft Active Directory
- Uso AWS de Directory Service para los servicios de dominio de Azure Active Directory

Usando AWS Directory Service for Microsoft Active Directory

Puede usarlo AWS Transfer Family para autenticar sus usuarios finales de transferencia de archivos mediante 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 AWS 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.

> **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 MFA basada en RADIUS 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 AWS 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. Añada el acceso desde uno o varios de sus AWS Directory Service grupos.
4. 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 tu proveedor de identidad
- Conceder acceso a los grupos
- Probando usuarios
- Eliminar el acceso al servidor de un grupo
- Conexión al servidor mediante SSH (Secure Shell)
- AWS Transfer Family Conectarse a un Active Directory autoadministrado mediante bosques y fideicomisos

Antes de empezar a usar AWS Directory Service for Microsoft Active Directory

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 in`SamAccountName`. Transfer Family no acepta el valor especificado en `userPrincipalName`.

Añada AWS Directory Service permisos a su función

También necesitas permisos de AWS Directory Service API para utilizarlos 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 AWS 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 detalles, consulte Probando usuarios. Si hay algún problema con el dominio del usuario o del grupo, recibirá el mensaje de error: No se ha encontrado ningún acceso asociado a los grupos de usuarios.

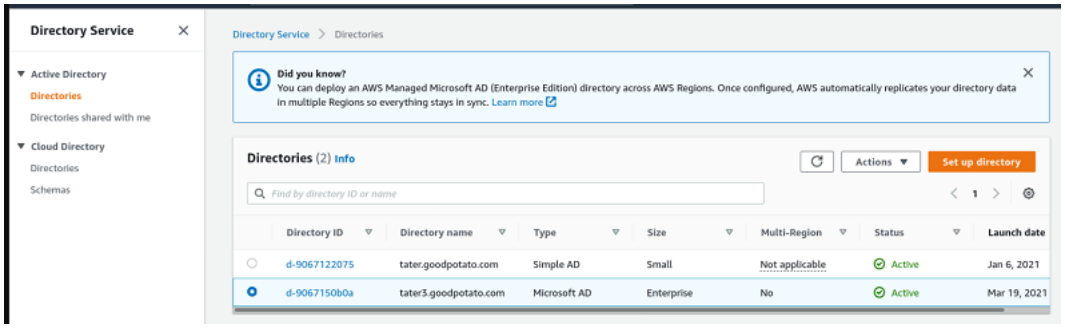
Elegir AWS Managed Microsoft AD como tu proveedor de identidad

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 la AWS Directory Service consola AWS Management Console y ábrela en https://console.aws.amazon.com/directoryservicev2/.

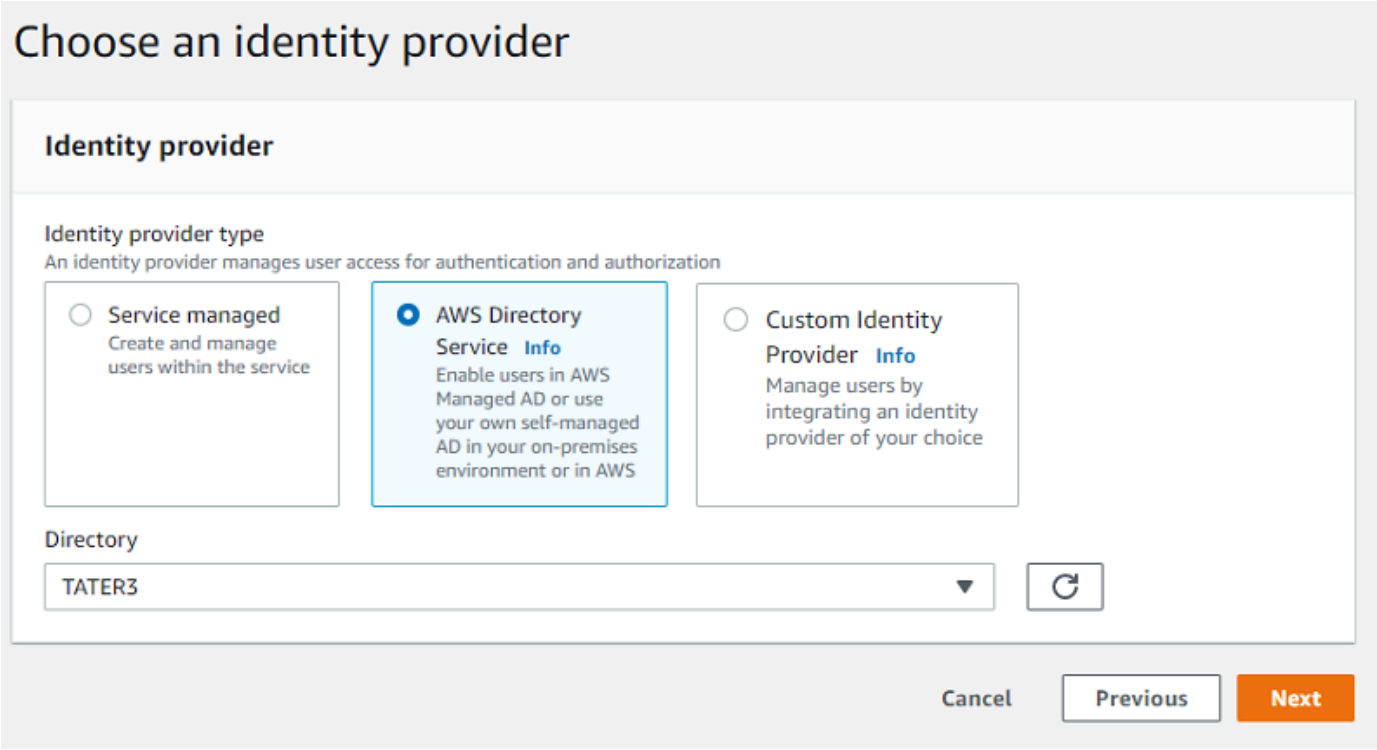
   Utilice la AWS Directory Service consola para configurar uno o más directorios gestionados. Para obtener más información, consulte AWS Managed Microsoft AD en la Guía para administradores de AWS Directory Service .



2. Abra la AWS Transfer Family consola en https://console.aws.amazon.com/transfer/ y elija Crear servidor.
3. 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 .

4. En Elegir un proveedor de identidad, elija Directory Service de AWS .



5. La lista Directorio contiene todos los directorios administrados que ha configurado. Elija un directorio de la lista y elija Siguiente.

> **Note**
>
> - No se admiten los directorios multicuenta y compartidos. AWS Managed Microsoft AD
> - Para configurar un servidor con Directory Service como proveedor de identidad, debe añadir algunos AWS Directory Service permisos. Para obtener más detalles, 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:

   - Cree un servidor compatible con SFTP
   - Cree un servidor compatible con FTPS
   - Cree un servidor compatible con FTP

   En esos procedimientos, continúe con el paso siguiente: elegir un proveedor de identidad.

> **Important**
>
> No puedes eliminar un directorio de Microsoft AD AWS Directory Service si lo usaste en un servidor Transfer Family. Primero debe eliminar el servidor y, a continuación, puede eliminar el directorio.

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**
>
> 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 AWS Transfer Family consola en 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 que acceda 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 de inicio, elija un bucket S3 que corresponda al directorio de inicio del grupo.

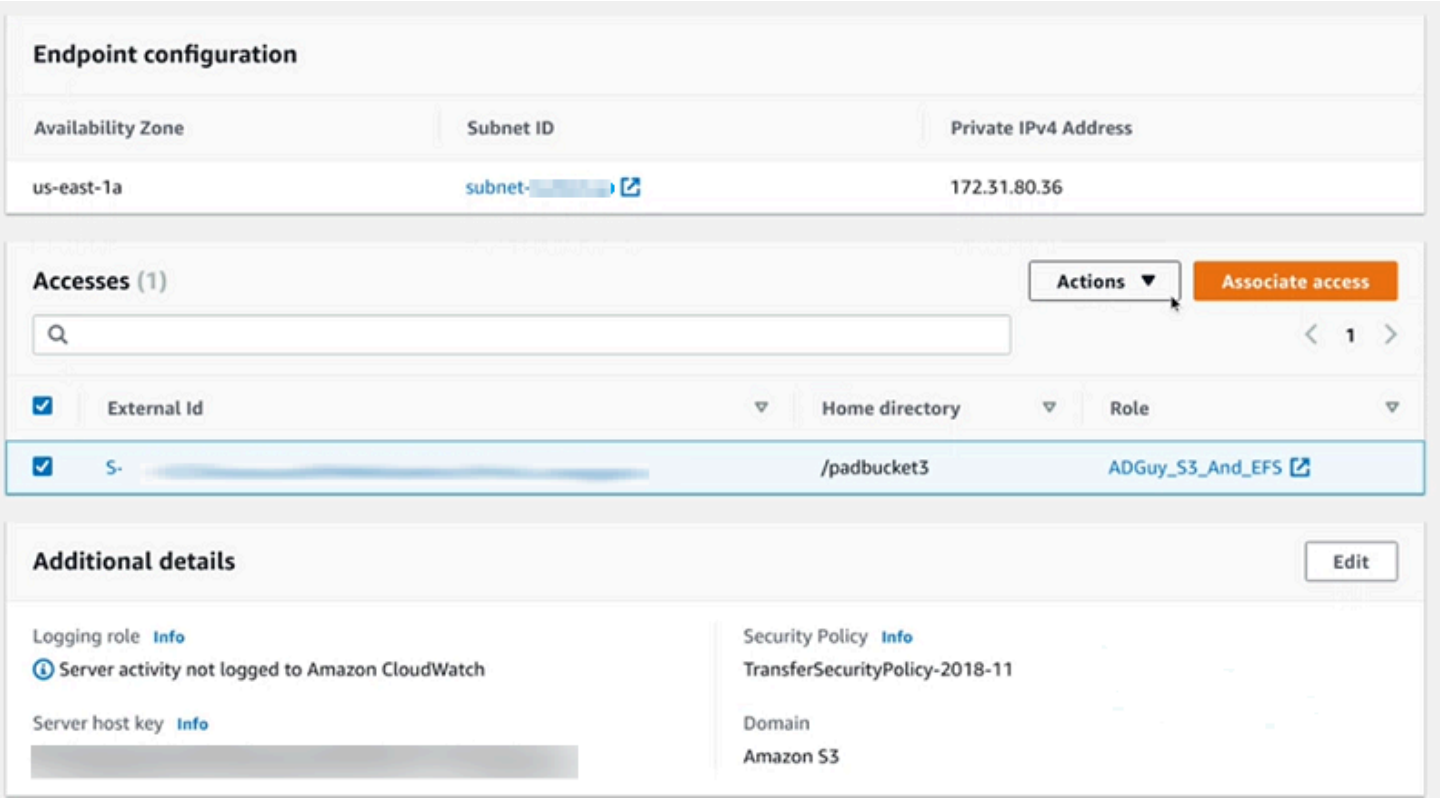
> **Note**
>
> Puede limitar las partes del bucket que ven los usuarios mediante la creación de una política de sesión. Por ejemplo, para limitar a los usuarios a su propia carpeta en el directorio de `/filetest`, introduzca el siguiente texto en el cuadro.
>
> ```
> /filetest/${transfer:UserName}
> ```
>
> 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.



Probando usuarios

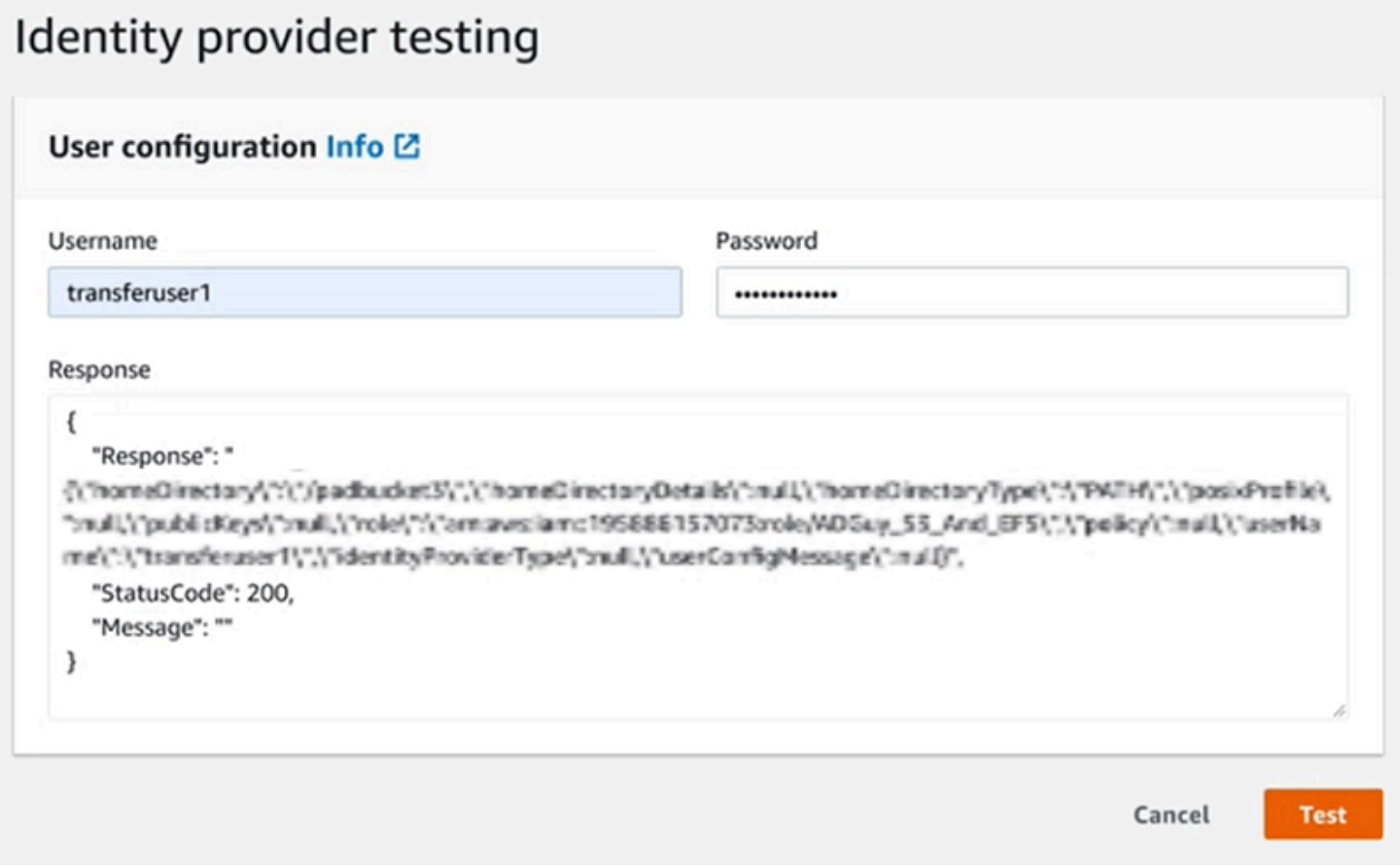
Puede comprobar si un usuario tiene acceso al AWS Managed Microsoft AD directorio de su servidor.

> **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.



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.

AWS Transfer Family Conectarse a un Active Directory autoadministrado mediante bosques y fideicomisos

Los usuarios de su Active Directory (AD) autogestionado también pueden utilizarlo AWS IAM Identity Center para el acceso mediante inicio de sesión único a los servidores Transfer Cuentas de AWS Family. Para ello, AWS Directory Service dispone de las siguientes opciones:

- La confianza unidireccional 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 una confianza bidireccional entre el Active Directory local AWS Managed Microsoft AD y el entorno 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 de Azure Active Directory

- 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 detalles, consulte Uso del proveedor de identidad de AWS Directory Service.

En este tema se describe cómo usar Conector Active Directory y Azure Active Directory Domain Services (Azure ADDS) para autenticar a los usuarios de SFTP Transfer con Azure Active Directory.

Temas

- Antes de empezar a usar AWS Directory Service para Azure Active Directory Domain Services
- Paso 1: agregar los servicios de dominio de Azure Active Directory
- 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 usar AWS Directory Service para Azure Active Directory Domain Services

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 site-to-site VPN con Microsoft Azure

Para Microsoft Azure, necesita lo siguiente:

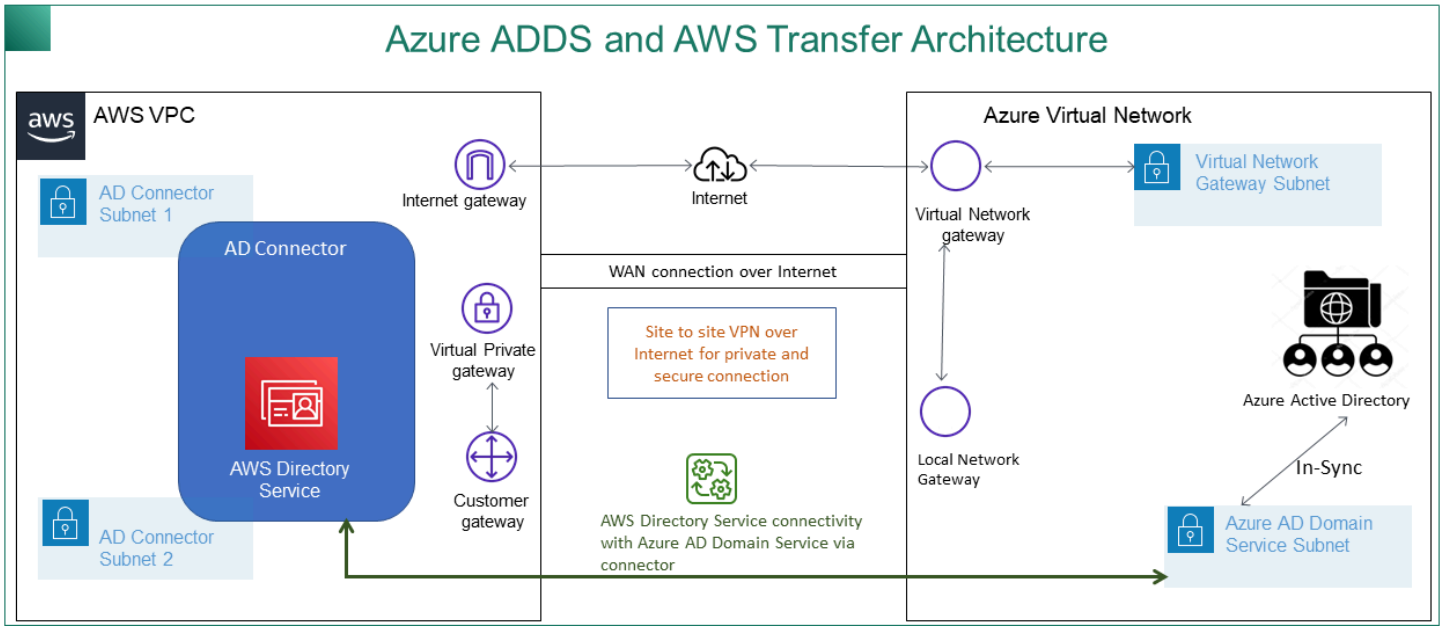
- Un servicio de dominio de Azure Active Directory y Active Directory (Azure ADDS)
- Un grupo de recursos de Azure

- Una red virtual de Azure
- Conectividad de VPN entre Amazon VPC y su grupo de recursos de Azure

> **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 virtual de Azure y una puerta de enlace de red local. Los túneles deben configurarse para permitir el tráfico entre los puntos de enlace de Azure ADDS y las subredes que alojan la AWS VPC.

- Una puerta de enlace para clientes y una puerta de enlace privada virtual para la conexión site-to-site VPN con Microsoft Azure

En el siguiente diagrama se muestra la configuración necesaria antes de comenzar.

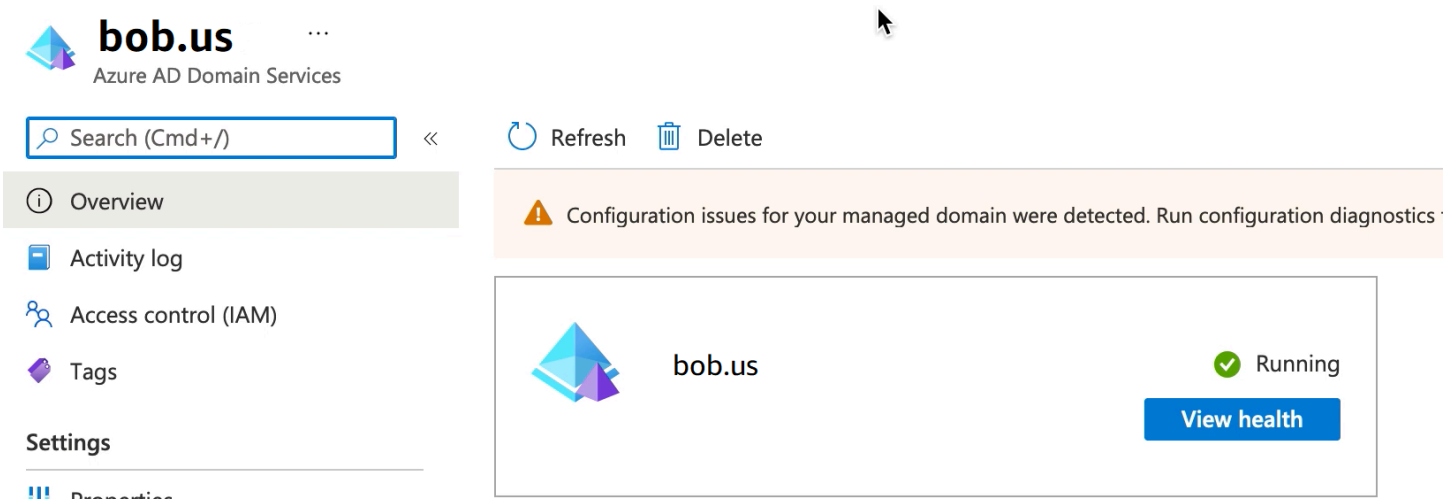


Paso 1: agregar los servicios de dominio de Azure Active Directory

De forma predeterminada, Azure AD no admite instancias que se unan a dominios. Para realizar acciones como unirse a un dominio y utilizar herramientas como la política de grupo, los administradores deben habilitar los servicios de dominio de Azure Active Directory. Si aún no ha agregado Azure AD DS o su implementación actual no está asociada al dominio que quiere que use su servidor de transferencia SFTP, debe agregar una nueva instancia.

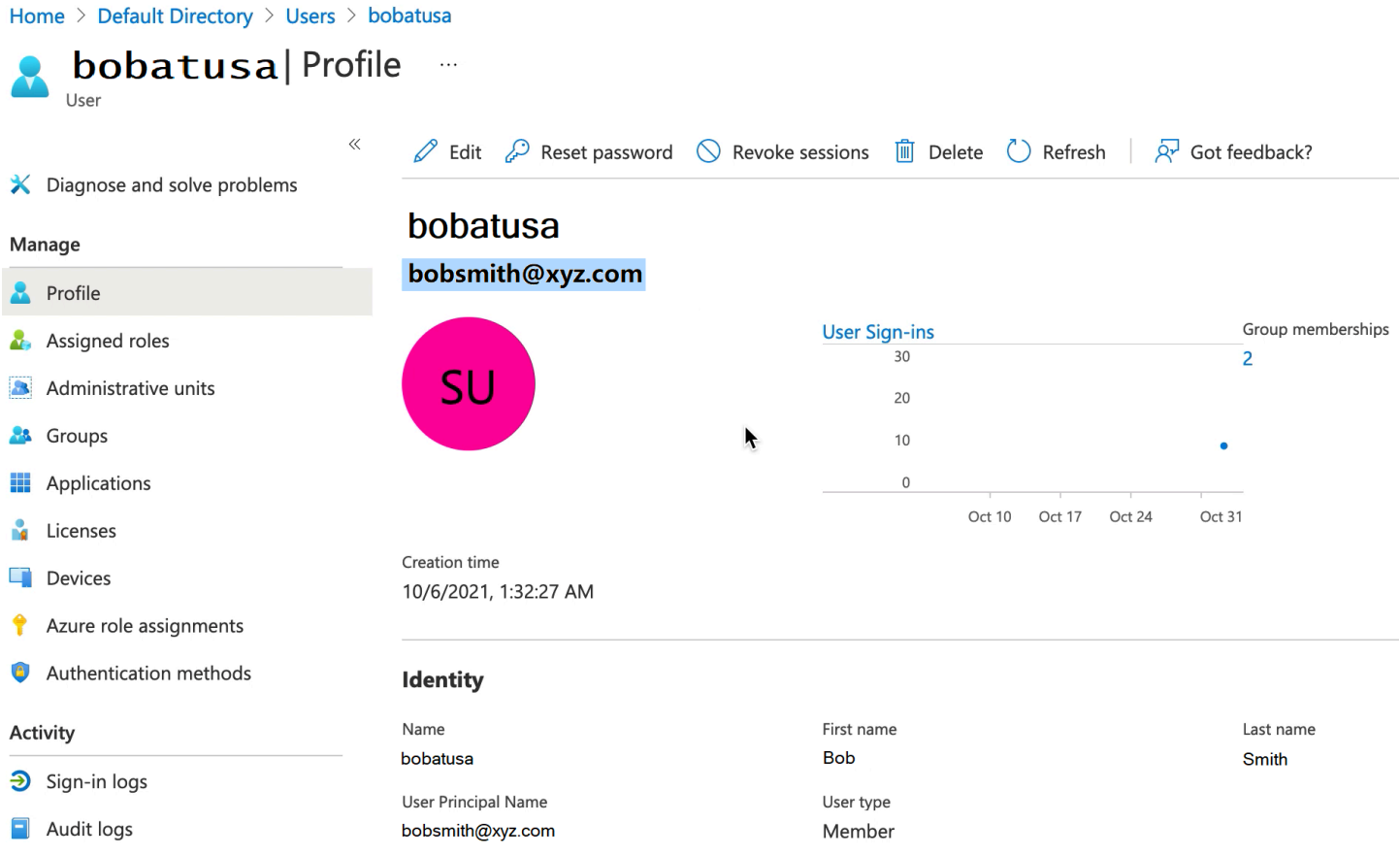
Para obtener información sobre cómo habilitar los Servicios de dominio de Azure Active Directory (Azure ADDS), consulte Tutorial: Creación y configuración de un dominio administrado de los Servicios de dominio de Azure Active Directory.

> **Note**
>
> Al habilitar Azure ADDS, asegúrese de que esté configurado para el grupo de recursos y el dominio de Azure AD al que va a conectar el servidor de transferencia SFTP.



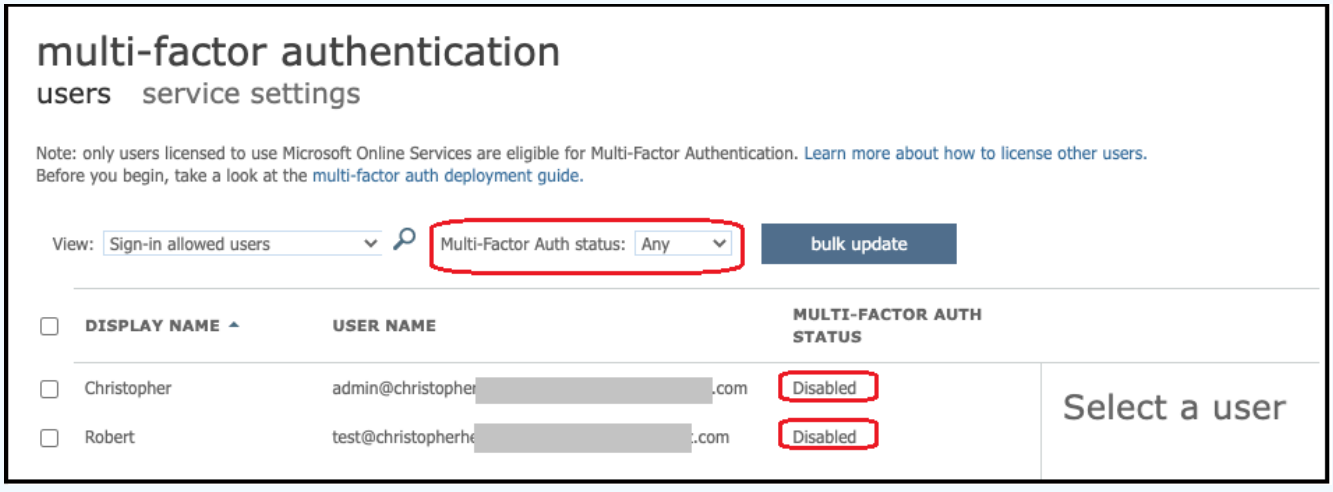
Paso 2: creación de una cuenta de servicio

Azure AD debe tener una cuenta de servicio que forme parte de un grupo de administradores en Azure ADDS. Esta cuenta se usa con el conector de AWS Active Directory. Asegúrese de que esta cuenta esté sincronizada con Azure ADDS.



Tip

La autenticación multifactor para Azure Active Directory no es compatible con los servidores de 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.



Paso 3: Configuración del AWS directorio mediante AD Connector

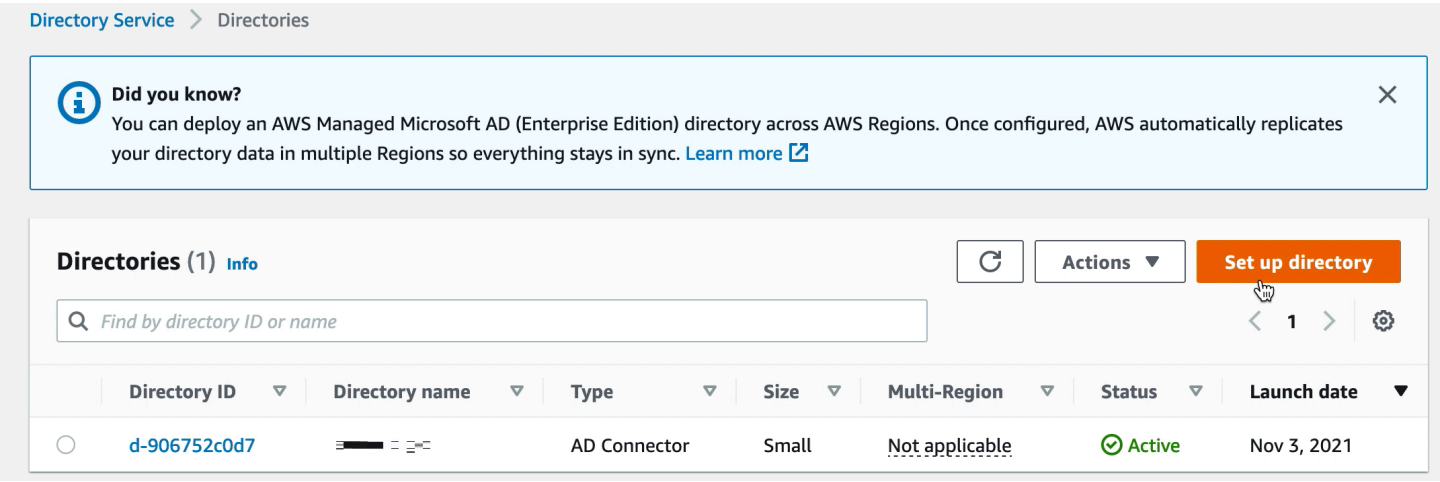
Tras configurar Azure ADDS y crear una cuenta de servicio con túneles VPN IPSEC entre la AWS VPC y la red virtual de Azure, puede probar la conectividad haciendo ping a la dirección IP DNS ADDS de Azure desde AWS cualquier instancia de EC2.

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: introduzca el nombre de dominio que está utilizando para su Azure ADDS.
   - Direcciones IP de DNS: introduzca sus direcciones IP de Azure ADDS.
   - 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.



Paso 4: Configurar el AWS Transfer Family servidor

Cree un servidor de 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: Configurar el AWS directorio 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

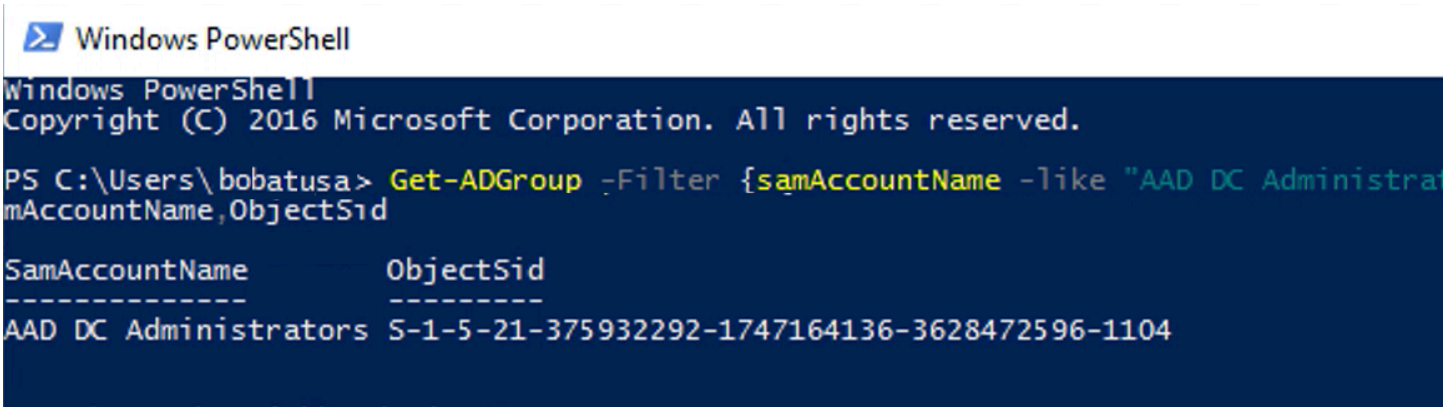
Tras crear el servidor, debe elegir qué grupos del directorio deben tener acceso para cargar y descargar archivos mediante los protocolos habilitados AWS Transfer Family. Para ello, debe crear un acceso.

> **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.

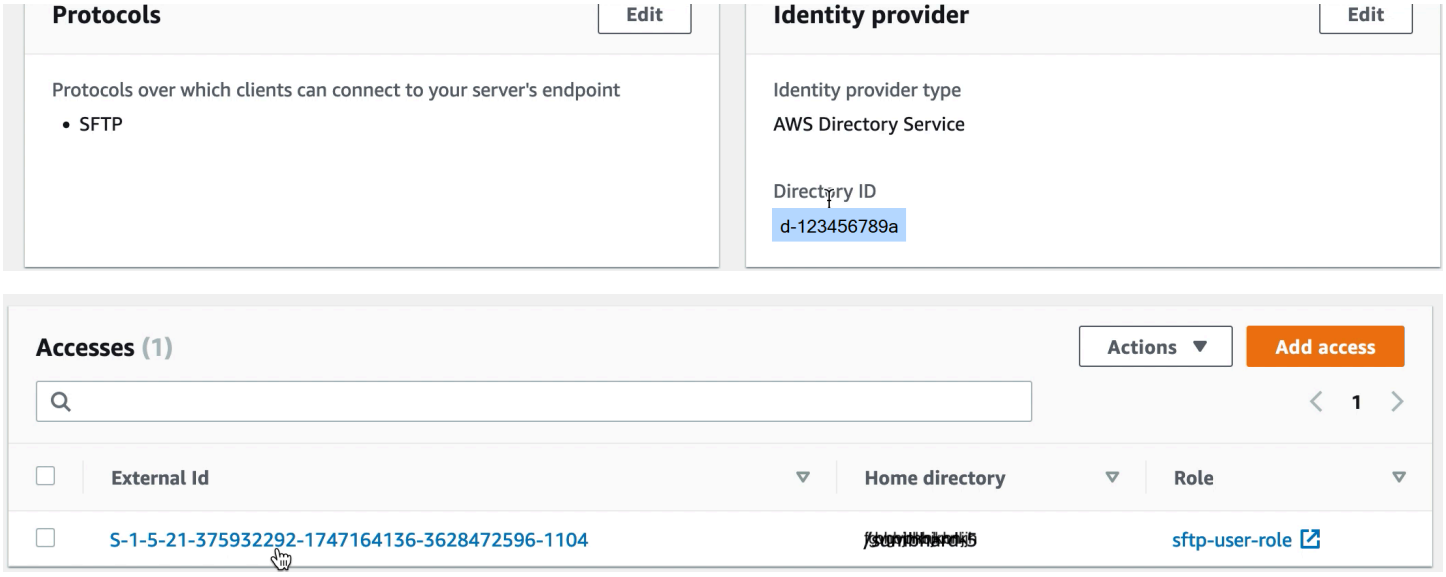
```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select
 SamAccountName,ObjectSid
```



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 de inicio, elija un bucket S3 que corresponda al directorio de inicio del grupo.
7. Seleccione Añadir para crear la asociación.

Los detalles de su servidor de transferencia deben ser similares a los siguientes:



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 proveedores de identidad personalizados

Para autenticar a sus usuarios, puede utilizar su proveedor de identidad actual con AWS Transfer Family. El proveedor de identidad se integra mediante una AWS Lambda función que autentica y autoriza a los usuarios a acceder a Amazon S3 o Amazon Elastic File System (Amazon EFS). Para obtener más detalles, consulte Se utiliza AWS Lambda para integrar su proveedor de identidad. También puede acceder a los CloudWatch gráficos para obtener métricas como la cantidad de archivos y bytes transferidos en la consola de AWS Transfer Family administración, lo que le brinda un panel único para monitorear las transferencias de archivos mediante un panel centralizado.

Como alternativa, 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 AWS WAF utilizarla para aprovechar sus capacidades para bloquear geográficamente o limitar la velocidad de las solicitudes. Para obtener más detalles, consulte Uso de Amazon API Gateway para integrar su proveedor de identidad.

En cualquier caso, puede crear un nuevo servidor mediante la consola de AWS Transfer Family o la operación de la API de CreateServer.

> **Note**
>
> 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 AWS Transfer Family puntos de enlace SFTP/FTPS administrados y Amazon Cognito y DynamoDB para la administración 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.

AWS Transfer Family proporciona las siguientes opciones para trabajar con proveedores de identidades personalizados.

- 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.

Para cualquiera de las opciones, también puede especificar cómo se va a autenticar.

- Contraseña o clave: los usuarios pueden autenticarse con su contraseña o su clave. Este es el valor predeterminado.
- 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.

Uso de varios métodos de autenticación para autenticarse con su proveedor de identidad personalizado

El servidor Transfer Family controla la lógica AND cuando se utilizan varios métodos de autenticación. Transfer Family trata esto como dos solicitudes independientes a tu proveedor de identidad personalizado; sin embargo, su efecto es combinado.

Ambas solicitudes deben devolverse correctamente con la respuesta correcta para permitir que se complete la autenticación. Transfer Family requiere que las dos respuestas estén completas, lo que significa que contienen todos los elementos necesarios (función, directorio principal, política y perfil POSIX si utiliza Amazon EFS para el almacenamiento). Transfer Family también exige que la respuesta de la contraseña no incluya claves públicas.

La solicitud de clave pública debe tener una respuesta independiente de la del proveedor de identidad. Ese comportamiento no cambia cuando se utiliza Contraseña O Clave o Contraseña Y Clave.

El protocolo SSH/SFTP desafía al cliente de software primero con una autenticación de clave pública y, a continuación, solicita una autenticación con contraseña. Esta operación exige que ambas se realicen correctamente antes de que el usuario pueda completar la autenticación.

Temas

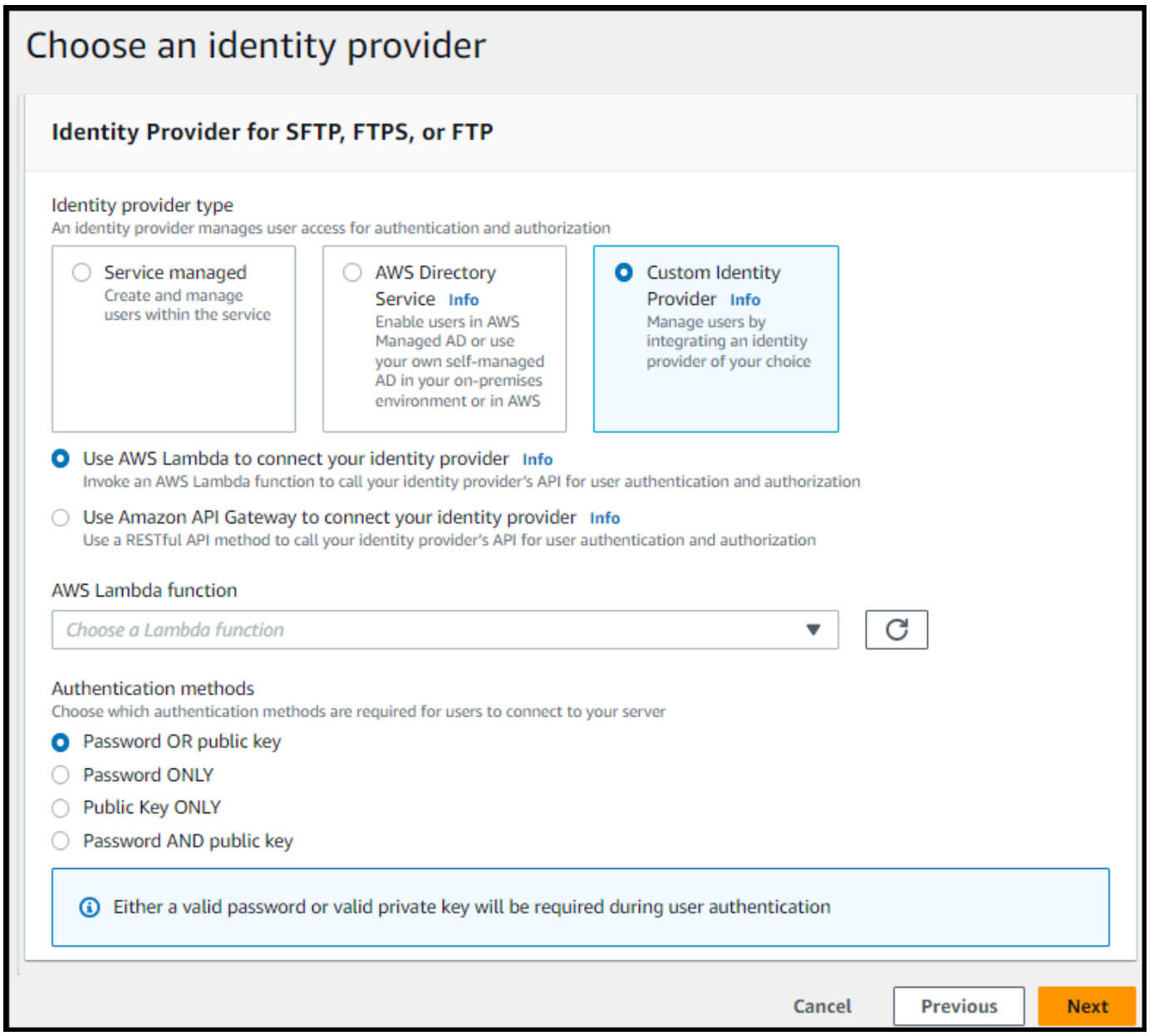
- Se utiliza AWS Lambda para integrar su proveedor de identidad
- Uso de Amazon API Gateway para integrar su proveedor de identidad

Se utiliza AWS Lambda para integrar su proveedor de identidad

Cree una AWS Lambda función que se conecte a su proveedor de identidad 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

> **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 losPlantillas 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.



> **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:transfer:region:account-id:function:my-lambda-auth-
function",
      "Condition": {
        "ArnLike": {
          "AWS:SourceArn": "arn:aws:transfer:region:account-id:server/server-id"
        }
      }
    }
  ]
}"
```

> **Note**
>
> En el ejemplo anterior, reemplace cada *marcador de posición del usuario* con 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 acerca de Lambda, consulte la Guía para desarrolladores de AWS Lambda o Crear funciones de Lambda con Node.js.

Temas

- Plantillas de función de Lambda
- Valores de Lambda válidos
- Ejemplo de función de Lambda
- Prueba de su configuración

Plantillas de función de Lambda

Puede implementar una AWS 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 AWS Transfer Family servidor compatible con FIPS AWS CloudFormation especificando una política de seguridad con FIPS en la plantilla. Las políticas de seguridad disponibles se describen en Políticas de seguridad para servidores AWS Transfer Family

Para crear una pila para utilizarla en la autenticación AWS CloudFormation

1. Abra la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
2. Siga las instrucciones para implementar una AWS 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

  Una 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.
- Plantilla apilada Okta-MFA: plantilla básica que se utiliza AWS Lambda con un AWS Transfer Family servidor para integrar Okta, con MultiFactor Authentication, como proveedor de identidad personalizado.
- Plantilla de Azure Active Directory: los detalles de esta pila se describen en la entrada del blog Cómo 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.

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	Descripción	Obligatorio
`Role`	Especifica el nombre de recurso de Amazon (ARN)	Obligatoria

Valor	Descripción	Obligatorio
	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 solicitud es de transferencia de los usuarios. Para obtener más informaci ón sobre cómo establecer una relación de confianza, consulte Para establecer una relación de confianza.	

Valor	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
`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.	Opcional

Valor	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	Descripción	Obligatorio
`HomeDirectory`	Directorio de destino de un usuario cuando inicia sesión en el servidor a través del cliente.	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.

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: '/fs-faa1a123' // Not required, defaults to '/'
    };

    // 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': '/fs-fs-faa1a123',
      '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 AWS 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 AWS 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 AWS 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 AWS 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": ""
}
```


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.

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 detalles, 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 de conexión HTTPS para que todas las llamadas a la 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 detalles, consulte Agregue un cortafuegos de aplicaciones web.

Uso del método API Gateway para la autenticación personalizada con Transfer Family

1. Crea una AWS CloudFormation pila. Para ello:

   > **Note**
   >
   > Las plantillas de pila se han actualizado para utilizar contraseñas codificadas en Base64: para obtener más información, consulte. Mejoras en las plantillas AWS CloudFormation

   a. Abra la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
   b. Siga las instrucciones para implementar una AWS CloudFormation pila a partir de una plantilla existente en Seleccionar una plantilla de pila en la Guía del AWS CloudFormation usuario.
   c. Usa una de las siguientes plantillas básicas para crear un método API Gateway AWS Lambda respaldado por API 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.

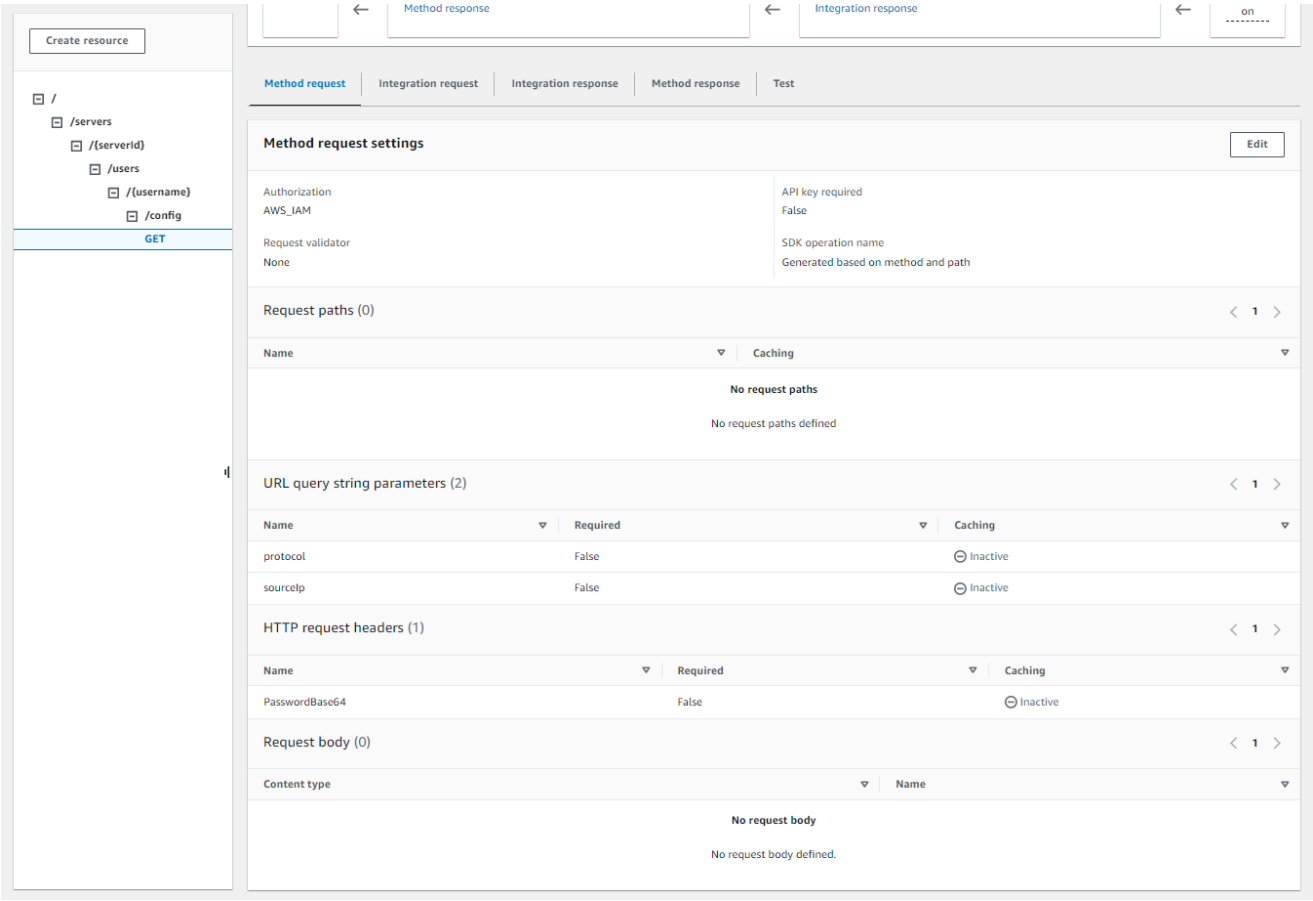
> **Note**
>
> Si utiliza la opción de proveedor de identidad personalizado para habilitar la autenticación basada en contraseñas para sus usuarios y habilita el registro de solicitudes y respuestas que proporciona API Gateway, API Gateway registra las contraseñas de sus usuarios en sus Amazon Logs. 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 AWS 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.

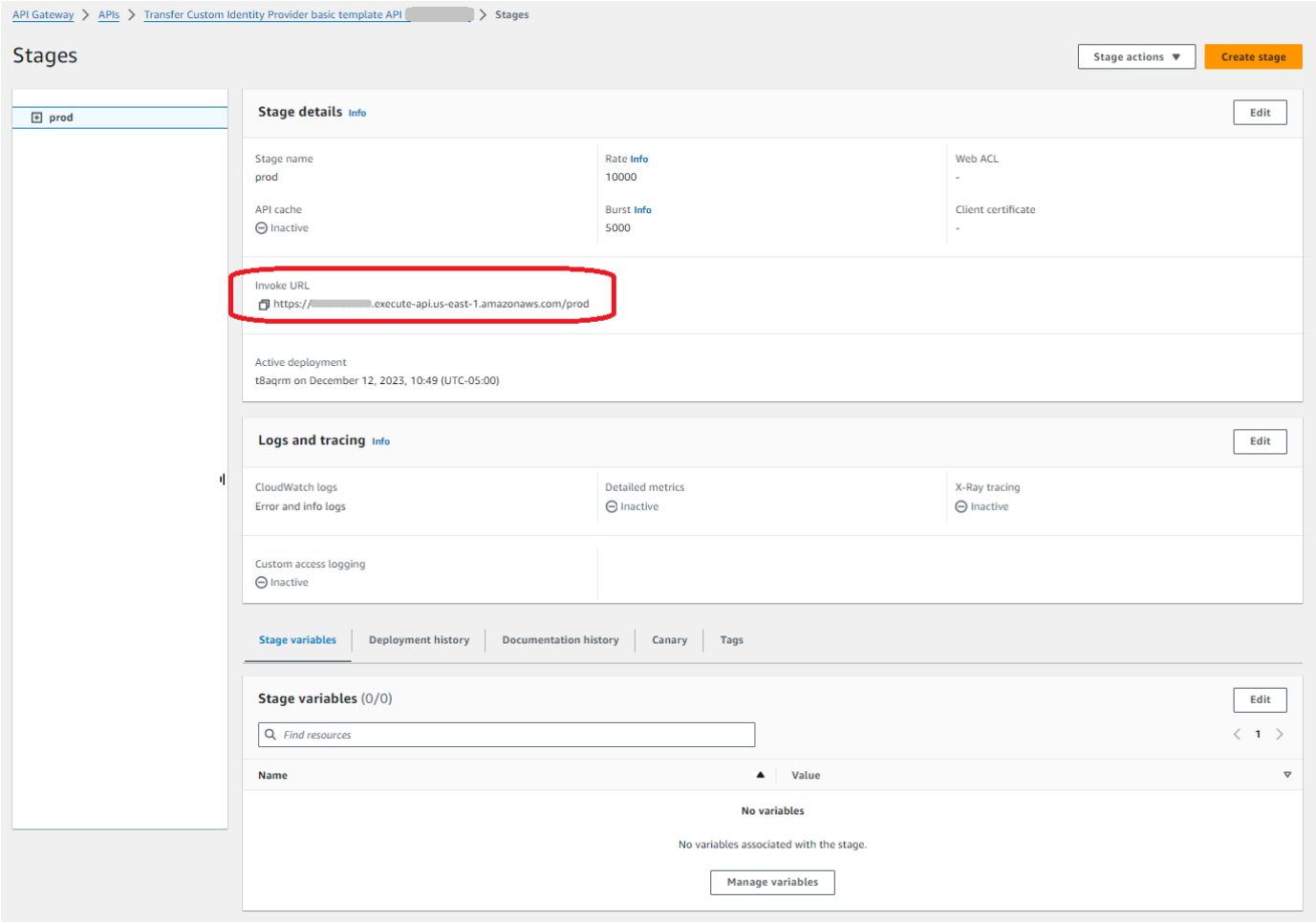


En este punto, su API Gateway está lista para ser implementada.

3. Para Acciones, elija Implementar API. Para la Etapa de implementación, elija prod y, a continuación, elija Implementar.

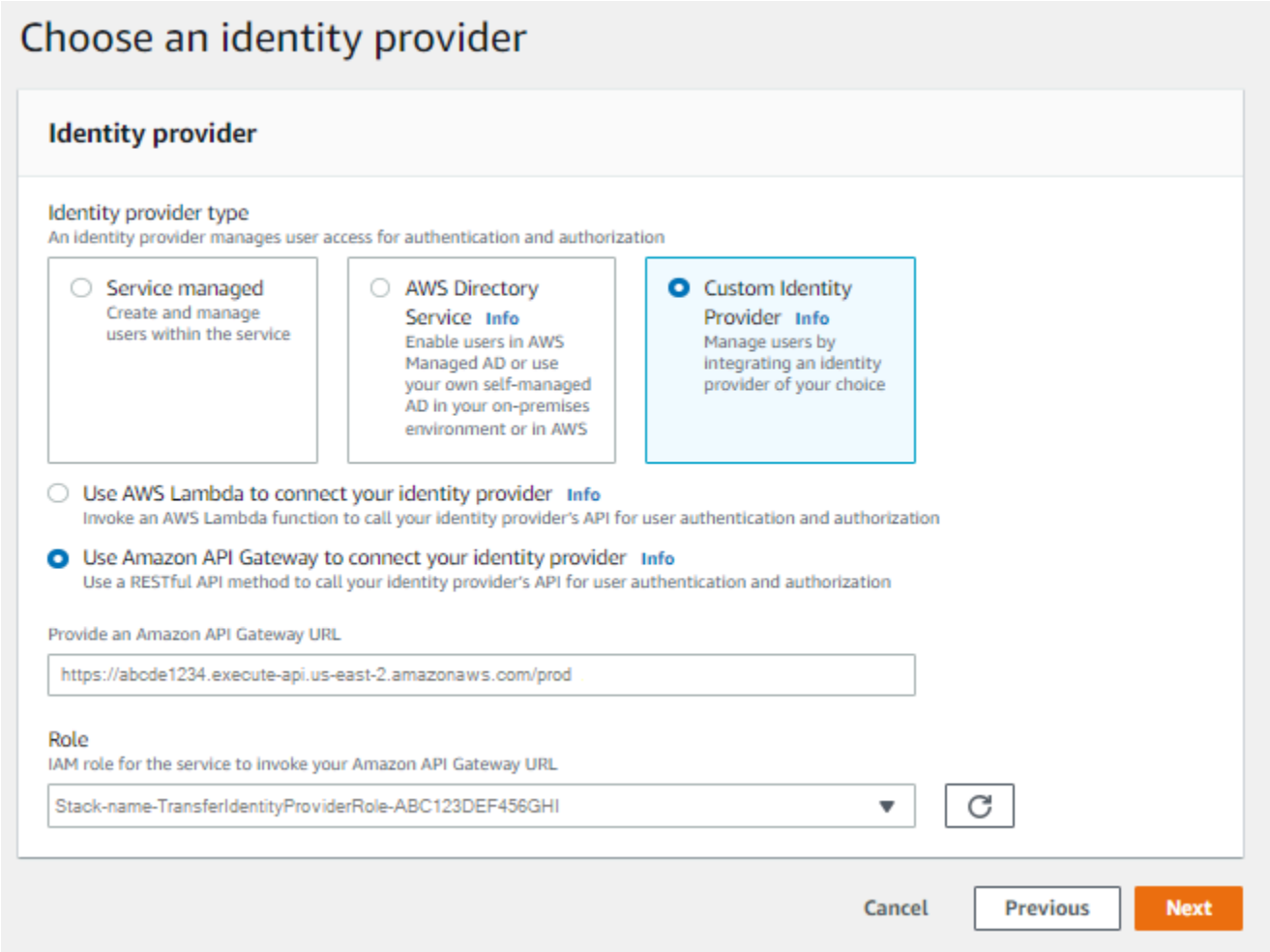
   Una vez que el método API Gateway se haya implementado correctamente, consulta su rendimiento en Stages > Stage details, como se muestra en la siguiente captura de pantalla.

> **Note**
>
> Copie la dirección URL de invocación que aparece en la parte superior de la pantalla. Puede que lo necesites para el siguiente paso.



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.



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.

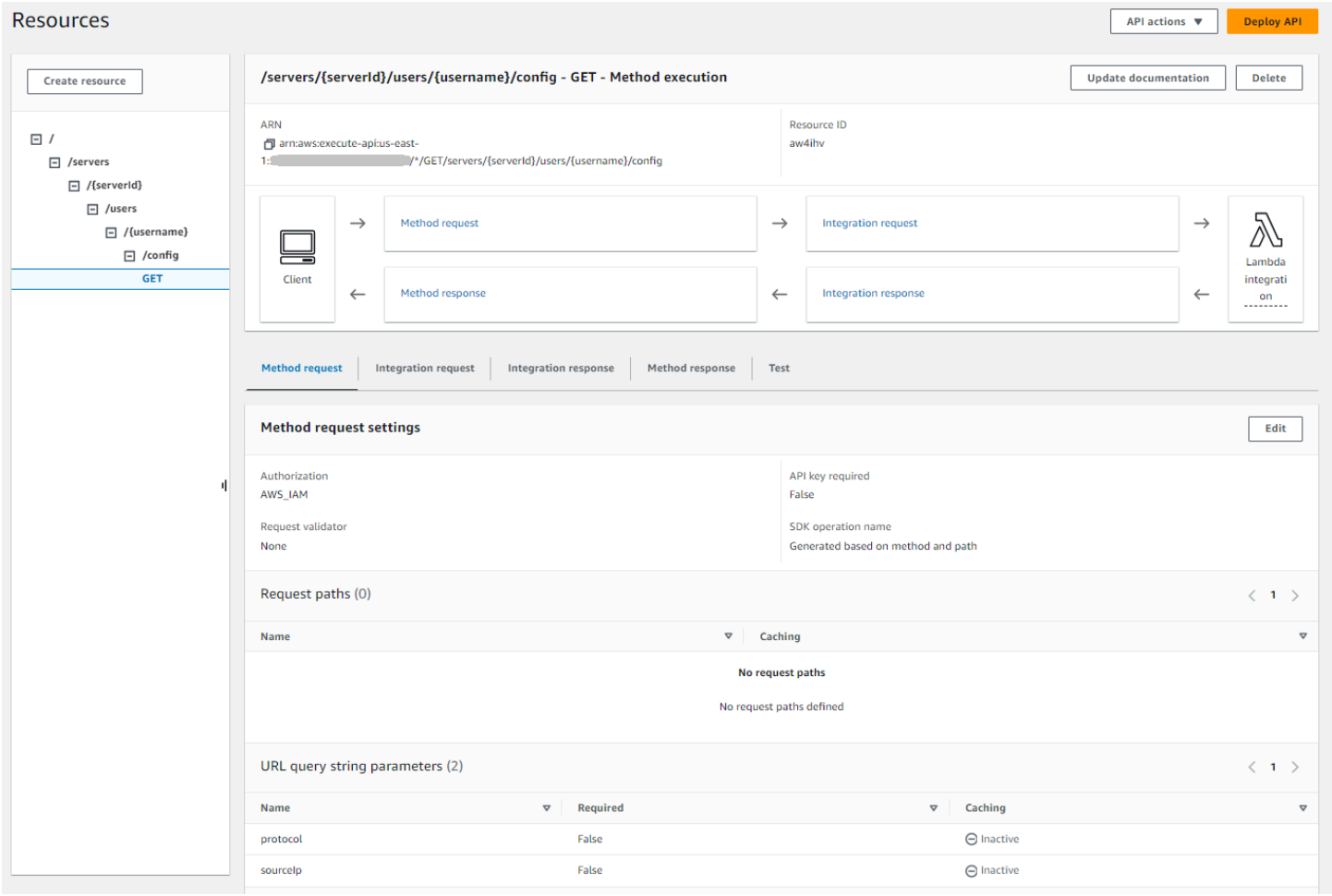
c. En Función, elige la función de IAM que creó la AWS CloudFormation plantilla. Este rol permite a Transfer Family invocar su método de puerta de enlace de API.

   El rol de invocación contiene el nombre de la AWS 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.



> **Note**
>
> El nombre de usuario debe tener un mínimo de 3 y un máximo de 100 caracteres. El nombre de usuario puede contener los siguientes caracteres: a-z, A-Z, 0-9, guion bajo (_) y guion (-), punto (.), y el signo de arroba (@). Sin embargo, el nombre de usuario no puede comenzar por un guion (-), un punto (.), ni una arroba (@).

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": "/bucketName/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:::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\":\"/MY-HOME-BUCKET\"}]",
   "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 las siguientes funciones de Lambda de ejemplo en Node.js. Para obtener más información acerca de Lambda, consulte la Guía para desarrolladores de AWS Lambda o Crear funciones de 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 campo `HomeDirectoryDetails` que proporciona las asignaciones de entrada/destino deseadas, similares a los valores descritos en el parámetro HomeDirectoryDetails para los usuarios administrados 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 AWS 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 AWS CloudFormation plantilla de ejemplo que utilice esta función Lambda, vaya al bucket de Amazon S3 proporcionado por. AWS Transfer Family

Mejoras en las plantillas AWS CloudFormation

Se han realizado mejoras en la interfaz de API Gateway en las CloudFormation plantillas publicadas. Las plantillas ahora utilizan contraseñas codificadas en Base64 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 básico de caracteres US-ASCII.

Los cambios en la plantilla que permiten 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 AWS 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.

4. Busque lo siguiente:

   - Busca `RequestTemplates` y asegúrate de tener esta línea:

     ```
     "password":
      "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(
     \'","'")",
     ```

   - Busca `RequestParameters` y asegúrate de tener esta línea:

     ```
     method.request.header.PasswordBase64: false
     ```

Si no ves las líneas actualizadas, edita tu pila. Para obtener más información sobre cómo actualizar la AWS CloudFormation pila, consulta Modificación de una plantilla de pila en la AWS CloudFormation Guía del usuario.

Uso de directorios lógicos para simplificar las estructuras de directorios de Transfer Family

Para simplificar la estructura de directorios AWS Transfer Family del servidor, puede utilizar directorios lógicos. Con los directorios lógicos, puede crear una estructura de directorio virtual que utilice nombres fáciles de utilizar para los usuarios cuando se conecten al bucket de Amazon S3 o al sistema de archivos de Amazon EFS. Al utilizar directorios lógicos, puede evitar revelar a sus usuarios finales las rutas de directorio absolutas, los nombres de los buckets de Amazon S3 y los nombres de los sistemas de archivos EFS.

> **Note**
>
> Debe usar políticas de sesión para que los usuarios finales solo puedan realizar las operaciones que usted les permita realizar.
> Debe utilizar 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.

Puede utilizar los directorios lógicos para establecer el directorio raíz del usuario en la ubicación que desee dentro de la jerarquía de almacenamiento mediante la realización de lo que se conoce como operación chroot. En este modo, los usuarios no pueden navegar a un directorio fuera del directorio de inicio o raíz que haya configurado para ellos.

Por ejemplo, aunque a un usuario de Amazon S3 se le ha limitado el acceso únicamente a `/mybucket/home/${transfer:UserName}`, algunos clientes permiten a los usuarios recorrer una carpeta hasta `/mybucket/home`. En esta situación, el usuario vuelve a acceder al directorio de inicio deseado solo después de cerrar sesión y volver a iniciar sesión en el servidor de Transfer Family. Realizar una operación chroot puede evitar que se produzca esta situación.

Puede crear su propia estructura de directorio en buckets y prefijos. Esta característica resulta útil si tiene un flujo de trabajo que espera una estructura de directorios específica que no pueda replicar mediante prefijos de bucket. 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.

Asignaciones lógicas de archivos de directorios

El tipo `HomeDirectoryMapEntry` de datos ahora incluye un `Type` parámetro. Antes de que existiera este parámetro, podría haber creado una asignación de directorios lógica en la que el destino fuera un archivo. Si ha creado anteriormente alguno de estos tipos de asignaciones de directorios lógicas, debe definirlo de forma explícita o estas asignaciones no funcionarán correctamente en el futuro. `Type FILE`
Una forma de hacerlo consiste en llamar a la `UpdateUser` API y establecer la t `Type FILE` para la asignación existente.

Reglas para el uso de directorios lógicos

Antes de crear las asignaciones de directorio lógico, debe comprender las siguientes reglas:

- Si `Entry` es `"/"`, solo puede tener una asignación, ya que no se permite la superposición de rutas.
- Los directorios lógicos admiten mapeos de hasta 2,1 MB (para los usuarios gestionados por el servicio, este límite es de 2000 entradas). Es decir, la estructura de datos que contiene las asignaciones tiene un tamaño máximo de 2,1 MB. Si tiene muchos mapeos, puede calcular el tamaño de los mapeos de la siguiente manera:

  1. Escribe un mapeo típico en el formato`{"Entry":"/`*`entry-path`*`","Target":"/`*`target-path`*`"}`, donde *`entry-path`* y *`target-path`* son 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.
- Los destinos pueden usar la variable `${transfer:UserName}` si la ruta del bucket o del sistema de archivos se ha parametrizado en función del nombre de usuario.
- Los destinos pueden ser rutas en distintos depósitos o sistemas de archivos, pero debe asegurarse de que la función asignada AWS Identity and Access Management (IAM) (el `Role` parámetro de la respuesta) proporcione acceso a esos depósitos o sistemas de archivos.
- No especifiques el `HomeDirectory` parámetro, ya que este valor viene implícito en los `Entry` `Target` pares cuando usas el `LOGICAL` valor del parámetro. `HomeDirectoryType`
- Los objetivos deben empezar con un carácter de barra diagonal (`/`), pero no deben utilizarse barras diagonales finales (`/`) al especificar el. `Target` Por ejemplo, `/DOC-EXAMPLE-BUCKET/images` es aceptable, pero no `DOC-EXAMPLE-BUCKET/images` lo es. `/DOC-EXAMPLE-BUCKET/images/`
- Amazon S3 es un almacén de objetos, lo que significa que las carpetas son un concepto virtual y no existe una jerarquía de directorios real. Si su aplicación ejecuta una `stat` operación desde un cliente, todo se clasifica como un archivo cuando utiliza Amazon S3 como almacenamiento. 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. Si su aplicación requiere que se muestre `stat` con precisión si algo es un archivo o una carpeta, puede utilizar Amazon Elastic File System (Amazon EFS) como opción de almacenamiento para los servidores 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`.

> **Important**
>
> A menos que elija optimizar el rendimiento de sus directorios de Amazon S3 (al crear o actualizar un servidor), el directorio raíz debe existir al inicio. En el caso de Amazon S3, esto significa que ya debe haber creado un objeto de cero bytes que termine con una barra diagonal (`/`) para crear la carpeta raíz. Evitar este problema es una razón para considerar la optimización del rendimiento de Amazon S3.

Implementar directorios lógicos y **`chroot`**

Para utilizar las características chroot y los directorios lógicos, debe hacer lo siguiente:

Active los directorios lógicos para cada usuario. Para ello, defina el parámetro `HomeDirectoryType` a `LOGICAL` cuando cree o actualice el usuario.

```
"HomeDirectoryType": "LOGICAL"
```

`chroot`

Para chroot, cree una estructura de directorios que consista en un único `Entry` y un par `Target` para cada usuario. La carpeta raíz es el punto `Entry` y `Target` es la ubicación del bucket o sistema de archivos a la que se realiza la asignación.

Example for Amazon S3

```
[{"Entry": "/", "Target": "/mybucket/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":
"/mybucket/${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`/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 una razón 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": "/bucket1/pics"},
{"Entry": "/doc", "Target": "/bucket1/anotherpath/docs"},
{"Entry": "/reporting", "Target": "/reportingbucket/Q1"},
{"Entry": "/anotherpath/subpath/financials", "Target": "/reportingbucket/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": "/mybucket/pics"
},
{
   "Entry": "/doc",
   "Target": "/mybucket/mydocs"
},
{
   "Entry": "/temp",
   "Target": "/mybucket"
}
```

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

Ejemplo 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-logical --server-id s-11112222333344445
 --role arn:aws:iam::1234abcd5678:role/marymajor-role --home-directory-type LOGICAL \
 --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/DOC-EXAMPLE-BUCKET1/
pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/DOC-EXAMPLE-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-logical \
 --server-id s-11112222333344445 --role arn:aws:iam::1234abcd5678:role/marymajor-role \
 --home-directory-type LOGICAL --home-directory-mappings "[{\"Entry\":\"/pics\",
 \"Target\":\"/DOC-EXAMPLE-BUCKET1/pics\"}, \
 {\"Entry\":\"/doc\", \"Target\":\"/DOC-EXAMPLE-BUCKET2/test/mydocs\"}]"
```

Tenga en cuenta lo siguiente:

- Si los directorios `/DOC-EXAMPLE-BUCKET1/pics` y `/DOC-EXAMPLE-BUCKET2/test/mydocs` aún no existen, el usuario (o un administrador) debe crearlos.
- Cuando **`marymajor`** se conecta al servidor y ejecuta el comando `ls -l`, 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.
- Los archivos que añade a `pics` y `doc` se añaden a las rutas de Amazon S3 `/DOC-EXAMPLE-BUCKET1/pics` y `/DOC-EXAMPLE-BUCKET2/test/mydocs`, 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.

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\": \"/DOC-EXAMPLE-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\\\":\\\"/DOC-EXAMPLE-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.

AWS Transfer Family Conectores SFTP

AWS Transfer Family Los conectores SFTP establecen una relación para el envío de archivos y mensajes entre el almacenamiento de Amazon y un socio externo mediante el protocolo SFTP. 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.

> **Note**
>
> Actualmente, los conectores SFTP solo se pueden usar para conectarse a servidores SFTP remotos que ofrecen un punto de conexión accesible a Internet.

Las siguientes entradas del blog proporcionan una arquitectura de referencia para crear un flujo de trabajo de MFT mediante 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

Consulte los conectores SFTP de AWS Transfer Family para ver una breve introducción a los conectores SFTP Transfer Family.

Temas

- Configure los conectores SFTP
- Enviar y recuperar archivos mediante un conector SFTP
- Listar el contenido de un directorio remoto
- Administrar conectores SFTP

Configure los conectores SFTP

En este tema se describe cómo crear conectores SFTP, los algoritmos de seguridad asociados a ellos, cómo almacenar un secreto para guardar las credenciales, detalles sobre el formato de la clave privada e instrucciones para probar los conectores.

Temas

- Creación de un Conector SFTP
- Guarde un secreto para usarlo con un conector SFTP
- Genere y formatee la clave privada del conector SFTP
- Prueba de un conector SFTP

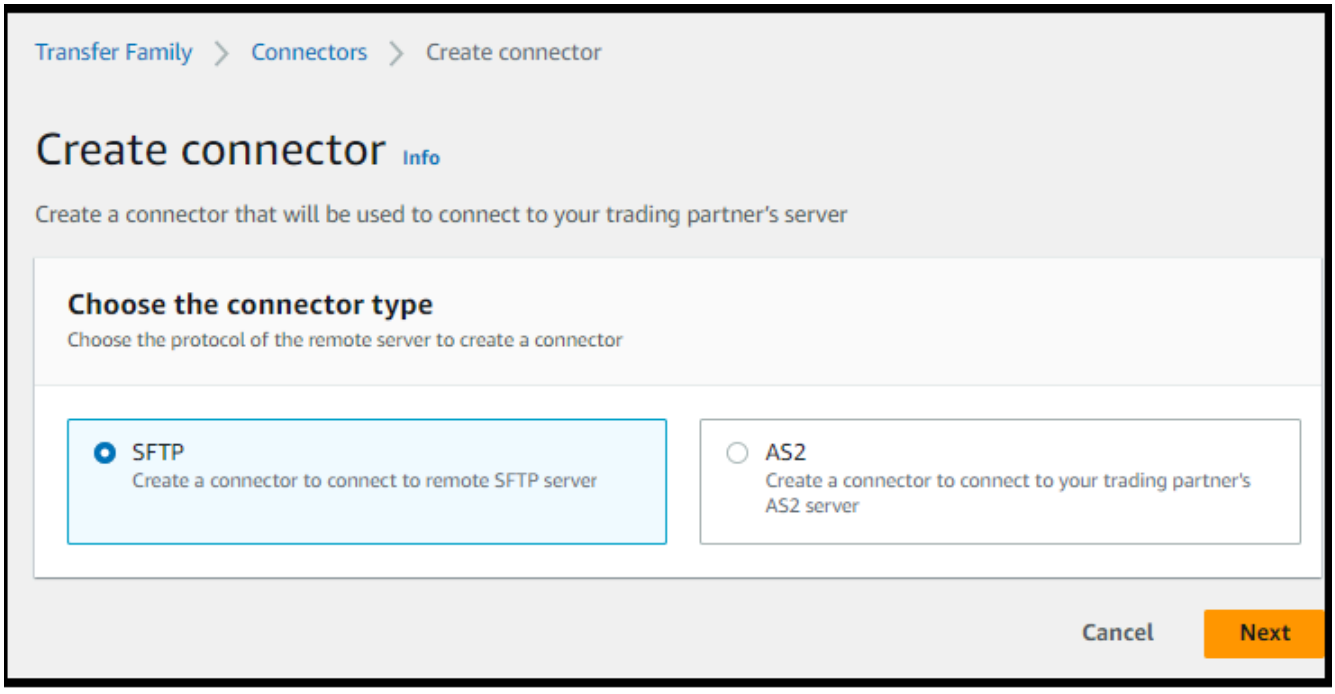
Creación de un Conector SFTP

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 y, a continuación, seleccione Crear conector.
3. Elija SFTP como tipo de conector para crear un conector SFTP y, a continuación, elija Siguiente.



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

- 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.

  El siguiente ejemplo concede los permisos necesarios para acceder al *DOC-EXAMPLE-BUCKET en Amazon* S3 y al secreto especificado almacenado en Secrets Manager.

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

```
    {
        "Sid": "AllowListingOfUserFolder",
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:region:account-id: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, consulte Permisos a los AWS Secrets Manager secretos para los usuarios de otra cuenta.

- (Opcional) Para la función de registro, elige la función de IAM para que el conector la utilice para enviar eventos a tus CloudWatch registros. En el siguiente ejemplo de política, se enumeran los permisos necesarios para registrar eventos en los conectores SFTP.

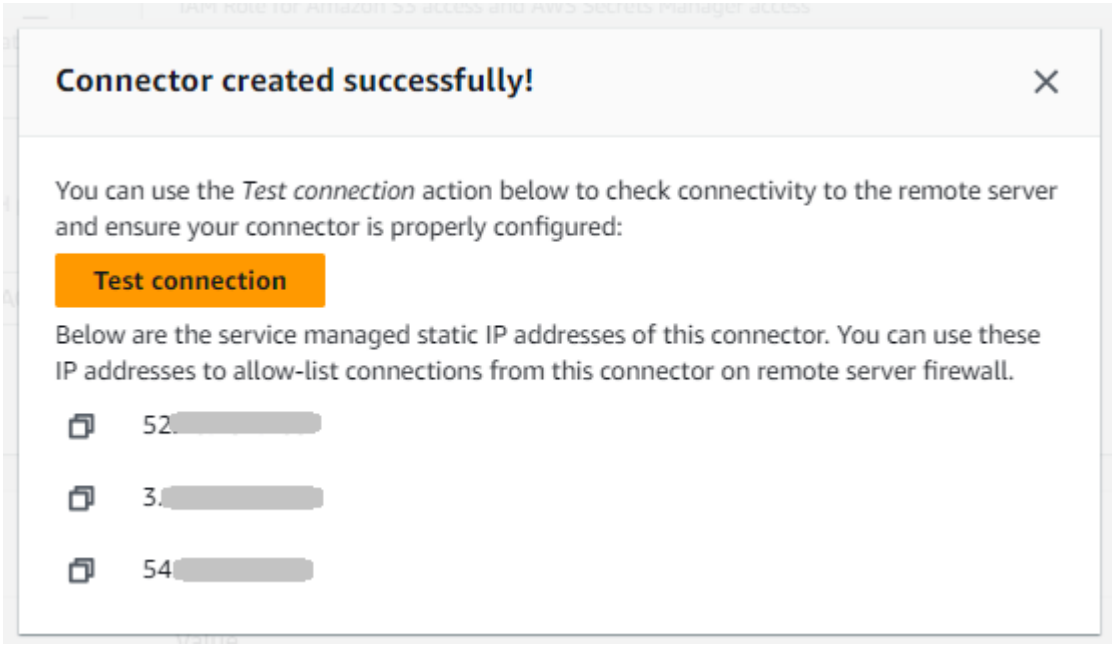
```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "SFTPConnectorPermissions",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogStream",
            "logs:DescribeLogStreams",
            "logs:CreateLogGroup",
            "logs:PutLogEvents"
        ],
        "Resource": [
            "arn:aws:logs:*:*:log-group:/aws/transfer/*"
        ]
    }]
}
```

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

   - Para las credenciales de Connector, en la lista desplegable, elija el nombre de un identificador 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 más detalles, consulte Guarde un secreto para usarlo con un conector SFTP.
   - En el caso de las claves de host de confianza, 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.

6. En la sección 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 AWS Transfer Family de seguridad para conectores SFTP.
7. (Opcional) En la sección Etiquetas, para Clave y Valor, escriba una o varias etiquetas como pares clave-valor.
8. Una vez que haya confirmado todos los ajustes, elija Crear conector para crear el conector SFTP. Si el conector se ha creado correctamente, aparece 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.

El siguiente ejemplo concede los permisos necesarios para acceder al *DOC-EXAMPLE-BUCKET en Amazon* S3 y al secreto especificado almacenado en Secrets Manager.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
        "Sid": "AllowListingOfUserFolder",
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        ]
```

```
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:region:account-id: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, consulte 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": "SFTPConnectorPermissions",
        "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**
>
> El `SecretId` puede ser el ARN completo o el nombre del secreto (*`example-username-key`* en la lista anterior).

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
```

Guarde un secreto para usarlo con un conector SFTP

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 detalles, 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 Precios de AWS Secrets Manager.

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

1. Inicie sesión en la AWS Secrets Manager consola AWS Management Console y ábrala 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 Pares clave-valor, seleccione la pestaña Clave/valor.
   - Clave: introduzca **`Username`**.
   - valor: introduzca el nombre del usuario que está autorizado a conectarse al servidor del socio.
6. Si desea proporcionar una contraseña, seleccione Añadir fila y, en la sección Pares clave/valor, elija la pestaña Clave/valor.

   Seleccione Añadir fila y, en la sección Pares clave/valor, elija la pestaña Clave/valor.
   - Clave: introduzca **`Password`**.
   - valor: introduzca una contraseña para el usuario.
7. Si desea proporcionar una clave privada, consulte Genere y formatee la clave privada del conector SFTP, que describe cómo introducir los datos de la clave privada.

   > **Note**
   >
   > 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.
8. Seleccione Next (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.

Genere y formatee la clave privada del conector SFTP

Los detalles completos para generar un key pair de claves pública/privada se describen en. Creación de claves SSH en macOS, Linux o Unix

Por ejemplo, para generar una clave privada para utilizarla con conectores SFTP, el siguiente comando de ejemplo produce el tipo de clave correcto (sustituya *key_name por el nombre* de archivo real del par de claves):

```
ssh-keygen -t rsa -b 4096 -m PEM -f key_name -N ""
```

> **Note**
>
> Cuando cree su key pair para usarlo con conectores SFTP, no utilice una contraseña. Es necesaria una contraseña vacía para que la configuración de SFTP funcione correctamente.

Este comando crea un key pair RSA, con un tamaño de clave de 4096 bits. La clave se genera en el formato PEM heredado, que Transfer Family requiere para su uso con el secreto del conector SFTP. Las claves se guardan en *key_name* (clave privada) y *key_name*`.pub` (clave pública) en el directorio actual, es decir, en el directorio en el que se ejecuta el `ssh-keygen` comando.

> **Note**
>
> Transfer Family no admite el formato OpenSSH `-----BEGIN OPENSSH PRIVATE KEY-----` () para las claves utilizadas en el conector SFTP. La clave debe estar en formato PEM antiguo (`-----BEGIN RSA PRIVATE KEY-----` o `-----BEGIN EC PRIVATE KEY-----`). Puede utilizar la herramienta ssh-keygen para convertir la clave, proporcionando la opción de `-m PEM` al ejecutar el comando.

Después de generar la clave, debe asegurarse de que la clave privada esté formateada con caracteres de nueva línea incrustados (»\n«) en formato JSON.

Usa un comando para convertir tu clave privada existente al formato correcto: formato JSON con caracteres de nueva línea incrustados. A continuación, se proporcionan ejemplos de Powershell. `jq` Puedes usar cualquier herramienta o comando para convertir la clave privada al formato JSON con caracteres de nueva línea incrustados.

jq command

En este ejemplo, se usa el `jq` comando, que se puede descargar desde Download jq.

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

Por ejemplo, si el archivo de clave privada se encuentra en`~/.ssh/my_private_key`, el comando es el siguiente.

```
jq -sR . ~/.ssh/my_private_key
```

Esto devuelve la clave en el formato correcto (con caracteres de nueva línea incrustados) a la salida estándar.

PowerShell

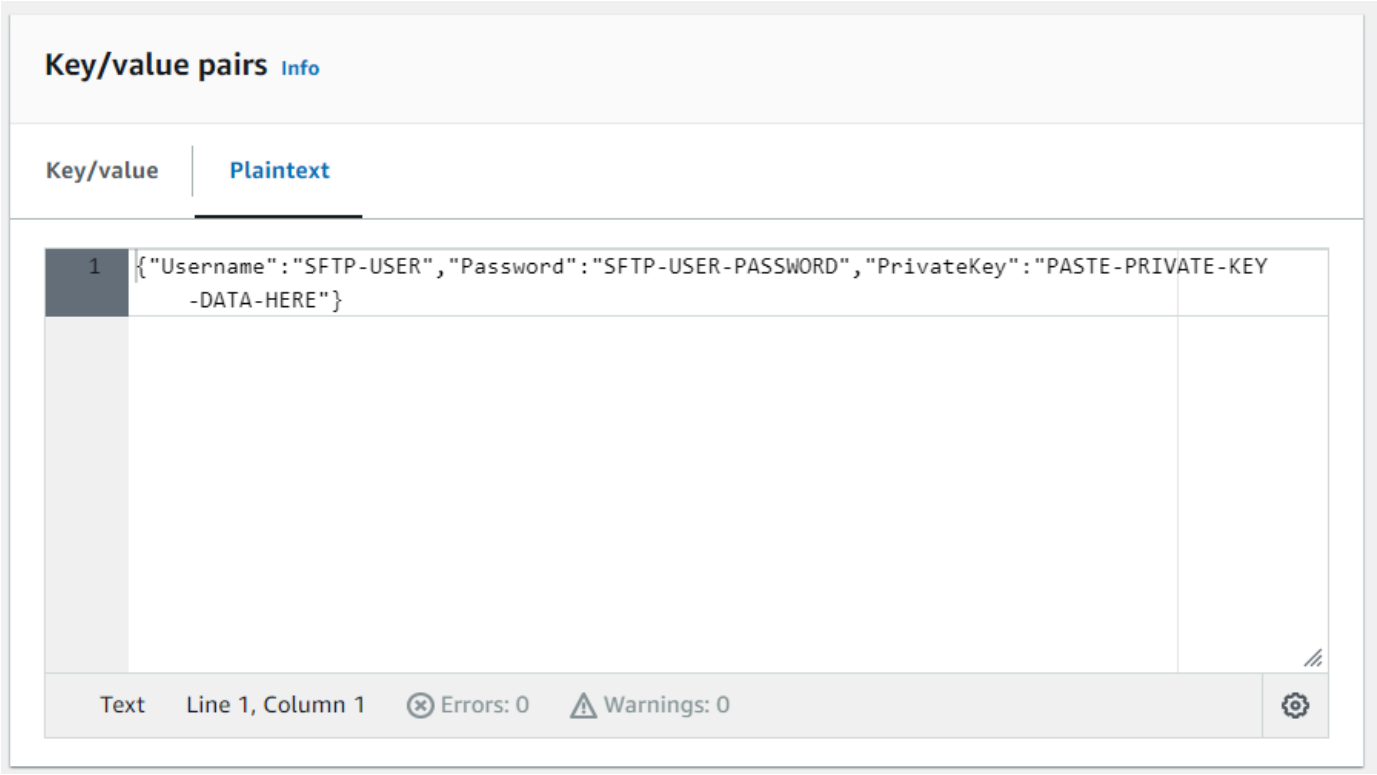
Si utiliza Windows, puede utilizarlo PowerShell para convertir la clave al formato correcto. El siguiente comando de Powershell convierte la clave privada al formato correcto.

```
Get-Content -Raw path-to-private-key-file | ConvertTo-Json
```

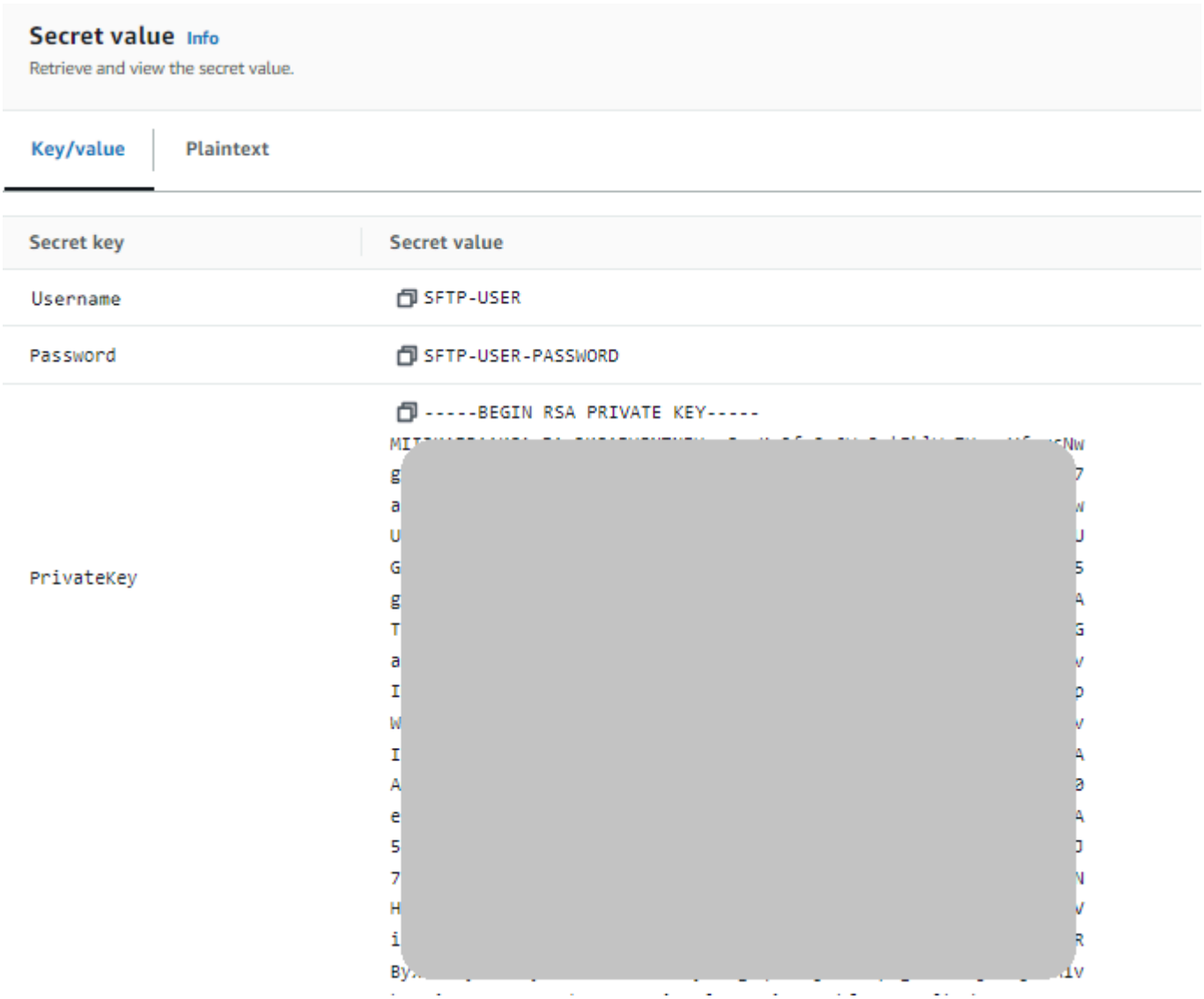
Cómo añadir datos de clave privada al secreto para su uso con los conectores SFTP

1. En la consola de Secrets Manager, cuando guarde Otro tipo de secreto, seleccione la pestaña Texto sin formato. El texto debe estar vacío, con solo una llave de apertura y cierre, {}.
2. Pegue su nombre de usuario, datos de clave privada o contraseña con el siguiente formato. Para sus datos de la clave privada, pegue el resultado del comando que ejecutó en el paso 1.

```
{"Username":"SFTP-USER","Password":"SFTP-USER-PASSWORD","PrivateKey":"PASTE-
PRIVATE-KEY-DATA-HERE"}
```



Si pega los datos de la clave privada correctamente, debería ver lo siguiente al seleccionar la pestaña Clave/valor. Observe que los datos de la clave privada se muestran line-by-line en lugar de mostrarse como una cadena continua de texto.



3. Continúe con el procedimiento en Guarde un secreto para usarlo con un conector SFTP en el paso 8 y sígalo hasta el final.

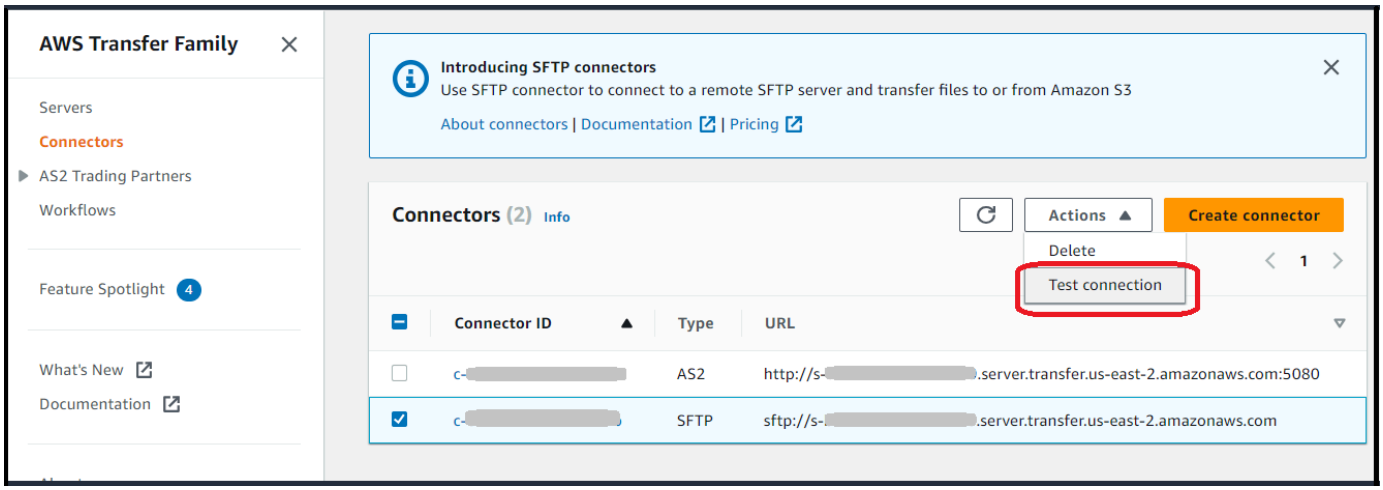
Prueba de un conector SFTP

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

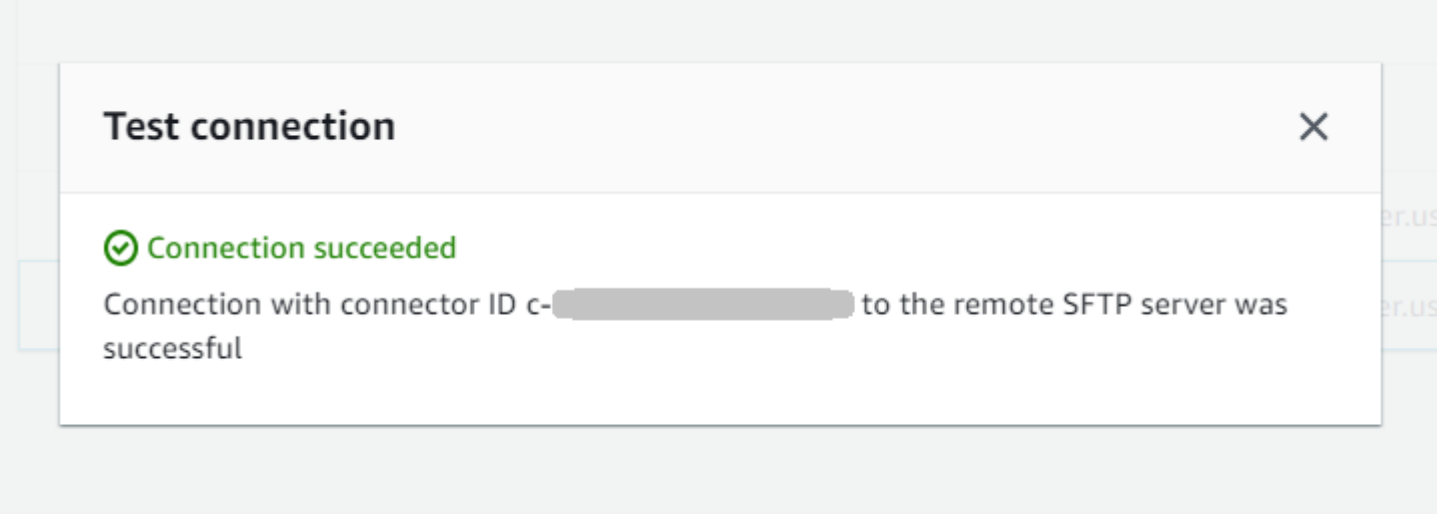
Prueba de un conector SFTP

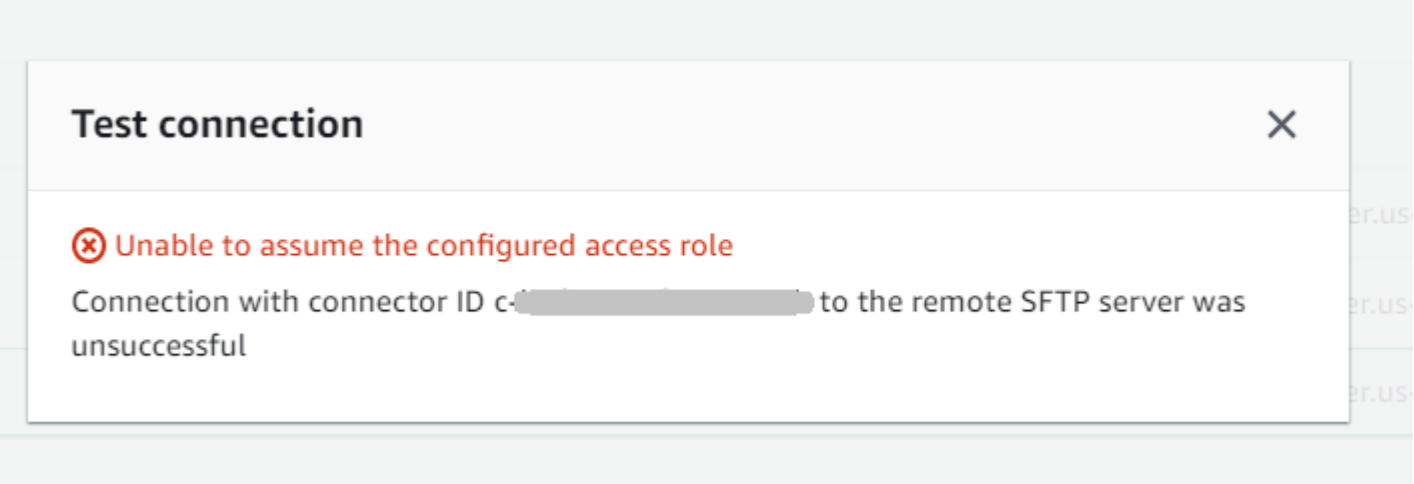
1. Abra la AWS Transfer Family consola en https://console.aws.amazon.com/transfer/.
2. En el panel de navegación izquierdo, seleccione Conectores y seleccione un conector.

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.

Enviar y recuperar archivos mediante un conector SFTP

Los conectores SFTP amplían las capacidades de AWS Transfer Family comunicación con servidores remotos tanto en la nube como en las instalaciones. Puede integrar los datos que se generan y almacenan en fuentes remotas con sus almacenes de datos AWS alojados para realizar análisis, aplicaciones empresariales, informes y auditorías.

Para iniciar una transferencia de archivos a un servidor SFTP remoto, utilice la operación API StartFileTransfer, que utiliza conectores SFTP para realizar la transferencia. Cada solicitud `StartFileTransfer` puede contener 10 rutas distintas.

Puede supervisar las transferencias de archivos consultando los registros del servidor. La actividad de los conectores se registra en los flujos de registro que tienen el formato de `aws/transfer/`*`connector-id`*, por ejemplo, `aws/transfer/c-1234567890abcdef0`. Si no ve ningún registro para su conector, asegúrese de haber especificado un rol de registro con los permisos correctos para el conector.

Para obtener información sobre cómo crear conectores, consulte Configure los conectores SFTP.

Para enviar y recuperar archivos mediante un conector SFTP, utilice el comando `start-file-transfer` AWS Command Line Interface (AWS CLI). Debe especificar los siguientes parámetros, en función de si envía archivos (transferencias salientes) o si recibe archivos (transferencias entrantes).

- 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 `/DOC-EXAMPLE-SOURCE-BUCKET/file1.txt` y `/DOC-EXAMPLE-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 *DOC-EXAMPLE-SOURCE-BUCKET* por su propio bucket.

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-SOURCE-BUCKET/
file1.txt /DOC-EXAMPLE-SOURCE-BUCKET/file2.txt \
    --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

Para recibir los archivos, debe especificar 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 el prefijo /DOC-EXAMPLE-BUCKET/ de la ubicación de Amazon S3.* 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 /DOC-EXAMPLE-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 `/DOC-EXAMPLE-SOURCE-BUCKET/file1.txt` a `/users/marymajor/test-connectors/file1.txt`.

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-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 archivos de un servidor SFTP remoto, puede recuperar el contenido de un directorio del servidor SFTP remoto. Para ello, utiliza la llamada a la StartDirectoryListingAPI.

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 `/DOC-EXAMPLE-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 /DOC-EXAMPLE-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 10 000 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"
}
```

Administrar conectores SFTP

En este tema se describe cómo ver y actualizar los conectores SFTP y se enumeran las cuotas que son relevantes para 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

Temas

- Actualizar conectores SFTP
- Ver los detalles del conector SFTP
- Cuotas para conectores SFTP

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
```

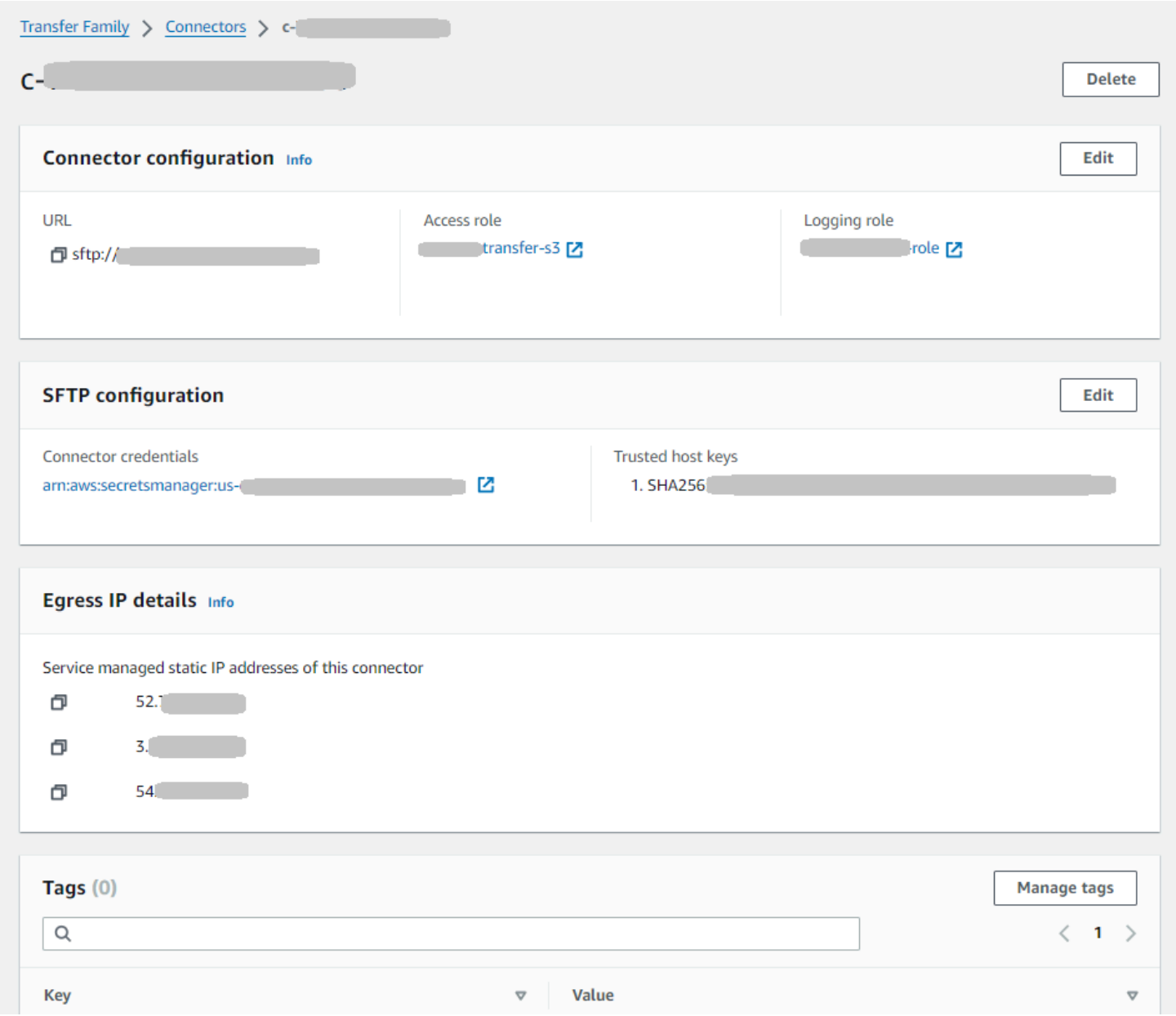
Ver los detalles del conector SFTP

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.



> **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.

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

Nombre	Valor 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	50 gibibytes (GiB)	No
Tiempo máximo de transfere ncia por archivo	6 horas	No
Tiempo máximo de espera de solicitudes por archivo	6 horas	No
Ancho de banda máximo para los conectores por cuenta (tanto los conectores SFTP como los AS2 contribuyen a este valor)	50 MBps	No

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

AWS Transfer Family para AS2

La Declaración de aplicabilidad 2 (AS2) es una especificación de transmisión de archivos definida por la RFC que incluye sólidos mecanismos de verificación y protección de mensajes. El protocolo AS2 es fundamental para los flujos de trabajo con requisitos de conformidad que se basan en la incorporación de características de seguridad y protección de datos en el protocolo.

> **Note**
>
> AS2 para Transfer Family cuenta con la certificación de Drummond.

Los clientes de sectores como el comercio minorista, las ciencias de la vida, la fabricación, los servicios financieros y los servicios públicos que confían en el AS2 para los flujos de trabajo de la cadena de suministro, la logística y los pagos pueden utilizar los puntos de conexión de AS2 de AWS Transfer Family para realizar transacciones de forma segura con sus socios comerciales. Se puede acceder de forma nativa a los datos transaccionados AWS para su procesamiento, análisis y aprendizaje automático. Estos datos también están disponibles para integrarlos con los sistemas de planificación de recursos empresariales (ERP) y de gestión de relaciones con los clientes (CRM) que se ejecutan en AWS. Con AS2, los clientes pueden ejecutar sus transacciones business-to-business (B2B) a escala y, al AWS mismo tiempo, mantener las integraciones y el cumplimiento de los socios comerciales existentes.

Si es cliente de Transfer Family y desea intercambiar archivos con un socio que tiene un servidor configurado compatible con AS2, la configuración implica generar un par de claves público-privadas para el cifrado y otro para firmar e intercambiar las claves públicas con el socio.

Transfer Family ofrece un taller al que puede asistir, en el que puede configurar un terminal Transfer Family con AS2 habilitado y un conector Transfer Family AS2. Puede ver los detalles de este taller aquí.

La protección de una carga AS2 en tránsito normalmente implica el uso de la sintaxis de mensajes criptográficos (CMS) y, por lo general, utiliza el cifrado y una firma digital para proporcionar protección de datos y autenticación entre 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 transporte de estas cargas útiles del CMS y las respuestas de MDN se realiza a través de HTTP.

> **Note**
>
> Actualmente no se admiten los puntos de conexión del servidor HTTPS AS2. La rescisión del TLS es actualmente responsabilidad del cliente.

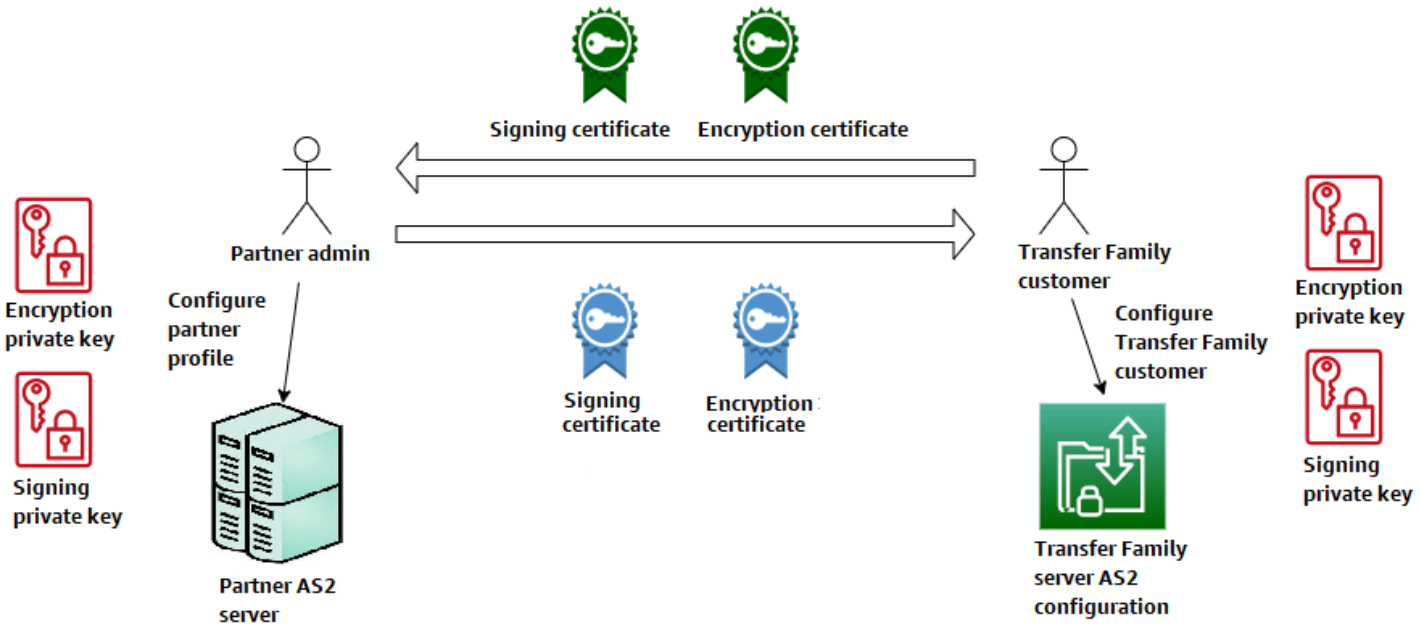
Para obtener un step-by-step tutorial detallado sobre cómo configurar una configuración de la Declaración de Aplicabilidad 2 (AS2), consulte el tutorial. Configuración de una configuración AS2

Temas

- Casos de uso de AS2
- Configuración de AS2
- Configure los conectores AS2
- Gestione los socios de AS2
- Envío y recepción de mensajes AS2
- Monitorización del uso de AS2

Casos de uso de AS2

Si es un AWS Transfer Family cliente que desea intercambiar archivos con un socio que tiene un servidor AS2 configurado, la parte más compleja de la configuración implica 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 con el AS2 AWS Transfer Family .

> **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

Casos de uso únicamente entrantes

- 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.

Casos de uso exclusivos para dispositivos salientes

- 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.

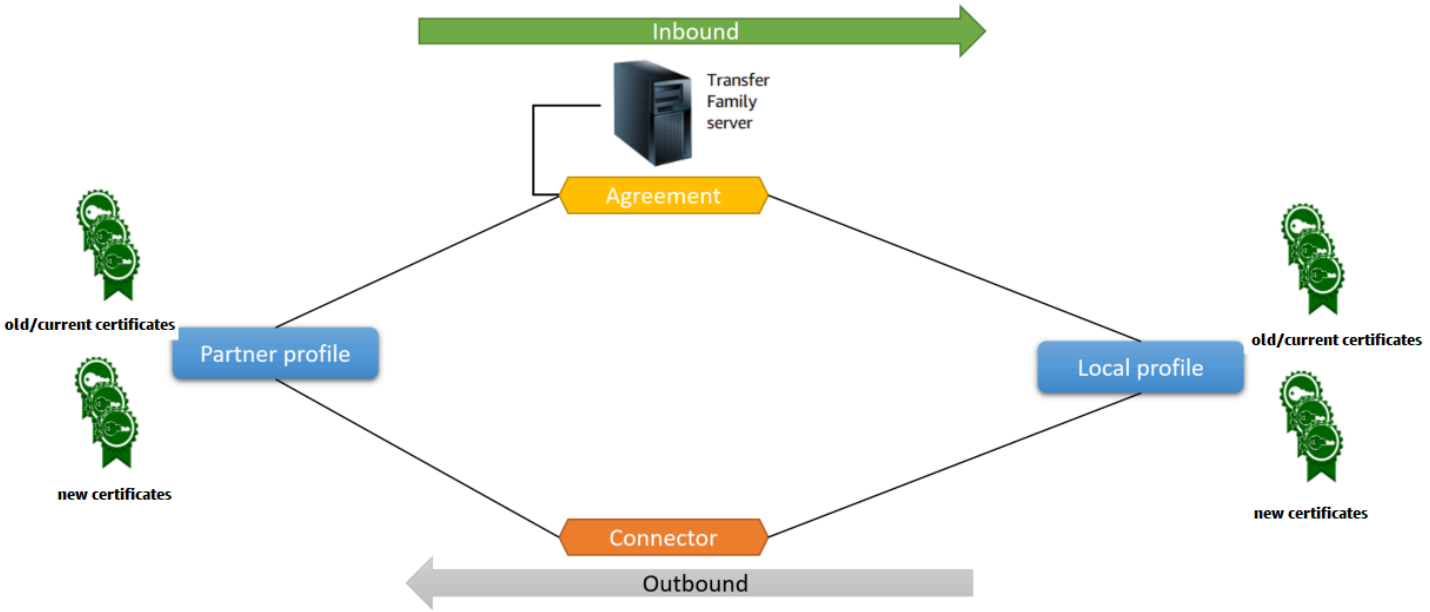
Configuración de AS2

Para crear un servidor compatible con AS2, 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. Los procesos entrantes de Transfer Family AS2 utilizan acuerdos.
- Certificados: los certificados (X.509) de clave pública 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 empresa o “parte” local (servidor Transfer Family habilitado para AS2). Del mismo modo, un perfil de socio define la empresa asociada remota, externa a Transfer Family.

Si bien no es obligatorio para todos los servidores compatibles con AS2, 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 servidor, del cliente. AWS

El siguiente diagrama muestra la relación entre los objetos AS2 que participan en los procesos de entrada y salida.



Para ver un end-to-end ejemplo de configuración AS2, consulteConfiguración de una configuración 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
- Configuraciones y cuotas de AS2
- Características y funciones básicas de AS2

Cree un servidor AS2 mediante la consola Transfer Family

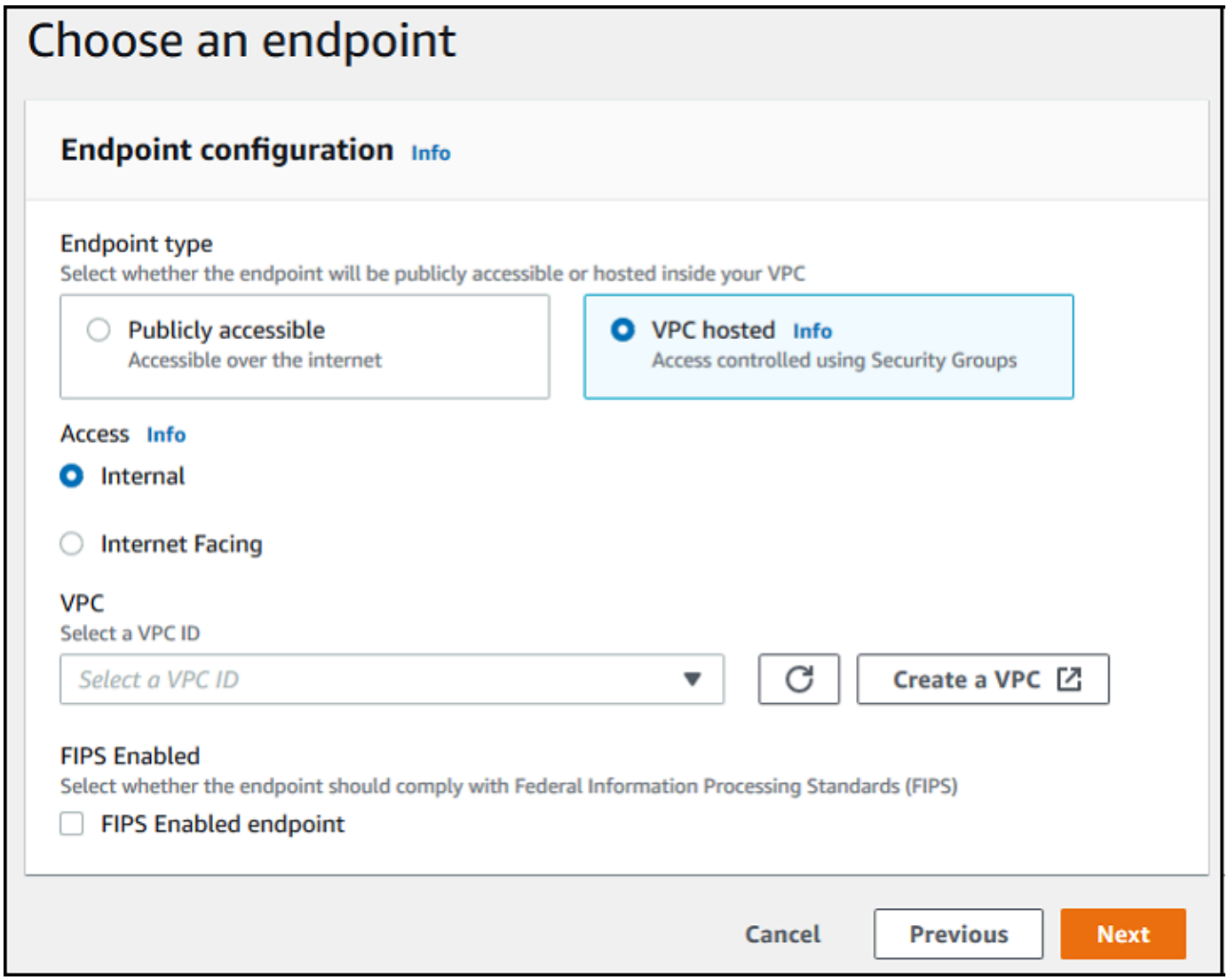
En este procedimiento, se explica cómo crear un servidor con AS2 desde la consola de Transfer Family. Si desea utilizar el en su AWS CLI lugar, consulte. the section called “Paso 2: creación de un servidor de Transfer Family que utilice el protocolo AS2”

Creación de un servidor compatible con AS2

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:



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 alojado en la VPC, 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 sus entornos de VPC y conectados a VPC, como un centro de datos en las instalaciones a través de un AWS Direct Connect o VPN.
- Orientado a Internet: elija esta opción para proporcionar acceso a través de Internet y desde sus entornos de VPC y conectados a VPC, como un centro de datos local a través de una VPN. AWS Direct Connect

  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**
>
> Los puntos de conexión habilitados para FIPS 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 CloudWatch secciones de 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 AWS CloudFormation plantilla independiente para crear rápidamente un servidor Transfer Family compatible con AS2. 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.

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 para AWS Secrets Manager 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 Transfer Family compatible con AS2 a partir de una plantilla CloudFormation

1. Abra la AWS 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 Requisito previo: preparar plantilla, elija La plantilla está lista.
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-`*`TransferS3BucketName`*.
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, debe reconocer que AWS CloudFormation podría 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 TransferExampleAscomando 2. 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 TransferS3BucketName --key test.txt && aws transfer
 start-file-transfer --region aws-region --connector-id TransferConnectorId --send-
file-paths /TransferS3BucketName/test.txt
```

> **Note**
>
> Su versión de este comando contiene los valores reales para los recursos *TransferS3BucketName* 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 TransferS3BucketName --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 /TransferS3BucketName/test.txt
```

Tras ejecutar el comando, puede ir a su bucket de Amazon S3 (*TransferS3BucketName*) 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.

Configuraciones y cuotas de 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. En esta sección, también se describen los límites y los problemas conocidos de las transferencias AS2.

Temas

- Configuraciones AS2 admitidas
- Cuotas y limitaciones de AS2

Configuraciones AS2 admitidas

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 proxy de terminación de TLS, como un equilibrador de carga de aplicación (ALB), y el encabezado `X-Forwarded-Proto: https` 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: solo sincrónicas
- 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

Nombre	Valor predeterminado	Ajustable
Número máximo de archivos entrantes recibidos por segundo	100	No
Número máximo de archivos salientes enviados por segundo	100	No
Número máximo de archivos entrantes simultáneos	400	No
Número máximo de archivos salientes simultáneos	400	No
Tamaño máximo del archivo entrante (sin comprimir)	1 GB	No

Nombre	Valor predeterminado	Ajustable
Tamaño máximo del archivo saliente (sin comprimir)	1 GB	No
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
Ancho de banda saliente máximo por cuenta (las solicitudes SFTP y AS2 salientes contribuyen a este valor)	50 MB por segundo	No
Número máximo de acuerdos por servidor	100	Sí
Número máximo de conectores por cuenta (los conectores SFTP y AS2 contribuyen a este límite)	100	Sí
Número máximo de certificados por perfil de socio	10	No
Número máximo de certificados por cuenta	1 000	Sí
Número máximo de perfiles de socios por cuenta	1 000	Sí

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 de GetSecretValue API DescribeSecret y la tasa, tal y como se describe en AWS Secrets Manager las cuotas.

Secrets Manager **`GetSecretValue`**

Nombre	Valor	Descripción
Tasa combinada de solicitud es DescribeSecret y GetSecretValue API	Cada región admitida: 10 000 por segundo	El número máximo de transacciones por segundo para las solicitudes de GetSecretValue API DescribeSecret y las solicitud es 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 que se utilice. Cada cuota se calcula por separado.

Nombre de la cuota	Límite predeterminado (solicitudes por segundo)

	• 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

- No se admite el protocolo TCP keep-alive del servidor. 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 procesado/Advertencia: documento duplicado.
- 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 a un 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. Actualmente, los certificados autofirmados solo se admiten para las 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 servidores AWS Transfer Family).
- 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.

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
Algoritmos criptográficos SHA-2	Sí

Característica	Compatible con AWS Transfer Family
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.

Capability	Entrante: recepción con servidor	Saliente: envío con conector
Transporte cifrado TLS (HTTPS)	Sí [1]	Sí
Transporte sin TLS (HTTP)	Sí	Sí [2]
MDN síncrono	Sí	Sí
Compresión de mensajes	Sí	Sí
MDN asíncrono	Sí	No

Capability	Entrante: recepción con servidor	Saliente: envío con conector
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 de entrada disponible con equilibrador de carga de red (NLB)

2. El transporte saliente sin TLS solo está disponible cuando el cifrado está activado

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.

Cree un conector AS2

En este procedimiento se explica cómo crear conectores AS2 mediante la AWS Transfer Family consola. Si desea utilizar el AWS CLI en su lugar, consultethe 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 y, a continuación, Crear conector.
3. En la sección de configuración del conector, especifique la siguiente información:
   - URL: introduzca la URL de las conexiones salientes.
   - 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:

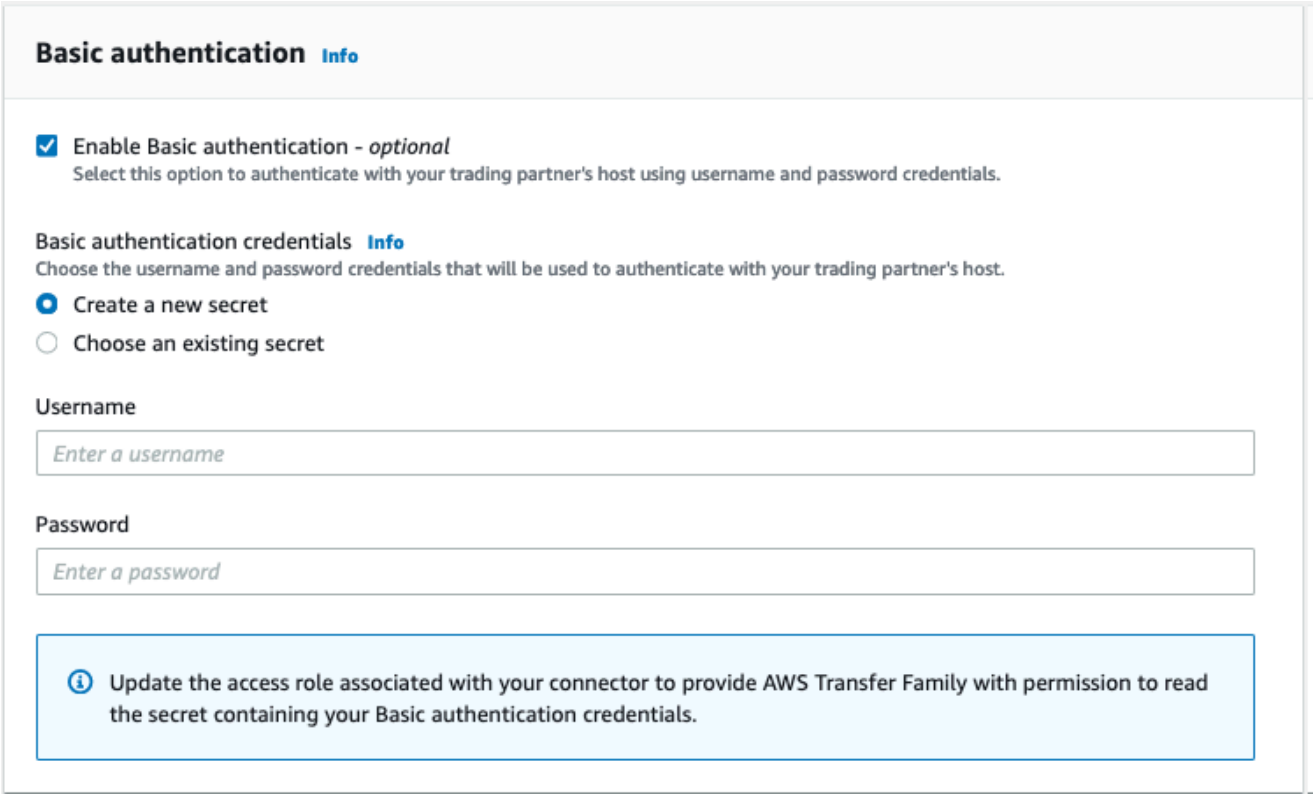
   - No elija el algoritmo de cifrado `DES_EDE3_CBC` a menos que sea compatible con un cliente antiguo que lo requiera, ya que se trata de un algoritmo de cifrado débil.
   - El Asunto se utiliza como atributo de encabezado `subject` HTTP en los mensajes de AS2 que se envían con el conector.
   - Si opta por crear un conector sin un algoritmo de cifrado, debe `HTTPS` especificarlo como protocolo.

5. En la sección de Configuración MDN, especifique la siguiente información:

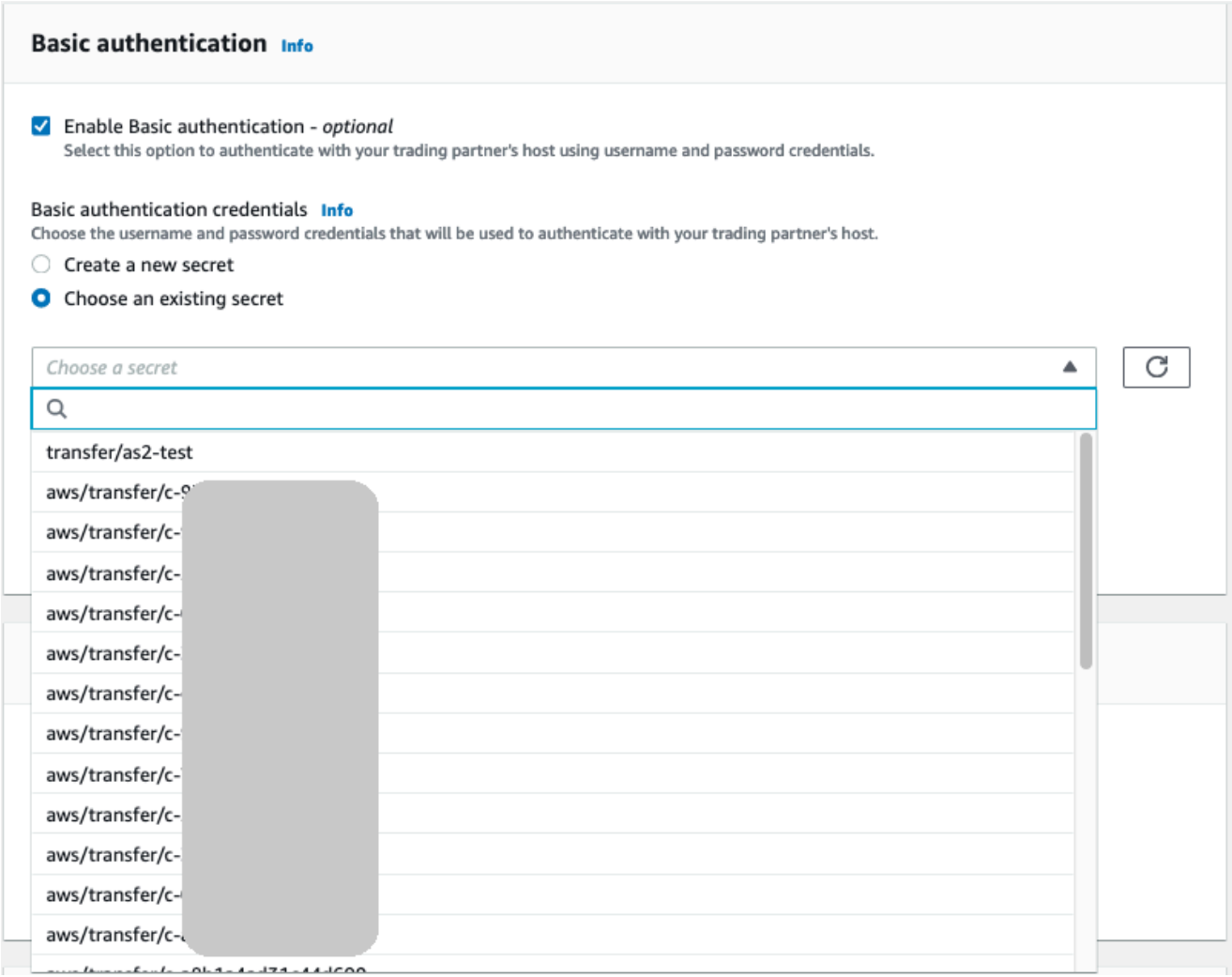
   - Solicite un MDN: tiene la opción de solicitar a su socio comercial que le envíe un MDN una vez que haya recibido correctamente su mensaje a través de AS2.
   - MDN firmado: tiene la opción de solicitar que el mDNS esté firmado. Esta opción solo está disponible si has seleccionado Solicitar MDN.

6. 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.



- 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.



7. Una vez que haya confirmado todos los ajustes, seleccione Crear conector 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

Tipo	Algoritmo
	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

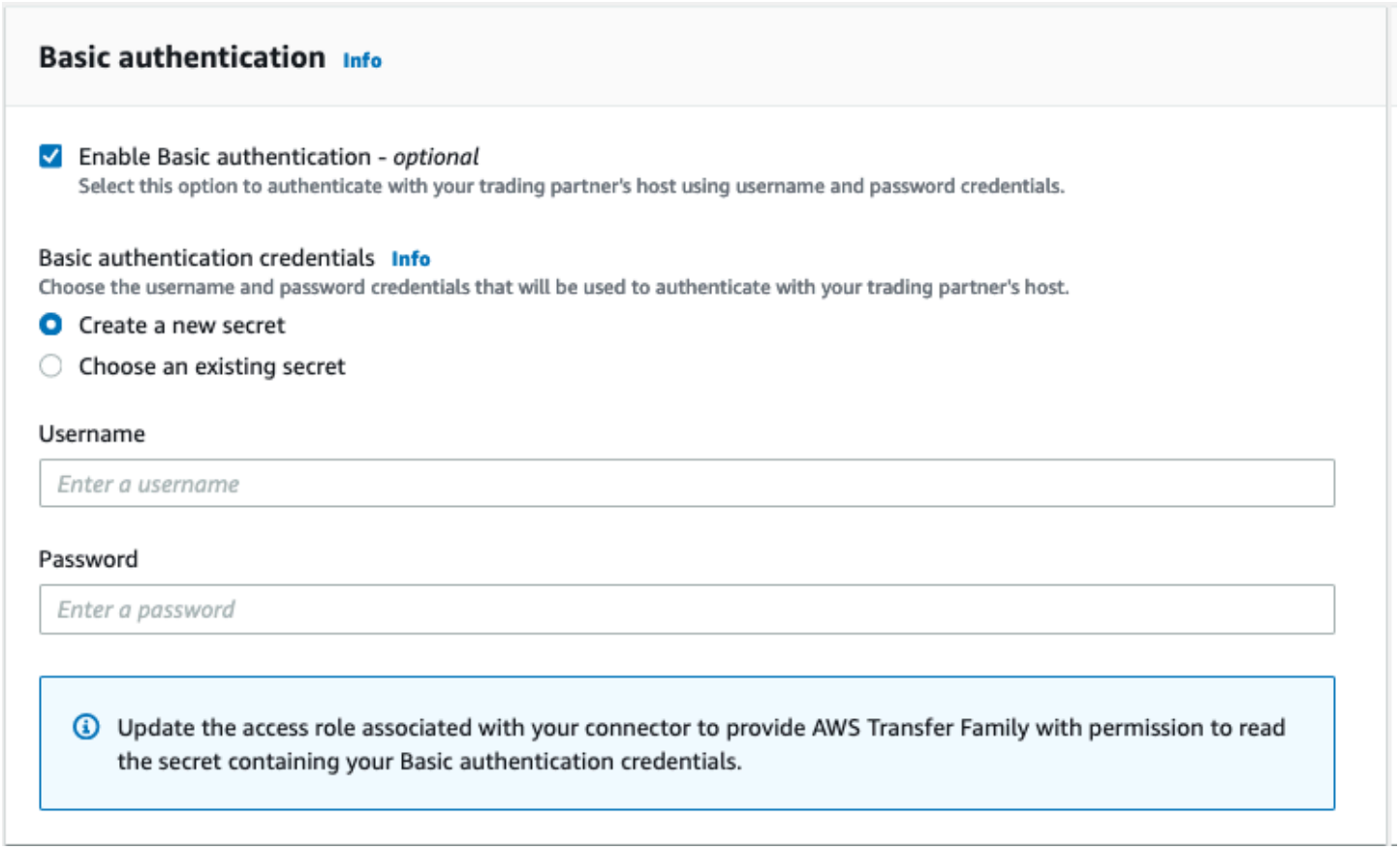
Autenticación básica para conectores AS2

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.

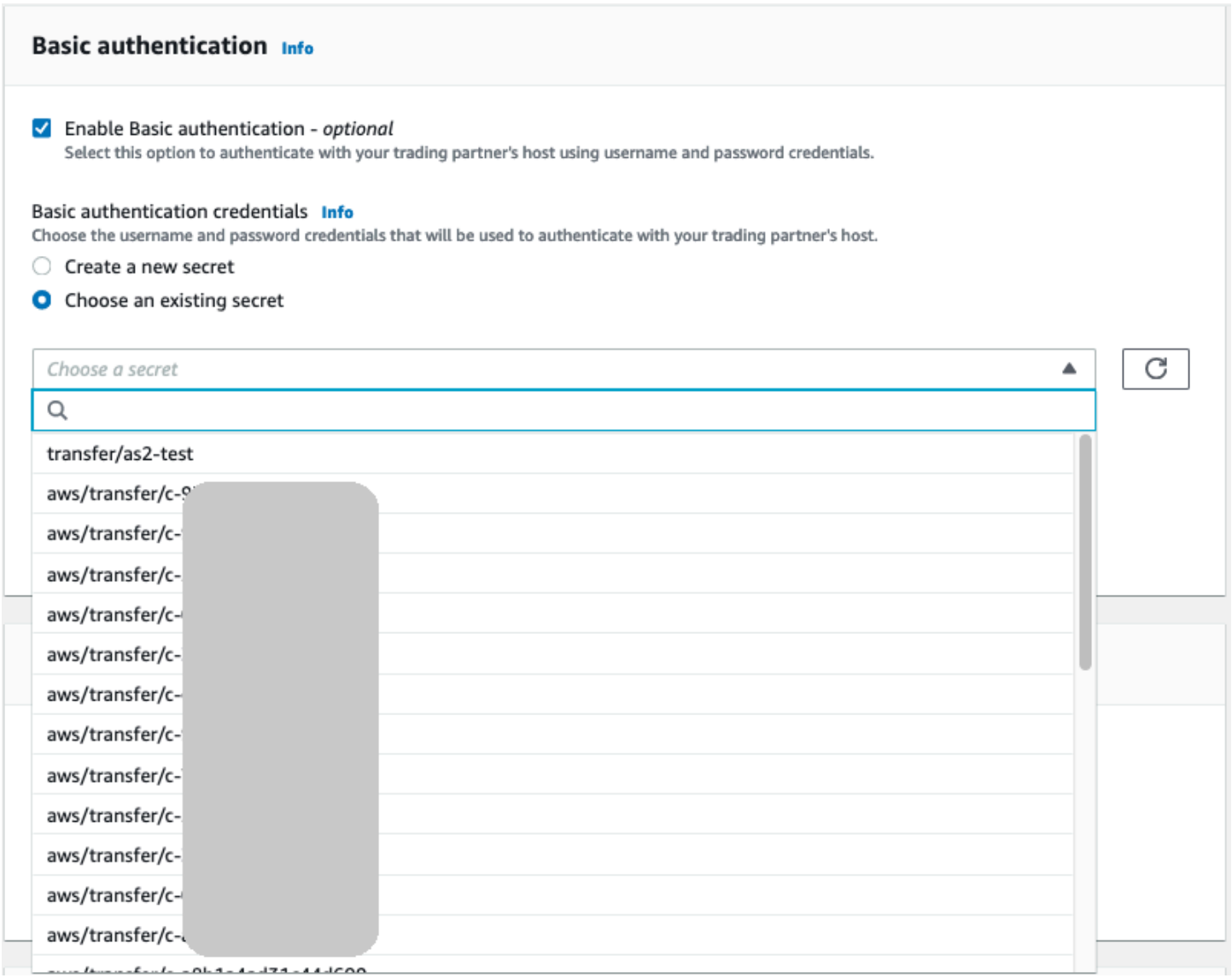
> **Note**
>
> La autenticación básica solo está disponible si utiliza HTTPS.

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.



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.

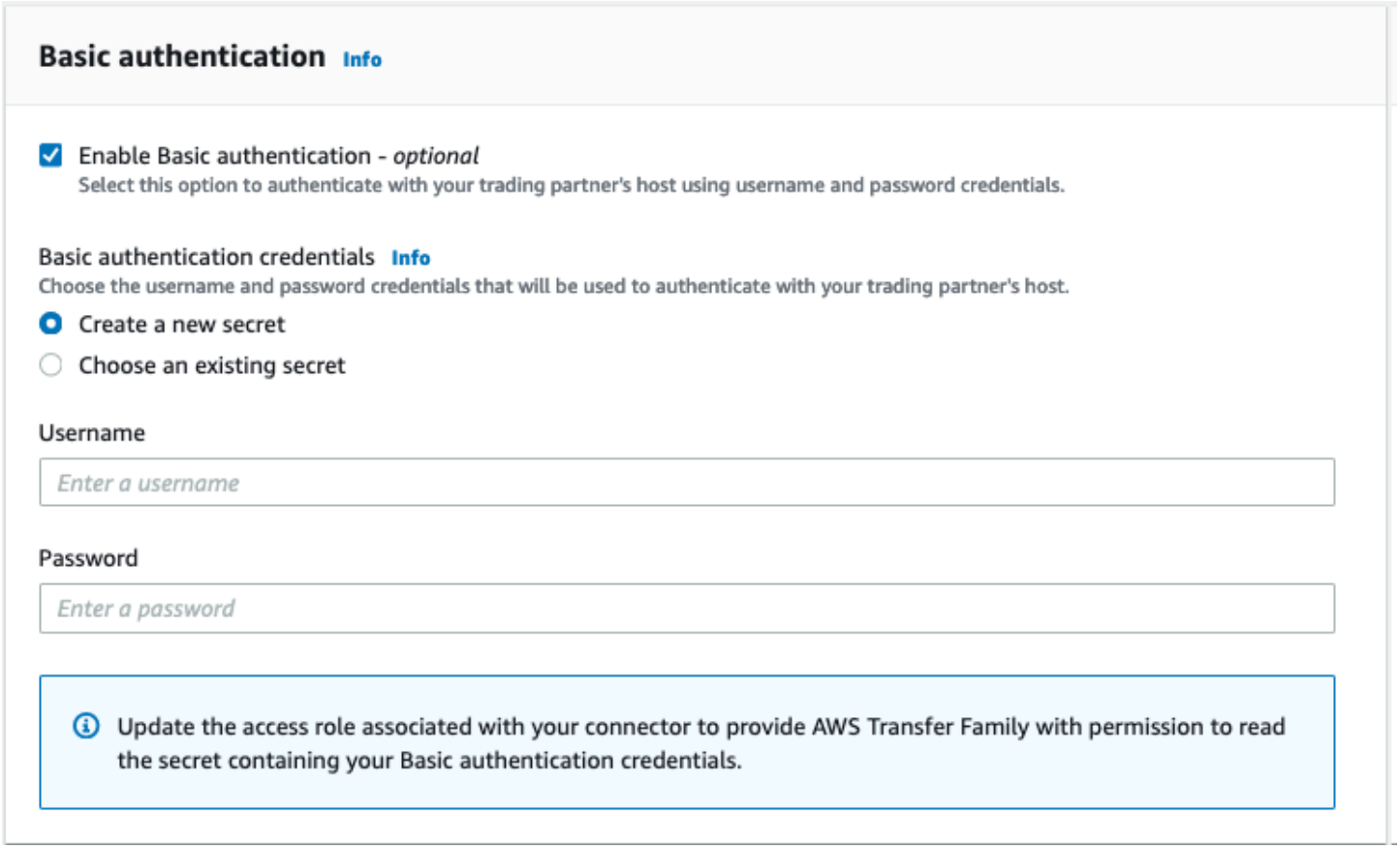
Temas

- 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.

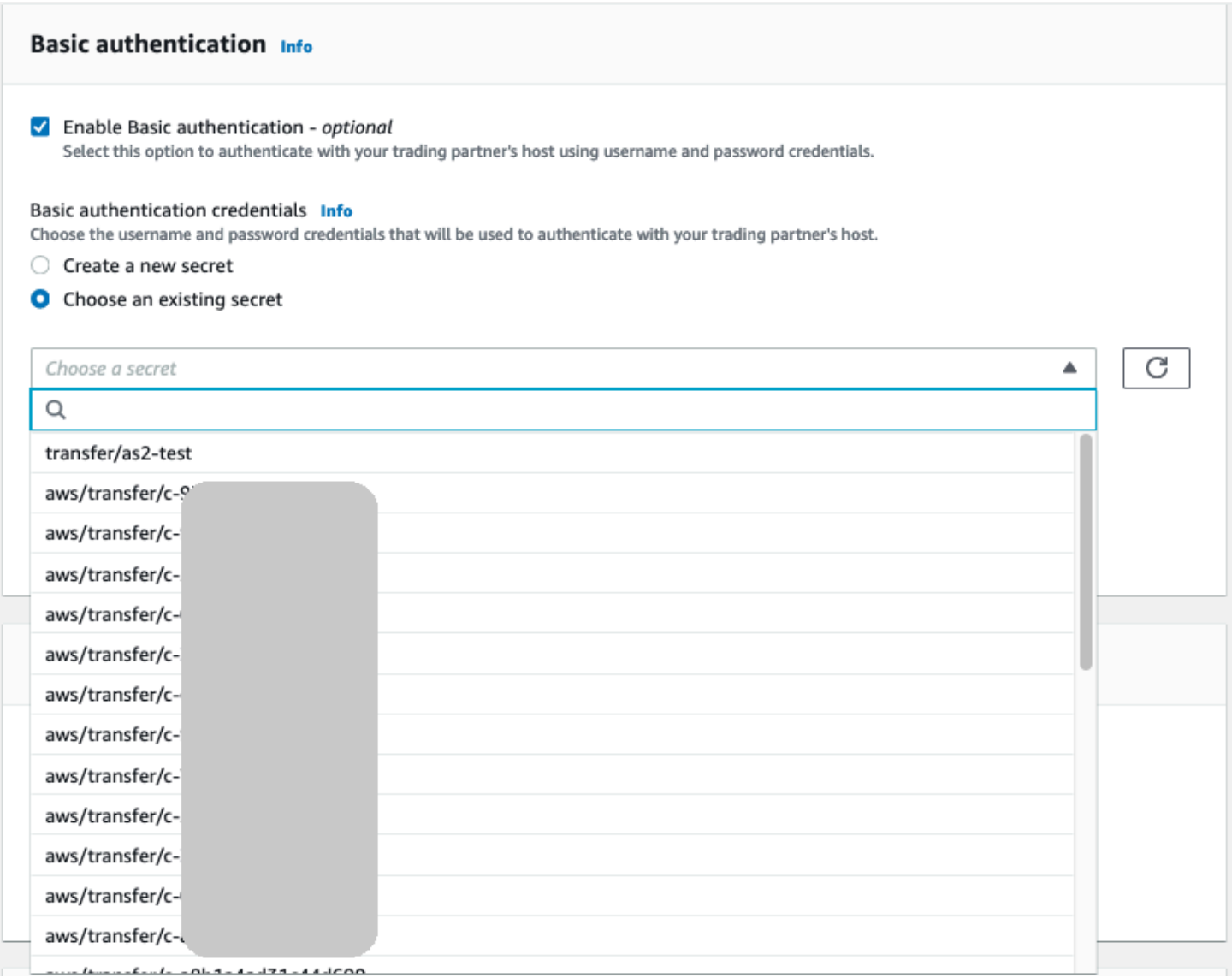


> **Note**
>
> Al crear un nuevo secreto en la consola, el nombre del secreto sigue esta convención de nomenclatura: **`/aws/transfer/`*`connector-id`***, donde *`connector-id`* es el ID del conector que se está creando. Ten esto en cuenta cuando intentes localizar el secreto AWS Secrets Manager.

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.



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 la AWS Secrets Manager consola AWS Management Console y ábrela 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 Pares clave-valor, seleccione la pestaña Clave/valor.
   - Clave: introduzca **`Username`**.
   - valor: introduzca el nombre del usuario que está autorizado a conectarse al servidor del socio.
6. Si desea proporcionar una contraseña, seleccione Añadir fila y, en la sección Pares clave/valor, elija la pestaña Clave/valor.

   Seleccione Añadir fila y, en la sección Pares clave/valor, elija la pestaña Clave/valor.
   - Clave: introduzca **`Password`**.
   - valor: introduzca una contraseña para el usuario.
7. Si desea proporcionar una clave privada, seleccione Añadir fila y, en la sección Pares clave/valor, elija la pestaña Clave/valor.
   - 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

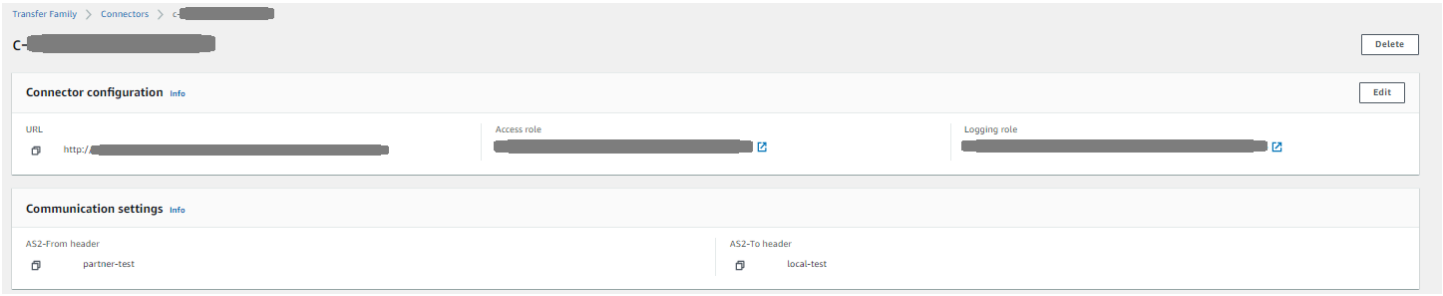
Encontrará una lista de detalles y propiedades de un AWS Transfer Family conector AS2 en la AWS Transfer Family consola. Las propiedades de un conector AS2 incluyen sus URL, roles, perfiles, MDN, etiquetas y métricas de supervisión.

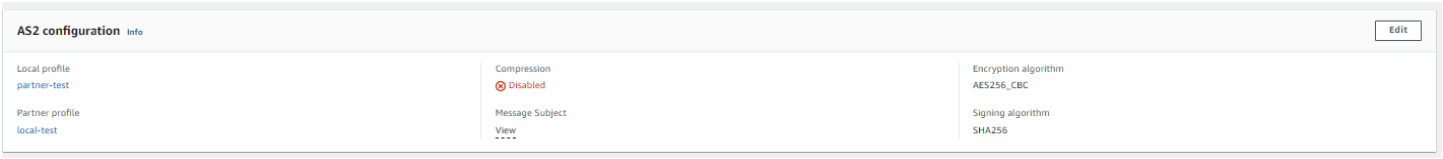
Este es el procedimiento para ver los detalles del conector.

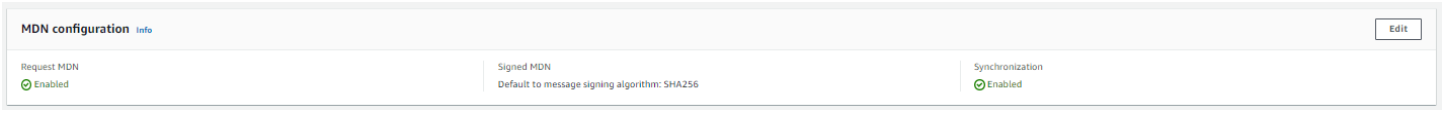
Visualización de los detalles del conector

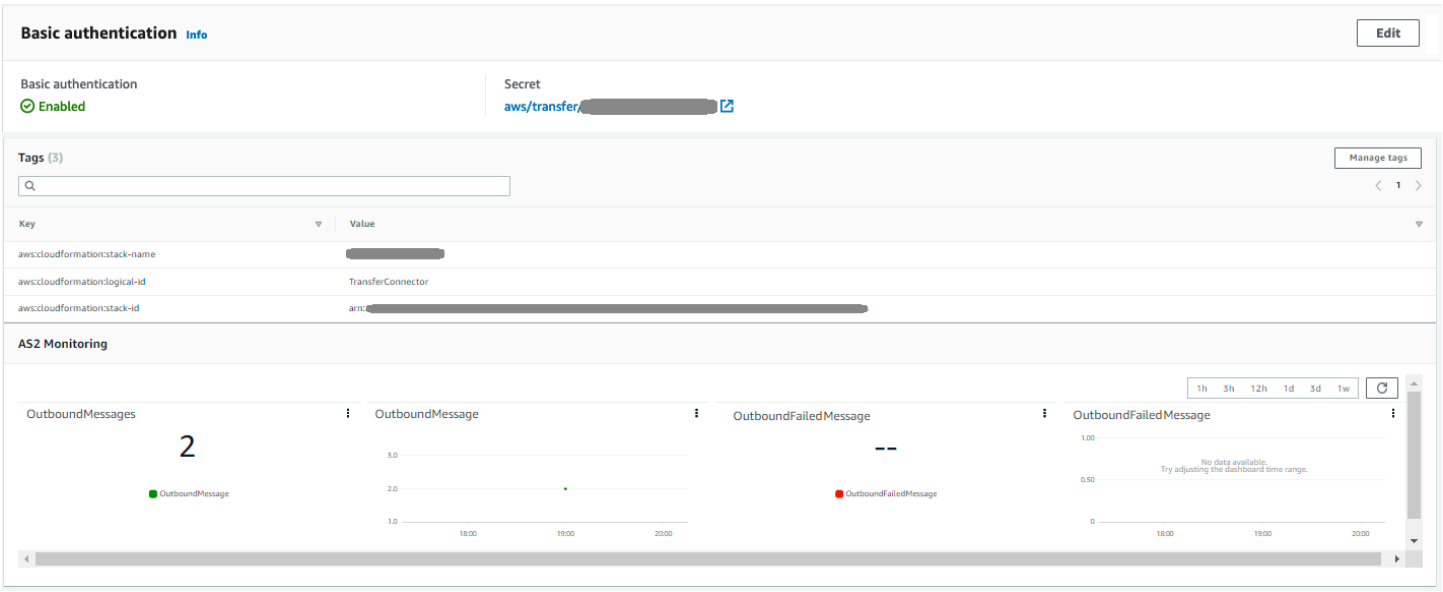
1. Abra la AWS Transfer Family consola en https://console.aws.amazon.com/transfer/.
2. En el panel de navegación izquierdo, seleccione Connectors (Conectores).
3. Elija el identificador en la columna ID del conector para ver la página de detalles del conector seleccionado.

Puede cambiar las propiedades del conector AS2 en la página de detalles del conector seleccionando Editar.









> **Note**
>
> Puede obtener gran parte de esta información, aunque en un formato diferente, ejecutando el siguiente comando AWS Command Line Interface (AWS CLI):
>
> ```
> aws transfer describe-connector --connector-id your-connector-id
> ```
>
> Para obtener más información, consulte DescribeConnector en la referencia de la API.

Gestione los socios de AS2

En este tema se explica cómo administrar los certificados, perfiles y acuerdos de 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 3: importación de certificados como recursos de certificados de Transfer Family”

Cómo especificar un certificado compatible con 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 Certificados.
3. Seleccione Importar certificado.

4. 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 Contenido del certificado, proporcione un certificado público de un socio comercial o las claves pública y privada de un certificado local.
6. En la sección Uso del certificado, elija el propósito de este certificado. Se puede usar para cifrar, firmar o ambas cosas.

   > **Note**
   >
   > Si elige Cifrado y la firma para el uso, Transfer Family crea dos certificados idénticos (cada uno con su propio ID): uno con un valor de uso `ENCRYPTION` y otro con un valor de uso de `SIGNING`.

7. Rellene la sección Contenido del certificado con los detalles correspondientes.

   - Si elige Certificado autofirmado, no proporciona una cadena de certificados.
   - Se pega en el contenido del archivo del certificado.
   - Si el certificado no está autofirmado, proporcione una cadena de certificados.
   - Si este certificado es un certificado local, pegue su clave privada.

8. Elija Importar certificado para completar el proceso y guardar los detalles del certificado importado.

> **Note**
>
> Los certificados TLS solo se pueden importar como certificados públicos 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.

Los certificados X.509 tienen fechas `Not Before` y `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.

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`.

En la siguiente tabla, se describe una forma posible de configurar dos certificados para un único perfil.

Dos certificados en rotación

Nombre	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)	01/11/2019	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

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 4: creación de perfiles para usted y su socio comercial”.

Creación de un perfil de AS2

1. Abra la consola en https://console.aws.amazon.com/transfer/ AWS Transfer Family .
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.

> **Note**
>
> 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.

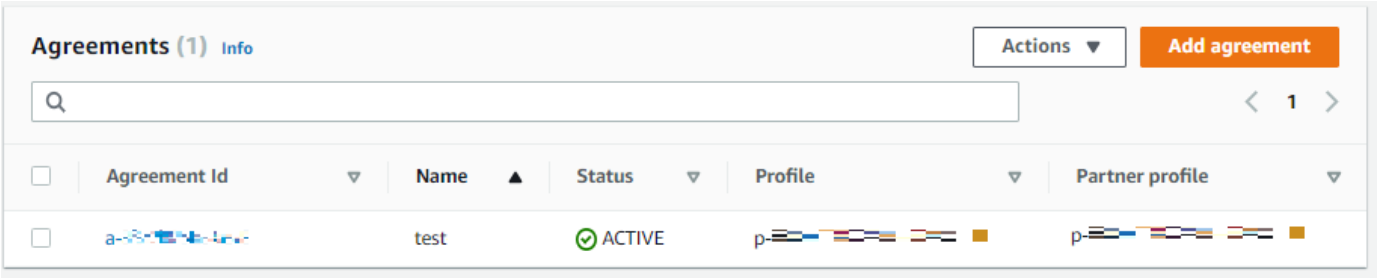
Creación de acuerdos AS2

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 la AWS CLI en su lugar, consultethe 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.
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.

c. En la sección de configuración de la carpeta Inbox, elija un bucket de Amazon S3 para almacenar los archivos entrantes y un rol de IAM que pueda acceder al bucket. Si lo desea, puede introducir un prefijo (carpeta) para almacenar los archivos en el bucket.

   Por ejemplo, si escribe **`DOC-EXAMPLE-BUCKET`** para su bucket y **`incoming`** para su prefijo, los archivos entrantes se guardarán en la carpeta `/DOC-EXAMPLE-BUCKET/incoming`.

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.

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

Algoritmo de cifrado	HTTP	HTTPS	Notas
			puede seleccionar `NONE` si utiliza un Application Load Balancer (ALB).

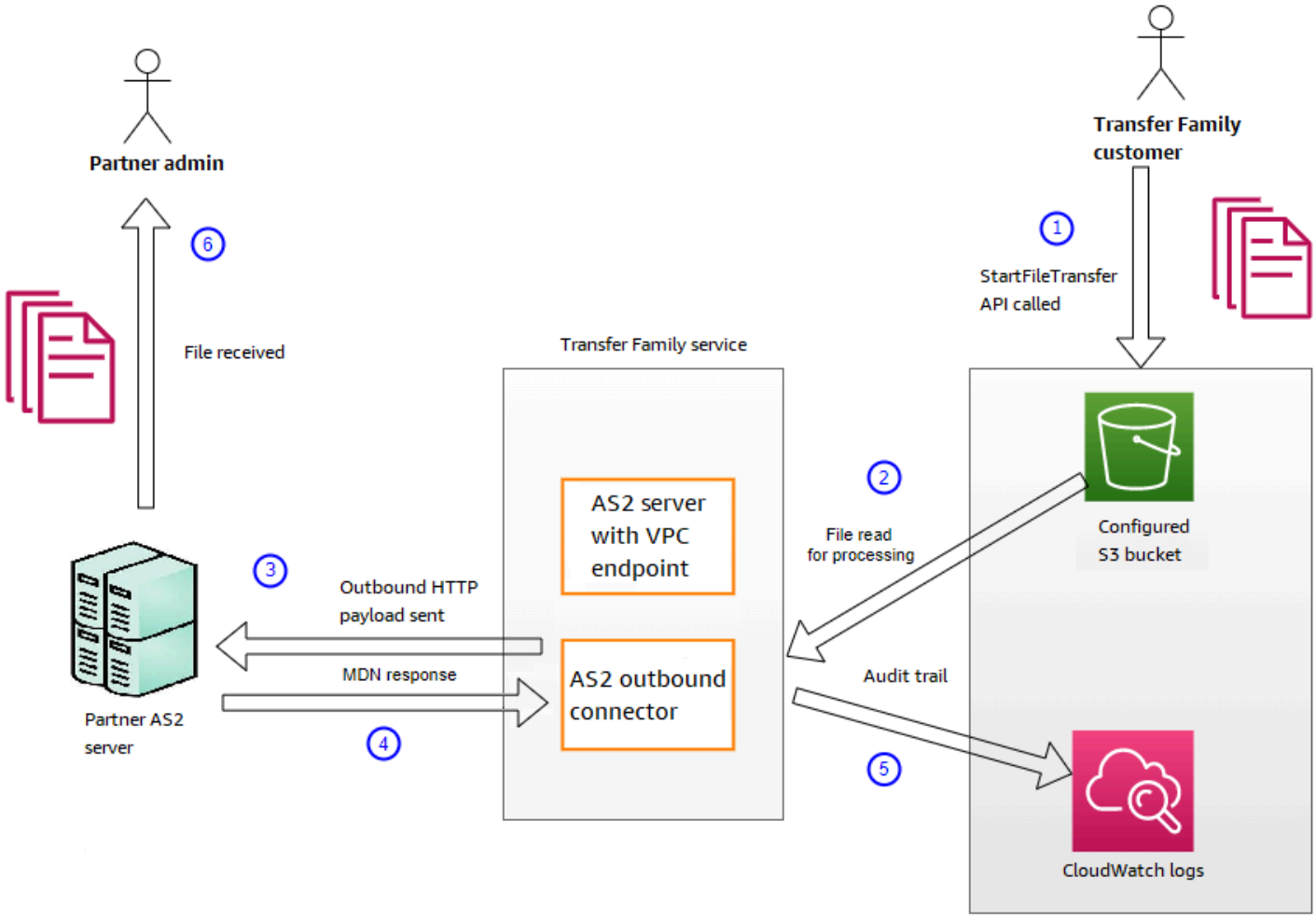
Temas

- Proceso de envío de mensajes AS2
- 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 envío de mensajes AS2

El proceso de salida se define como un mensaje o 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, en línea con la respuesta HTTP (MDN síncrona).
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.



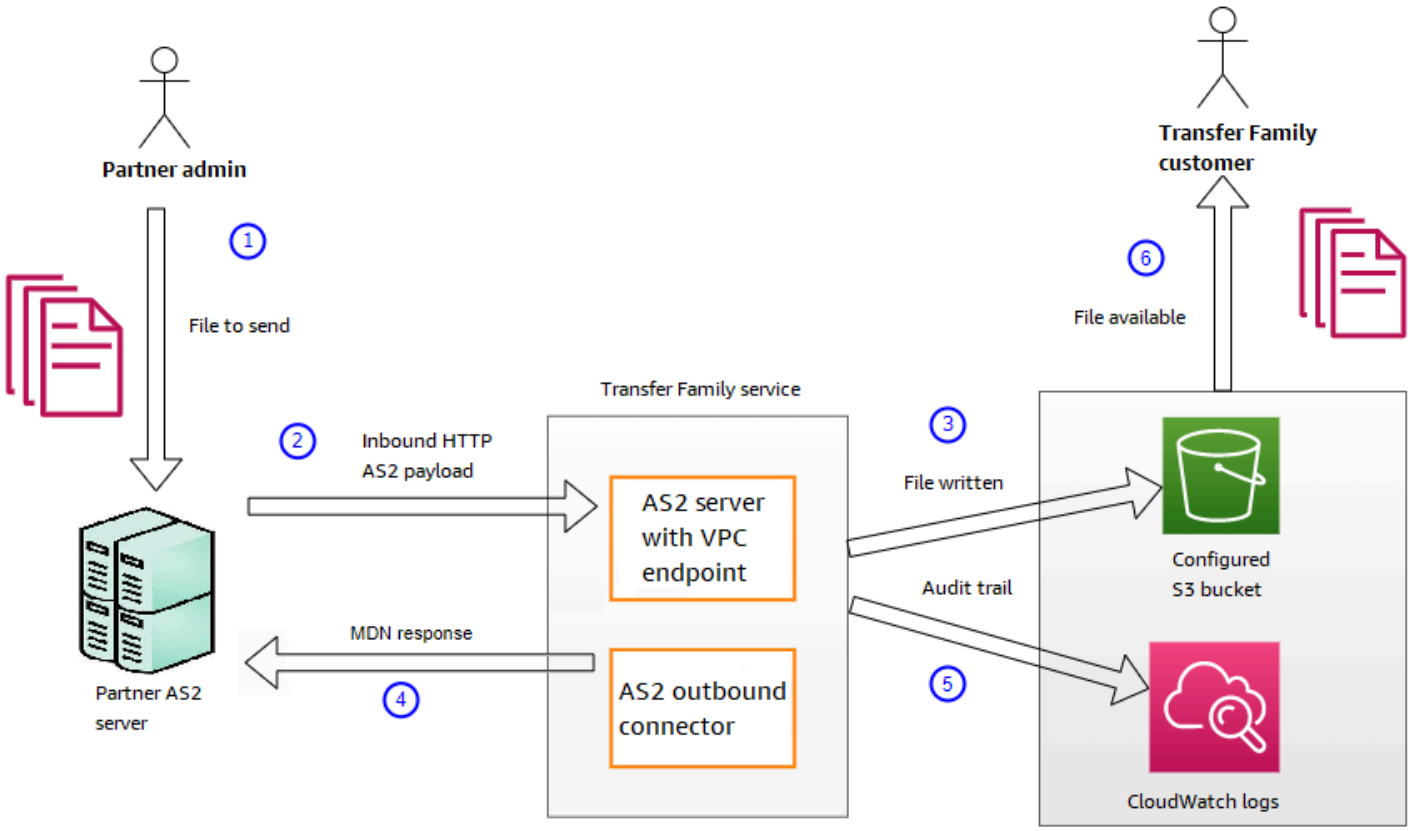
El procesamiento AS2 es compatible con muchos de los protocolos RFC 4130 y se centra en los casos de uso comunes y en la integración con las implementaciones de servidores compatibles con AS2 existentes. Para más información sobre las configuraciones compatibles, consulte Configuraciones AS2 admitidas.

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 X-Forwarded-Proto en el sitio web developer.mozilla.org.

Característica	Network Load Balancer (NLB)	Application Load Balancer (ALB)
Terminación de TLS/SSL	Soporta la terminación de TLS/SSL	Soporta la terminación de TLS/SSL
TLS mutuo (mTLS)	Transfer Family no admite actualmente 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 de oyente seguro, elija su certificado en el área de Certificados SSL/TLS 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 (NLB) 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, crea 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 certificado SSL/TLS 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 TCP 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 utilice 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 Protocol, seleccione TCP.
   - 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 Comprobación de estado, elija TCP para el protocolo de comprobación de estado.
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 "/DOC-EXAMPLE-SOURCE-BUCKET/myfile1.txt" "/DOC-EXAMPLE-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.

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, `/DOC-EXAMPLE-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, `/DOC-EXAMPLE-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, `/DOC-EXAMPLE-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 `start-file-transfer` AWS CLI comando de la `StartFileTransfer` API. Por ejemplo:

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-BUCKET/AS2-folder/
file-to-send.txt
```

Si ejecutas este comando, los archivos MDN y JSON se guardan en `/DOC-EXAMPLE-BUCKET/AS2-folder/processed` (si las transferencias se realizan correctamente) o `/DOC-EXAMPLE-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.j`
  - MDN: `ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.m`

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	Descripción	¿Se ha completado el procesamiento?
PROCESAMIENTO	El mensaje está en proceso de convertirse a su formato final. Por ejemplo, los pasos	No

Código	Descripción	¿Se ha completado el procesamiento?
	de descompresión y descifrado 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",
  "mesage-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": "/DOC-EXAMPLE-BUCKET/as2testcell0000/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": "/testbucket-4c1tq6ohjt9y/as2IntegCell0002/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-5Ab6bTfCO.dat sent from MyCompany
 to PartnerA",
```

```
  "client-ip": "10.0.109.105",
  "requester-file-name": "openAs2TestInboundAsyncMdn-necco-5Ab6bTfCO.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-5Ab6bTfCO.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"
}
```


Monitorización del uso de AS2

Puede supervisar la actividad de AS2 mediante Amazon CloudWatch yAWS CloudTrail. Para ver otras métricas del servidor Transfer Family, consulte Amazon CloudWatch inicia sesión para AWS Transfer Family.

métricas de AS2

Métrica	Descripción
`InboundMessage`	El número total de mensajes AS2 recibidos correctamente de un socio comercial. 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. 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

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	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
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 función de acceso tiene los permisos necesarios. • Ruta de archivo no válida *`send-file-path`* • No se pudieron obtener las credenciales con ErrorCode: código de *`error`*	Se produce al gestionar una solicitud `StartFileTransfer` 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 ruta incluye caracteres que no son válidos. También ocurre si Transfer Family no asume la función de acceso o la función 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.

Código	Error	Descripción y resolución
		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 `StartFileTransfer` . Además, asegúrese de que el rol proporciona acceso de lectura y escritura al directorio principal de los archivos que desea enviar con `StartFileTransfer` . 3. Si se utiliza una clave administrada por el cliente como secreta, 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 ID del mensaje.* 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 coinciden te.	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 de SMIME se solicitó mediante un algoritmo no compatible con el ID: *`encryption-ID`* .	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 compatibl e 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: *`local-profile-ID`*.	Transfer Family está intentando 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 *`nombre del archivo`*.	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`	*`partner-URL`* devolvió el estado 400 para un mensaje con un ID=*`message-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.
`INSUFFICENT_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`	1. Hay un problema con el encabezado de un mensaje. 2. No se han podido analizar el JSON secreto. El JSON secreto no coincidía con el formato esperado. 3. Secret debe ser una cadena JSON. 4. 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. 1. 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. 2. 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. 3. Asegúrese de que el secreto se proporciona como cadena y no como binario. 4. 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: *URL*	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_INDICATES_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_INDICATES_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_INDICATES_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 la firma o el cifrado en el conector para que se ajusten 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-check-failed
`PATH_NOT_FOUND`	No se pudo crear *`la ruta del archivo.`* del directorio. 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 `StartFileTransfer` contiene el nombre de un bucket existente.

Código	Error	Descripción y resolución
SEND_FILE_NOT_FOUND	Ruta del archivo: no se encontró la *ruta del archivo*.	Transfer Family no encuentra el archivo en la operación de envío de archivos. Compruebe que el directorio principal 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	El *server-ID* del 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.

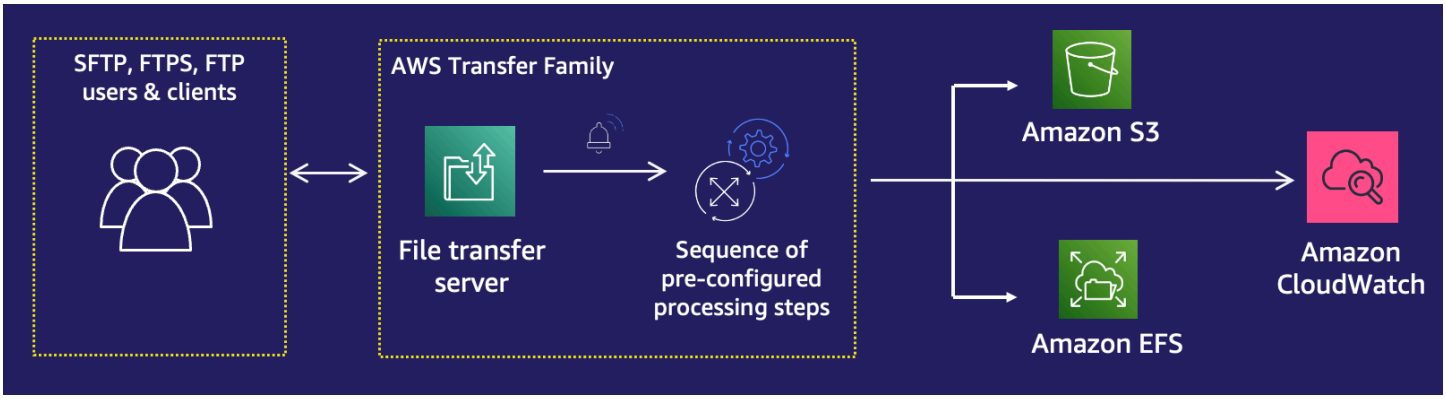
Código	Error	Descripción y resolución
`SIGNING_FAILED_NO_SIGNING_KEY_FOUND`	No se ha encontrado ningún certificado para el perfil: *`local-profile-ID`* .	Se está intentando firmar un mensaje saliente, pero no se encuentra ningún certificado de firma para el perfil local. Opciones de resolución: • Asegúrese 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 pudo resolver el nombre de host *`hostname`*.	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 con el mensaje *`message-ID`* 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 ha encontrado ningún certificado público que coincidiera con la firma del mensaje en el perfil: *`partner-profile-ID`* . • No se pueden obtener certificados para un perfil inexistente: *`partner-profile-ID`* . • No se ha encontrado ningún certificado válido en el perfil: *`partner-profile-ID`* .	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.

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 función, puede cumplir de forma segura y rentable sus requisitos de conformidad para el intercambio de archivos business-to-business (B2B) mediante la coordinación de todos los pasos necesarios para el procesamiento de archivos. Además, se beneficia de la end-to-end auditoría y 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 administrado diferente en los archivos que se

hayan cargado solo parcialmente debido a una desconexión prematura de la sesión. La gestión de excepciones integrada le ayuda a reaccionar rápidamente ante los resultados del procesamiento de archivos y, al mismo tiempo, le ofrece el control sobre cómo administrar 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 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 AWS Transfer Family puntos de enlace SFTP/FTPS administrados y Amazon Cognito y DynamoDB para la administración 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.

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 AWS Management Console, 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.
- Pasos de gestión de excepciones: 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 https://console.aws.amazon.com/transfer/. AWS Transfer Family
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.

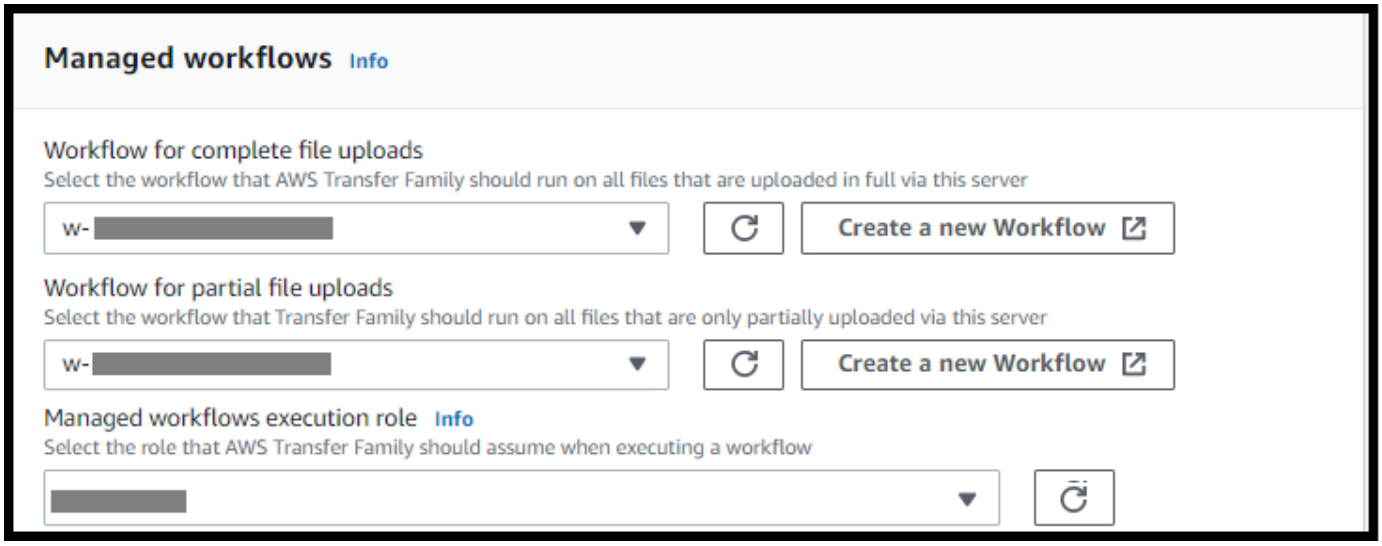
   > **Note**
   >
   > De forma predeterminada, los servidores no tienen ningún flujo de trabajo asociado. Utilice la sección Detalles adicionales para asociar un flujo de trabajo al servidor seleccionado.

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 (Guardar).



> **Note**
>
> Si ya no desea que un flujo de trabajo esté asociado al servidor, puede eliminar la asociación. Para obtener más detalles, 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 /DOC-EXAMPLE-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

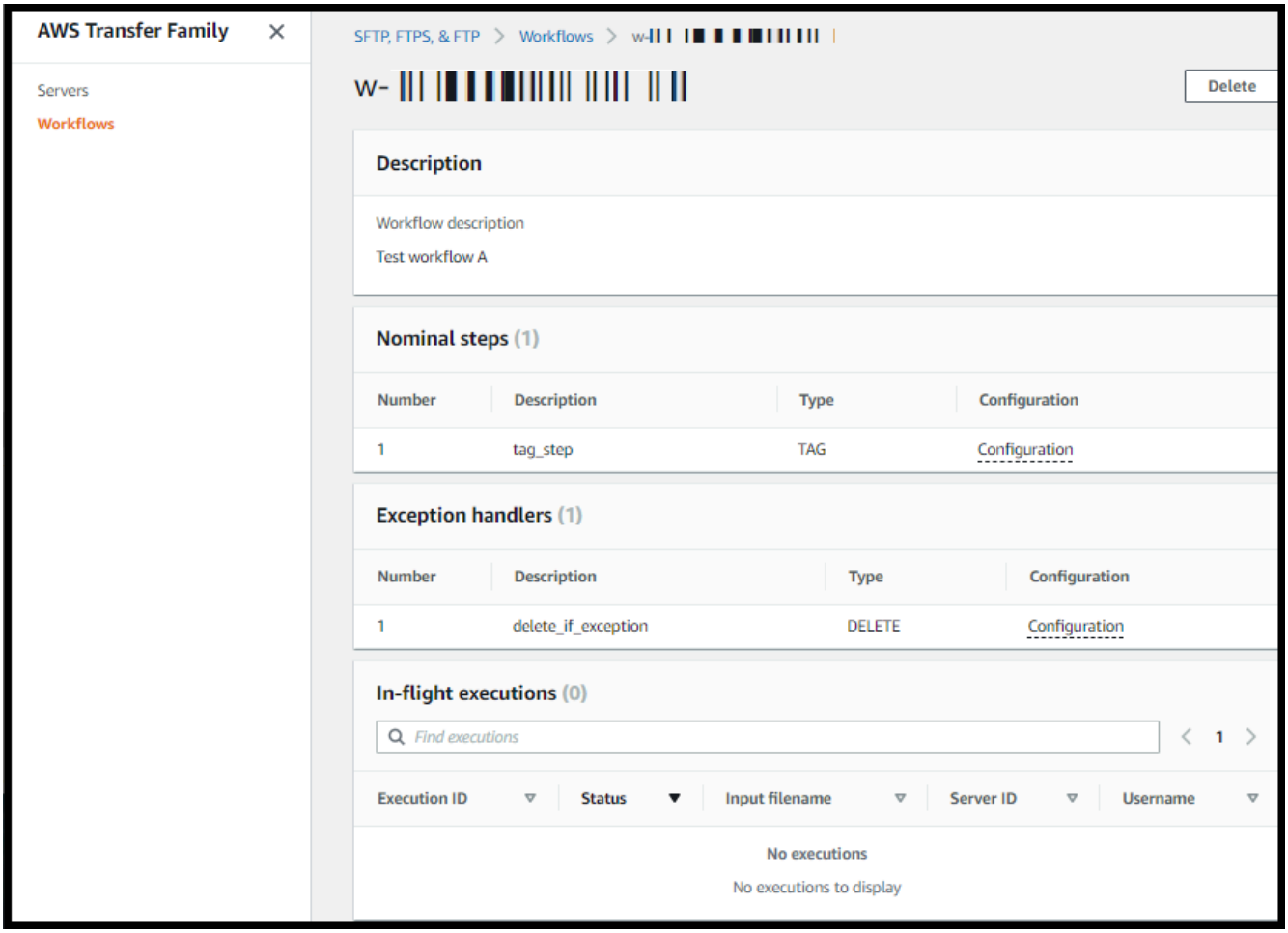
Puede ver los detalles de los flujos de trabajo creados anteriormente o de las ejecuciones de los flujos de trabajo. Para ver estos detalles, puede usar la consola o el AWS Command Line Interface (AWS CLI).

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.



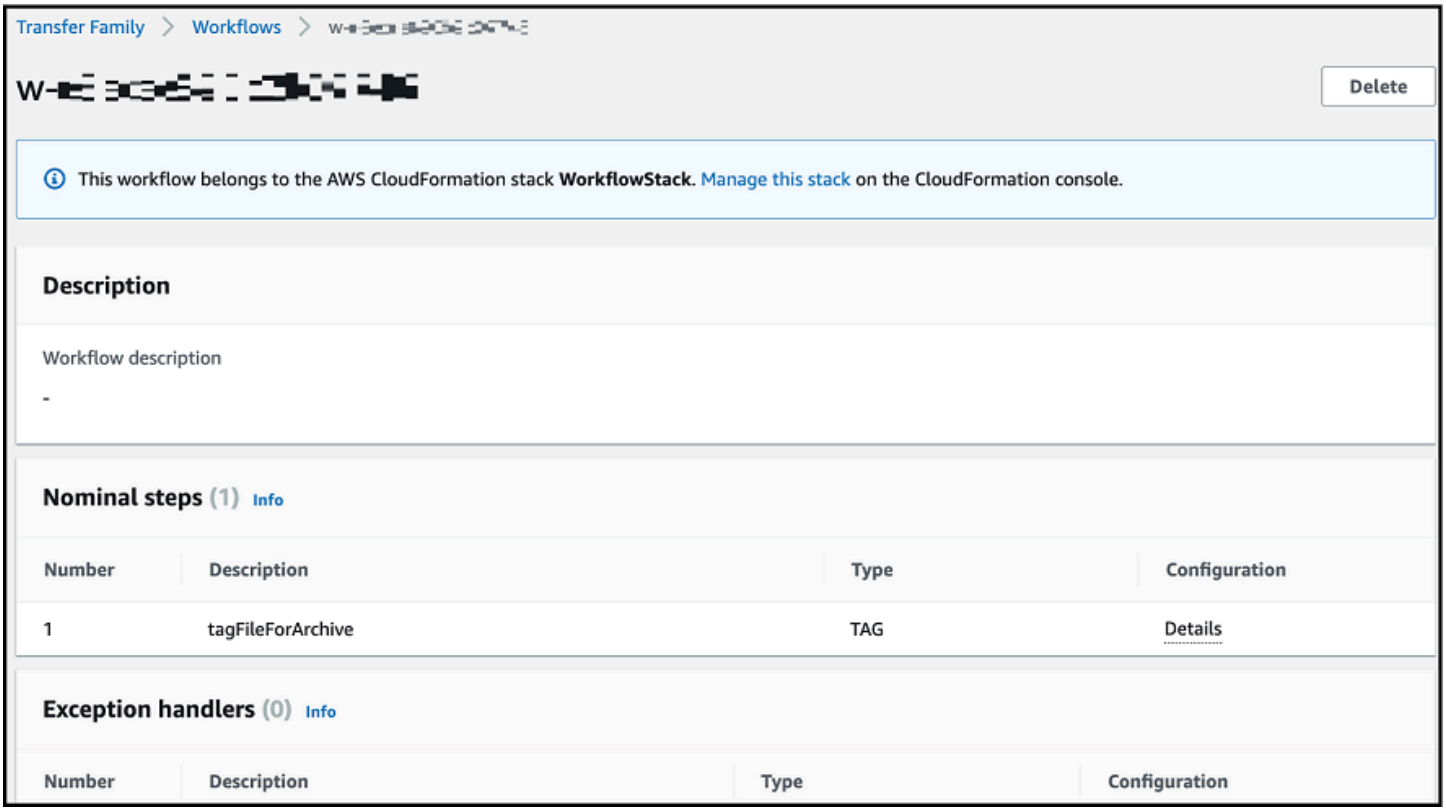
CLI

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": "DOC-EXAMPLE-BUCKET",
                        "Key": "home/shared_files/"
                    }
                }
                }
            }
        ],
        "OnException": {}
    }
}
```

Si el flujo de trabajo se creó como parte de una AWS CloudFormation pila, puede gestionarlo mediante la AWS CloudFormation consola (https://console.aws.amazon.com/cloudformation).



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

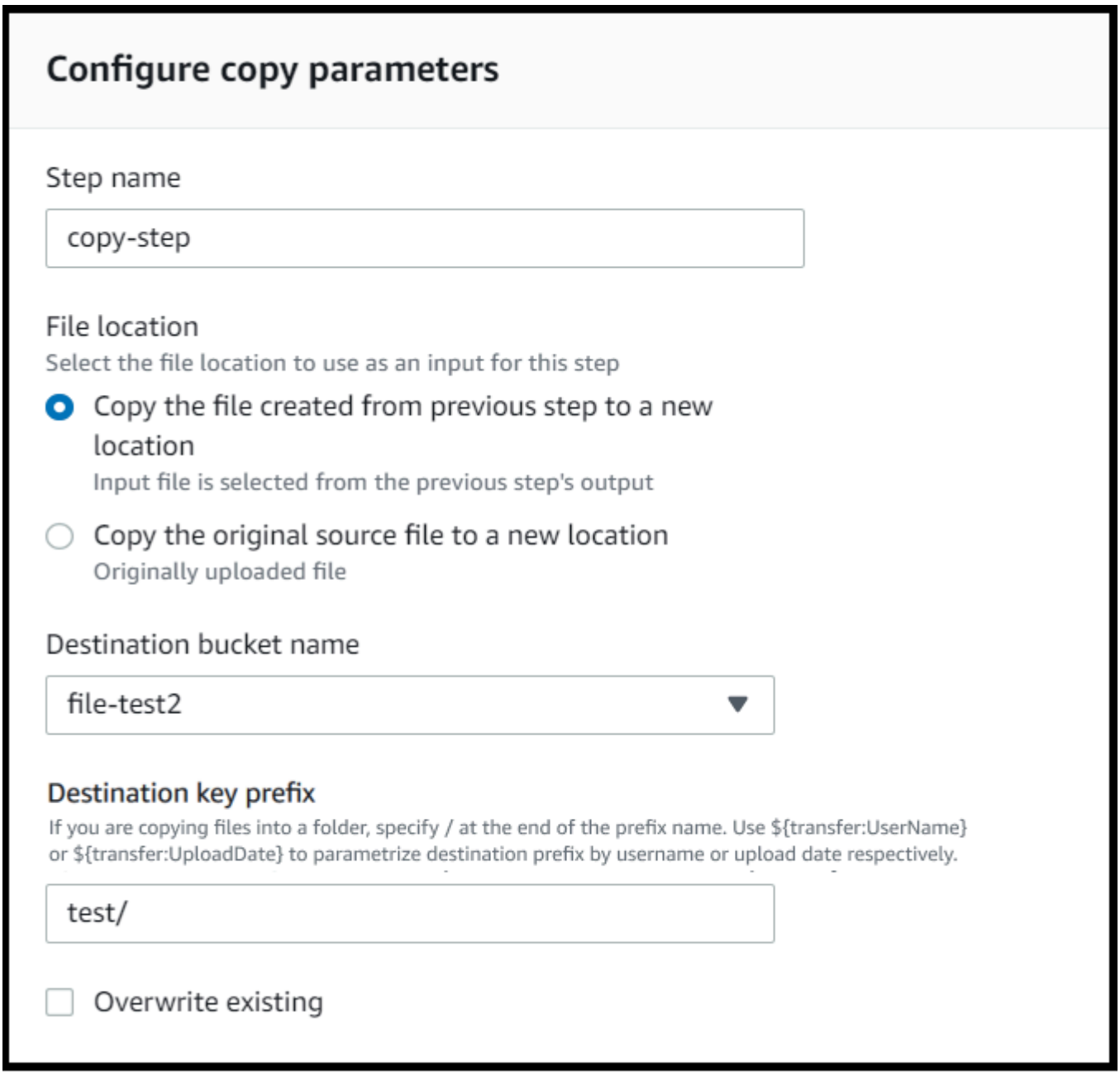
- Copiar archivo
- Descifrar el archivo
- Etiquetado de archivos
- Eliminar archivo
- Variables con nombre para los flujos de trabajo
- Ejemplo de flujo de trabajo de etiquetado y eliminación

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.

El siguiente paso para copiar archivos copia los archivos en la carpeta `test` del bucket de destino `file-test`.

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, consulte Ejemplo de flujo de trabajo de etiquetado y eliminación.



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.

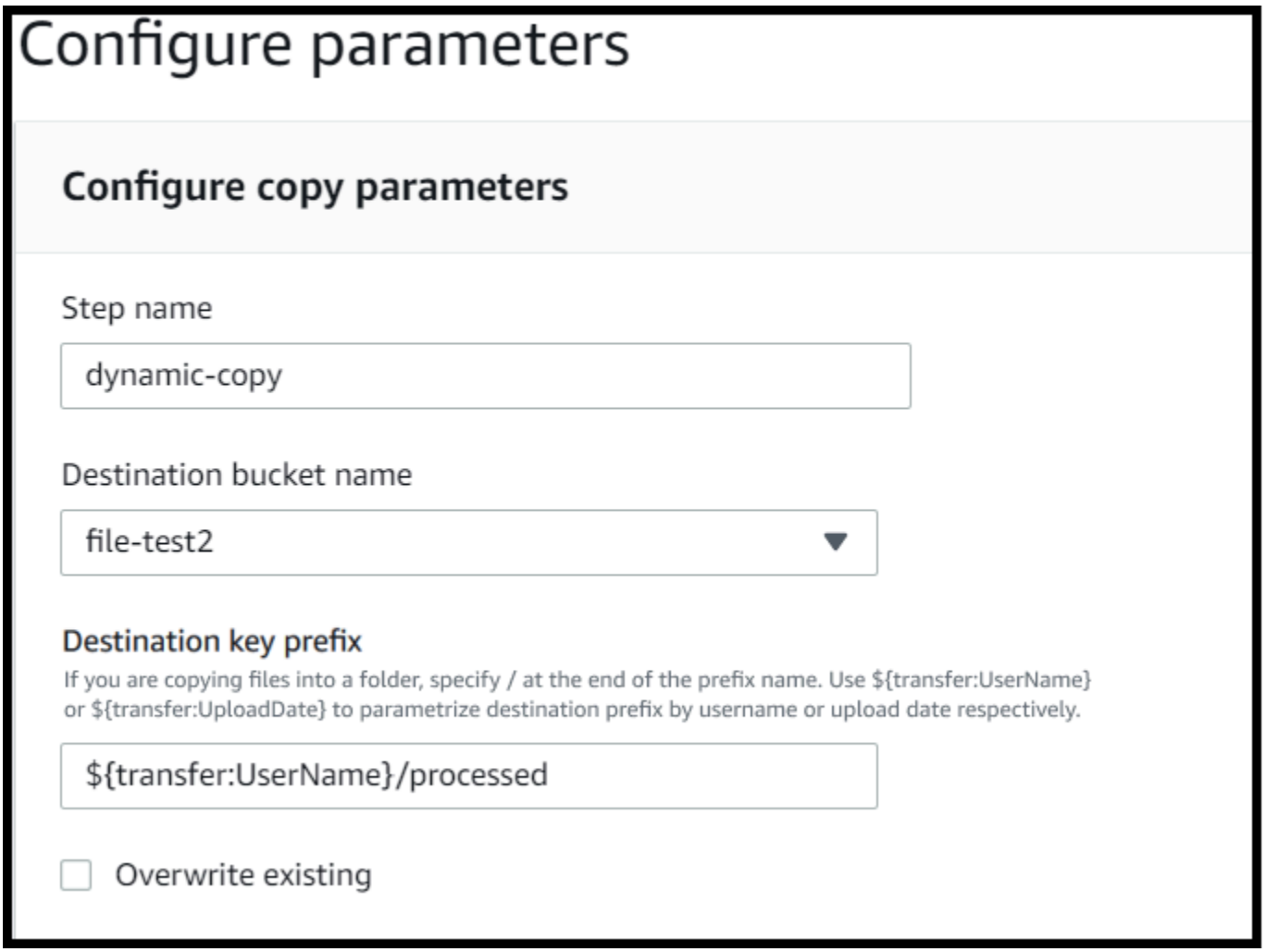
Por ejemplo, si el valor de la clave es `test/`, los archivos cargados se copian en la carpeta `test`. Si el valor de la clave es `test/today` (y la opción Sobrescribir existente está seleccionada), todos los archivos que cargue se copiarán en un archivo llamado `today` en la carpeta `test` y cada archivo 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.

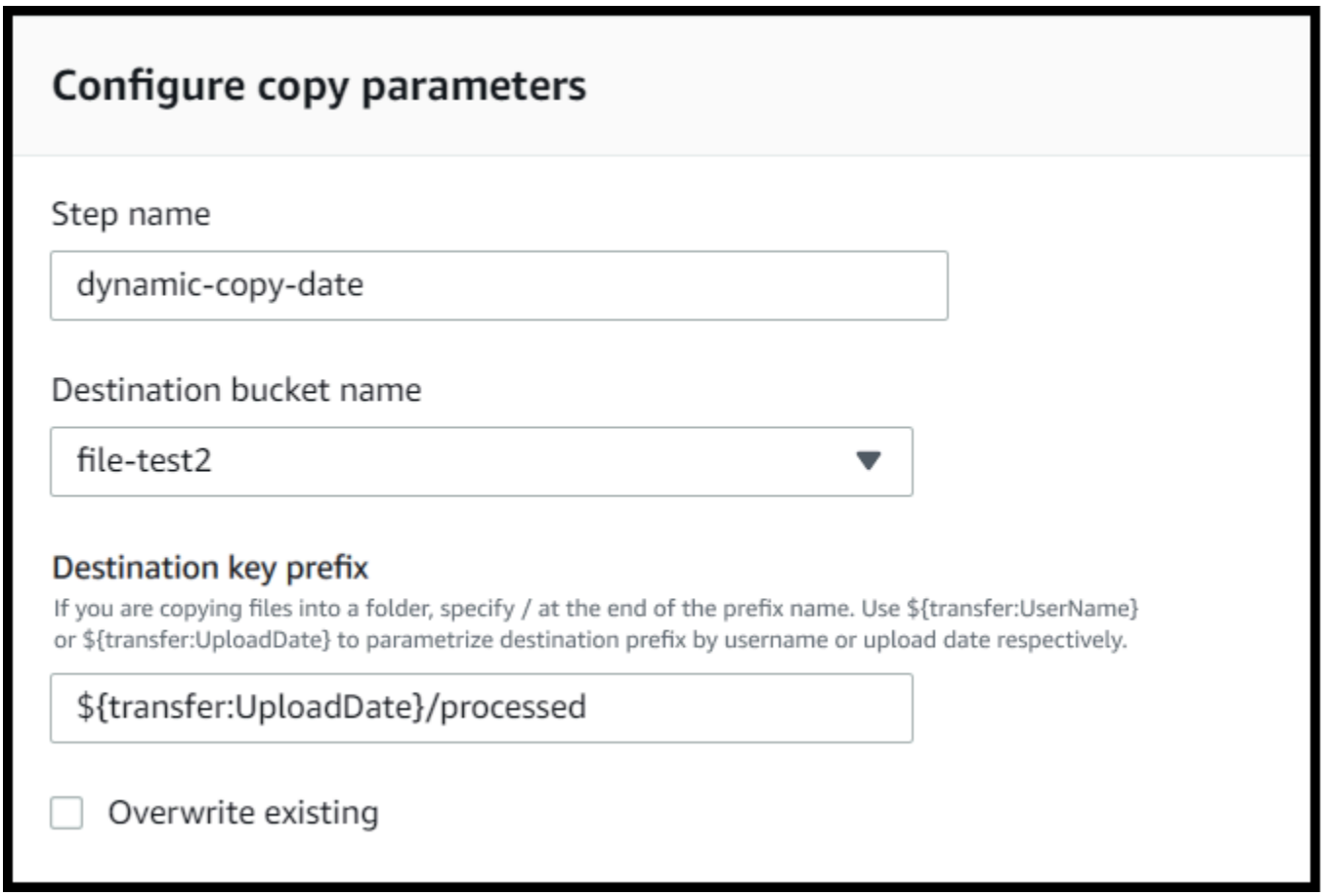
Utilizar una variable con nombre en el paso de copiar un archivo

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 `file-test2/richard-roe/processed/`. En el siguiente ejemplo, si el usuario `mary-major` carga un archivo, queda copiado en la carpeta `file-test2/mary-major/processed/`.



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 `file-test2/2022-02-01/processed/`.



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/`.
- Puede establecer el prefijo de la clave de destino en **`folder/${transfer:UserName}-${transfer:UploadDate}/`** para concatenar las dos variables, 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:::destination-bucket-name"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*"
        }
```

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

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.

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 para poder almacenar sus claves PGP AWS Secrets Manager con el nombre secreto correcto.
2. Guarde su clave PGP AWS Secrets Manager con el nombre secreto requerido. Para obtener más detalles, 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 Precios de AWS Secrets Manager.

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
   ```

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.

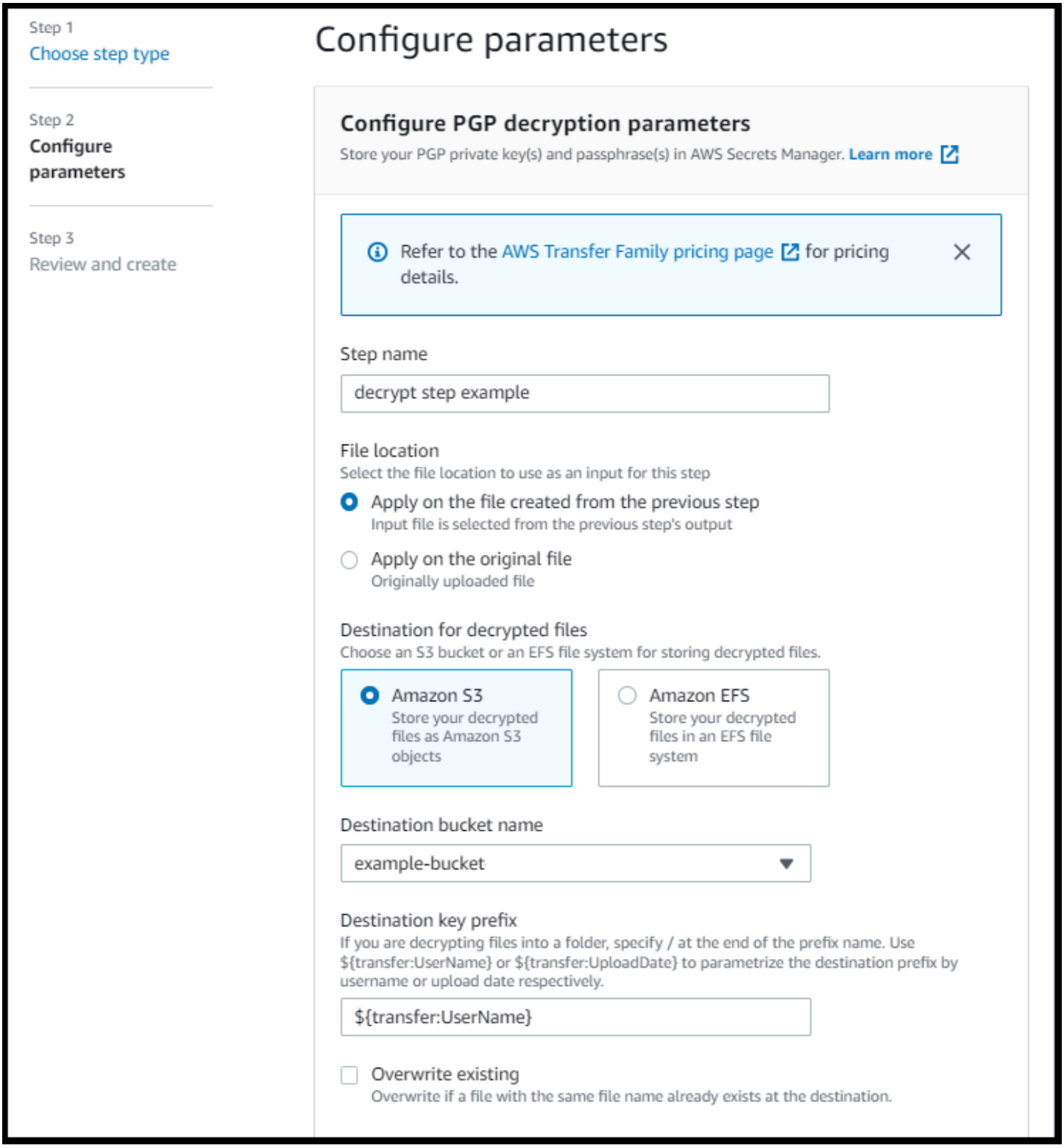
- Destino de los archivos descifrados: elija un bucket de Amazon S3 o un sistema de archivos Amazon EFS como destino del archivo descifrado.
  - Si elige Amazon S3, debe proporcionar un nombre de bucket de destino y un prefijo de clave. Para establecer los parámetros del prefijo de la clave de destino 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
decrypt step example
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
example-bucket
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.
${transfer:UserName}
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:::destination-bucket-name"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*"
        },
        {
            "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.

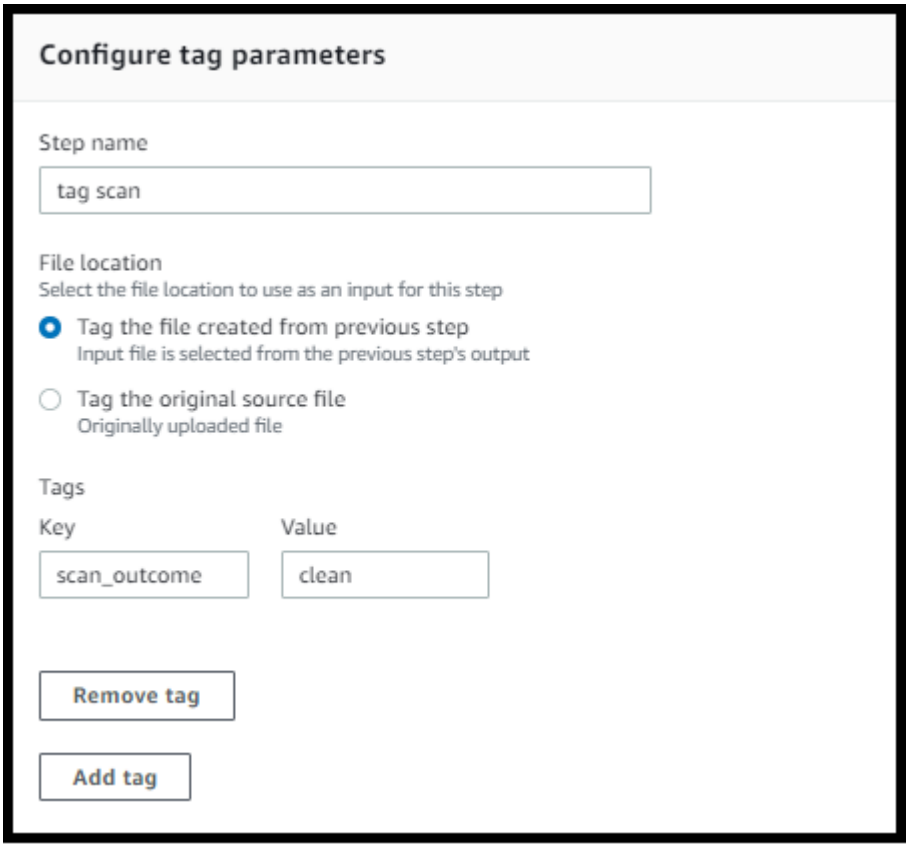
Si sus archivos de Amazon S3 tienen etiquetas, debe añadir uno o dos permisos a su política de IAM.

- 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.



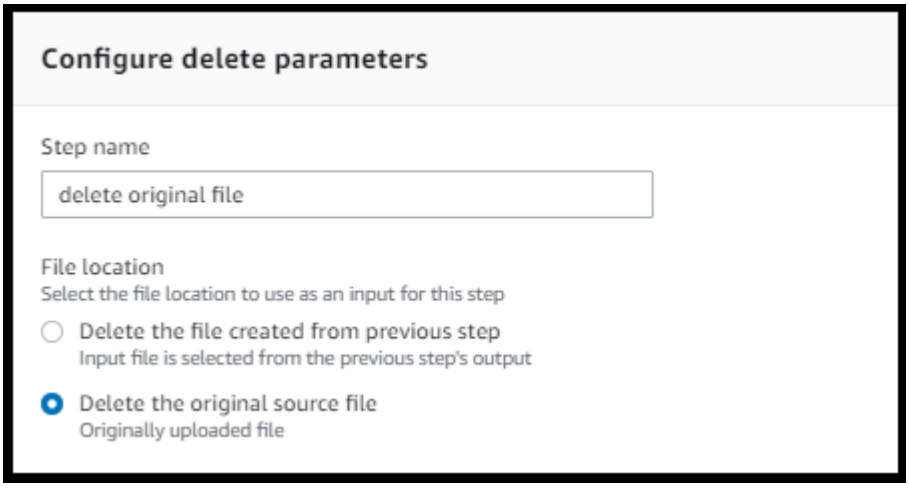
Para permitir que un paso de etiquetado se realice correctamente, asegúrese de que el rol de ejecución de su flujo de trabajo contenga los siguientes permisos.

```
{
            "Sid": "Tag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-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.



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

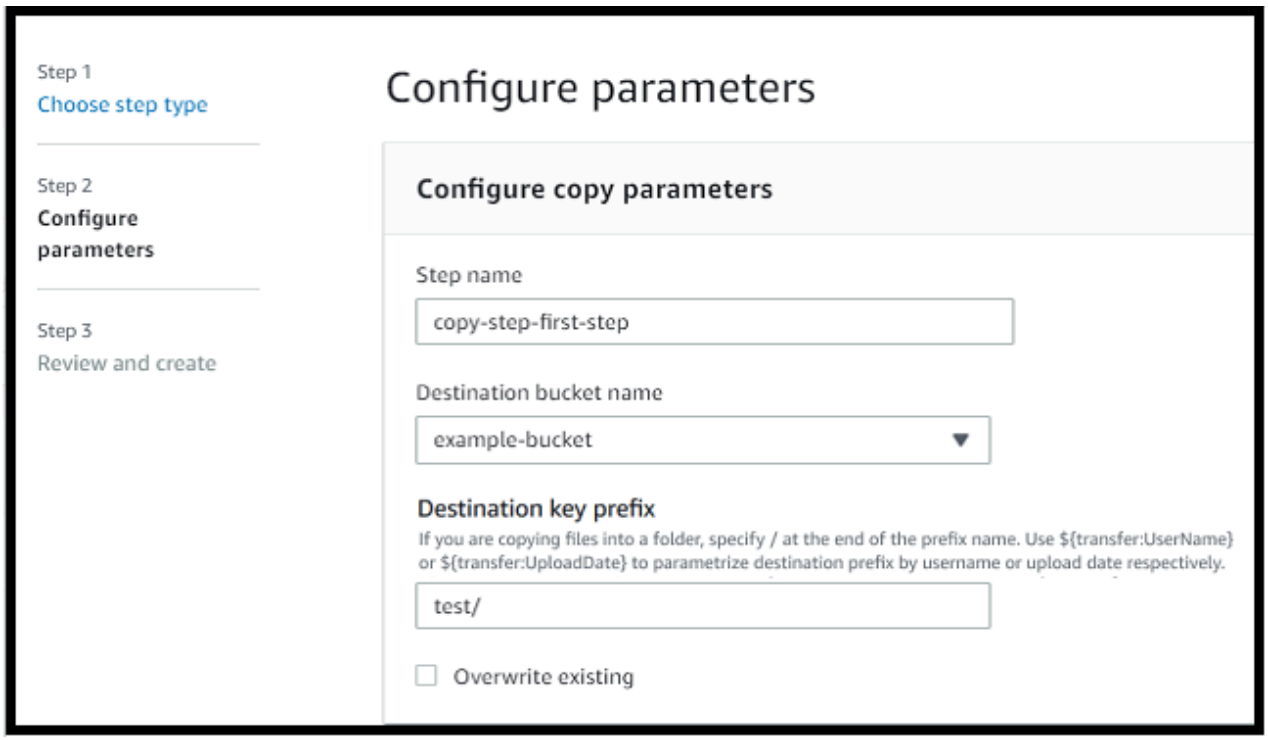
El siguiente ejemplo ilustra un flujo de trabajo que etiqueta los archivos entrantes que deben ser procesados por una aplicación secundaria, como una plataforma de análisis de datos. Tras etiquetar el archivo entrante, el flujo de trabajo elimina el archivo cargado originalmente para ahorrar costos de almacenamiento.

Console

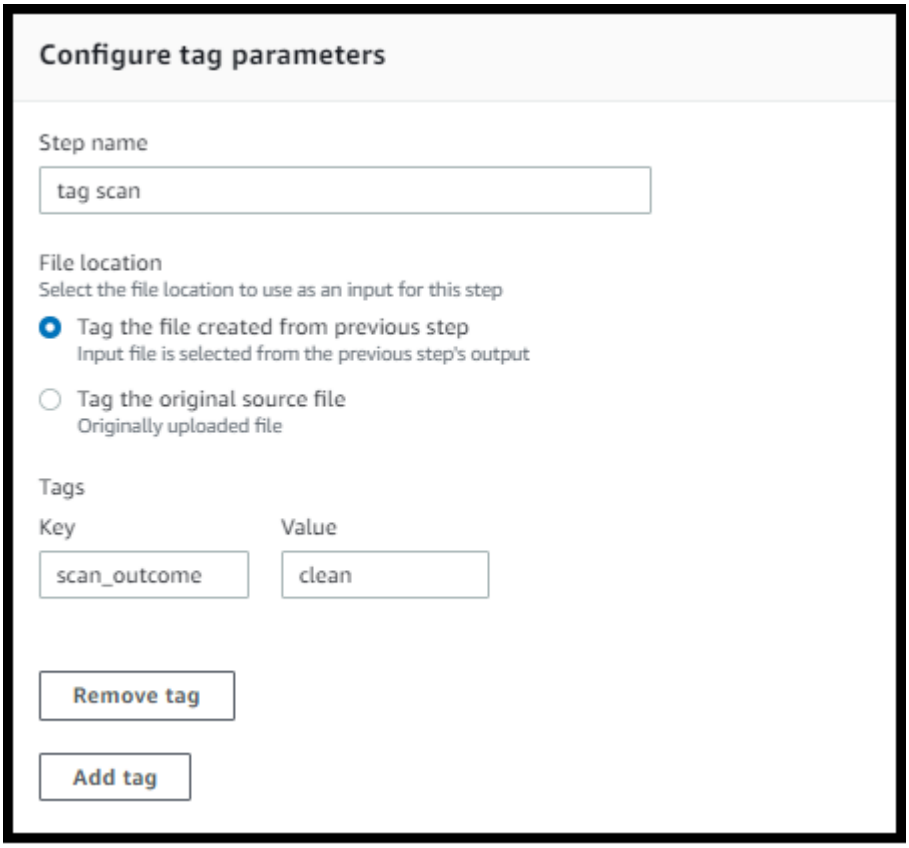
Ejemplo de etiquetado y flujos de trabajo

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.



   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 Etiquete 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.



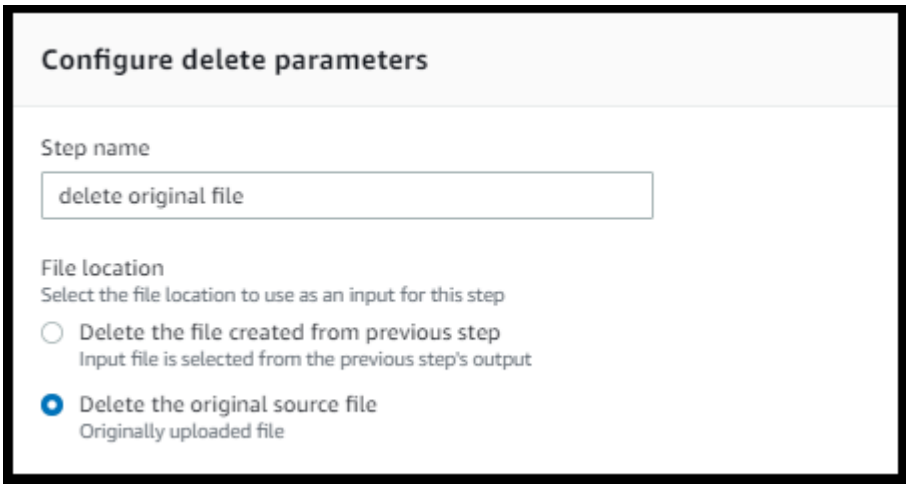
f. Seleccione Siguiente y, a continuación, revise los detalles del paso.

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.



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": "DOC-EXAMPLE-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
```

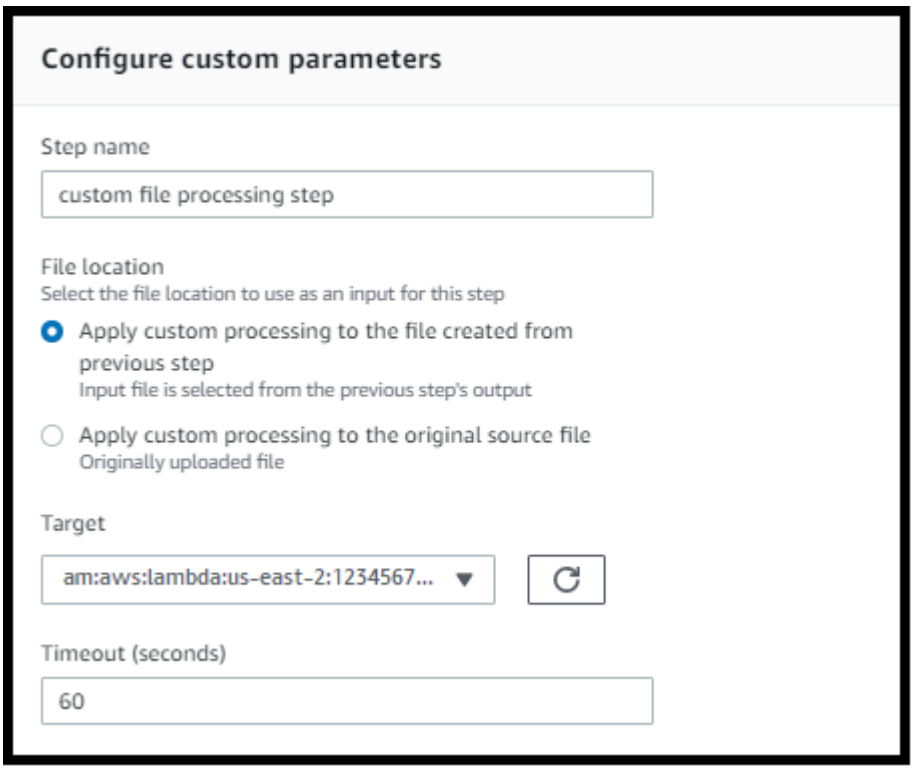
```
  --workflow-details '{"OnUpload":[{ "WorkflowId": "workflow-
ID","ExecutionRole": "execution-role-ARN"}]}'
```

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.



> **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 cargar un archivo.

Con un paso de flujo de trabajo personalizado, debe configurar la función Lambda para llamar a la operación de la SendWorkflowStepStateAPI. `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 archivo procesado por Lambda 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 cargar un 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": "DOC-EXAMPLE-BUCKET",
        "key": "path/to/mykey",
        "eTag": "d8e8fca2dc0f896fd7cb4cb0031ba249",
        "versionId": null
    }
}
```

Custom step that uses an Amazon EFS domain

```
{
    "token": "MTg0N2Y3N2UtNWI5Ny00ZmZlLTk5YTgtZTU3YzViYjllNmZm",
    "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 SendWorkflowStepStateAPI para devolver el estado al flujo de trabajo del pasoSUCCESS, 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 asóciela 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:::DOC-EXAMPLE-BUCKET"
            ]
        },
        {
            "Sid": "AllObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        },
        {
            "Sid": "GetObjectVersion",
            "Effect": "Allow",
            "Action": "s3:GetObjectVersion",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        },
        {
            "Sid": "Custom",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:region:account-id:function:function-name"
            ]
        },
        {
            "Sid": "Tag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-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 “Prevención de la sustitución confusa entre servicios”.

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:::source-bucket-name/*"
        },
        {
            "Sid": "CopyWrite",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectTagging"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*"
        },
        {
            "Sid": "CopyList",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::source-bucket-name",
                "arn:aws:s3:::destination-bucket-name"
            ]
        },
        {
            "Sid": "Tag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*",
            "Condition": {
                "StringEquals": {
                    "s3:RequestObjectTag/Archive": "yes"
                }
            }
        },
        {
            "Sid": "ListBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::destination-bucket-name"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
```

```
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::destination-bucket-name/*"
        },
        {
            "Sid": "Decrypt",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:region:account-ID: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:region:account-id:function:function-name"
            ]
        }
    ]
}
```

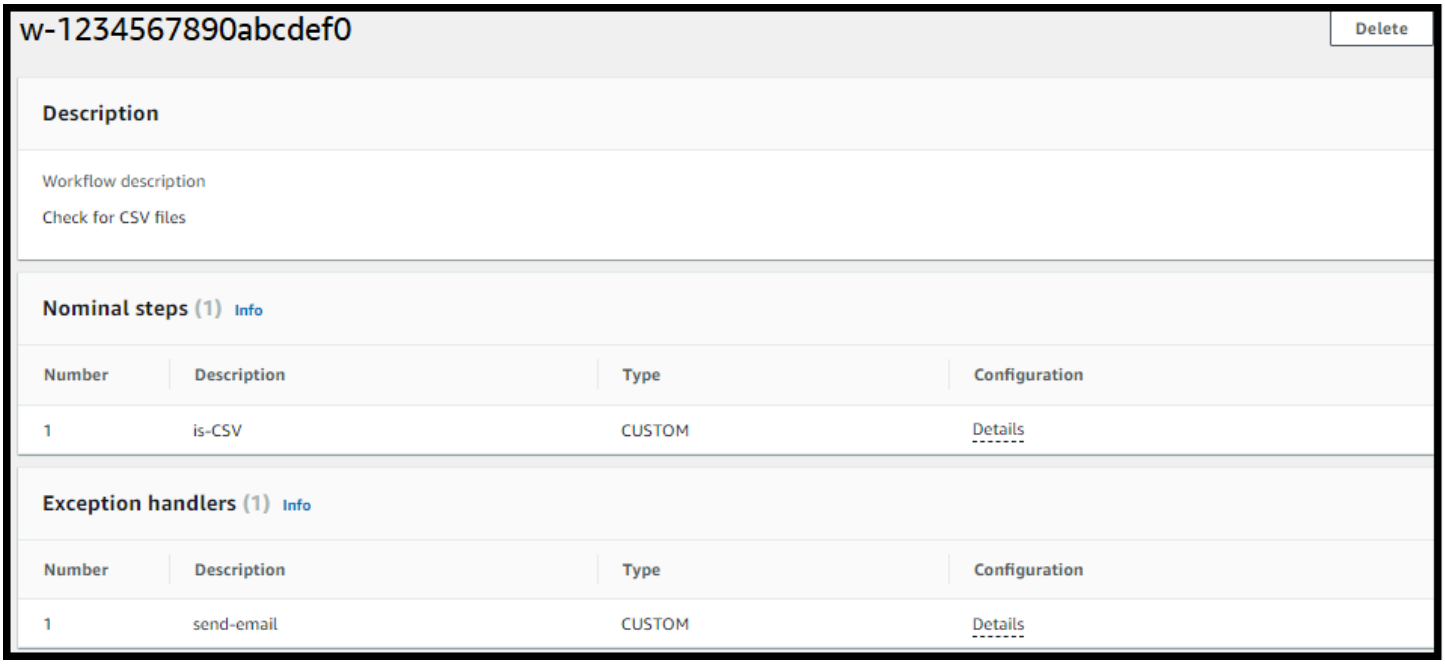
Gestión de excepciones para un flujo de trabajo

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”.



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": "DOC-EXAMPLE-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":"DOC-EXAMPLE-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 enUso de CloudWatch métricas para Transfer Family.

Creación de un flujo de trabajo a partir de una plantilla

Puede implementar una AWS 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 AWS CloudFormation pila que cree un AWS Transfer Family flujo de trabajo y un servidor

1. Abra la AWS 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 AWS 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

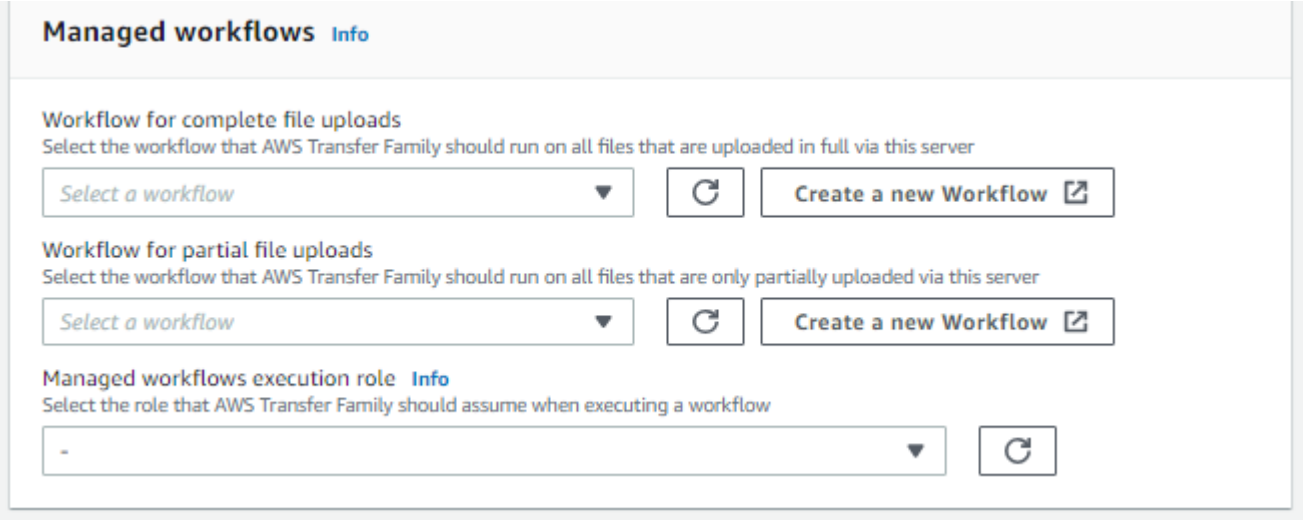
Eliminación de un flujo de trabajo de un servidor de Transfer Family

1. Abra la AWS Transfer Family consola en 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.



6. 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.

- No se admiten las AWS Lambda funciones entre cuentas y 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.

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 servidor compatible con SFTP.

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
- Editar detalles del servidor
- Administración de las claves de host de su servidor habilitado para SFTP
- 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.

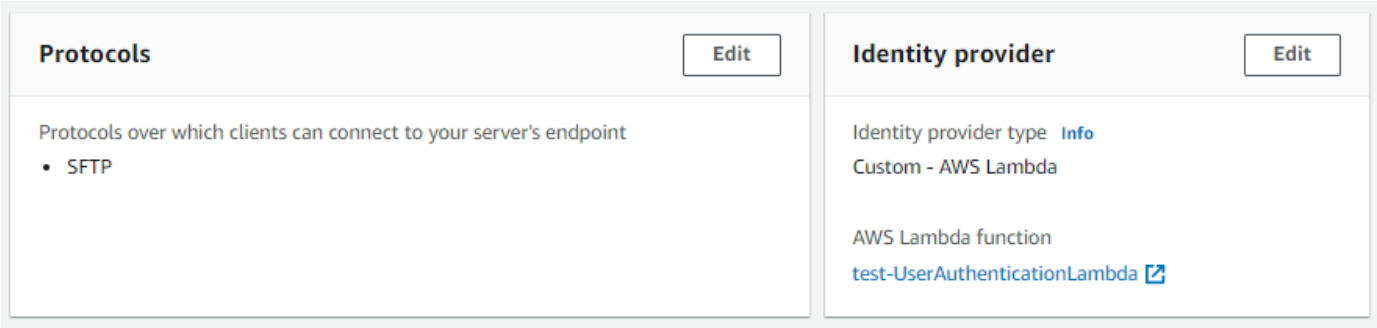
Vea los detalles de los servidores SFTP, FTPS y FTP

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

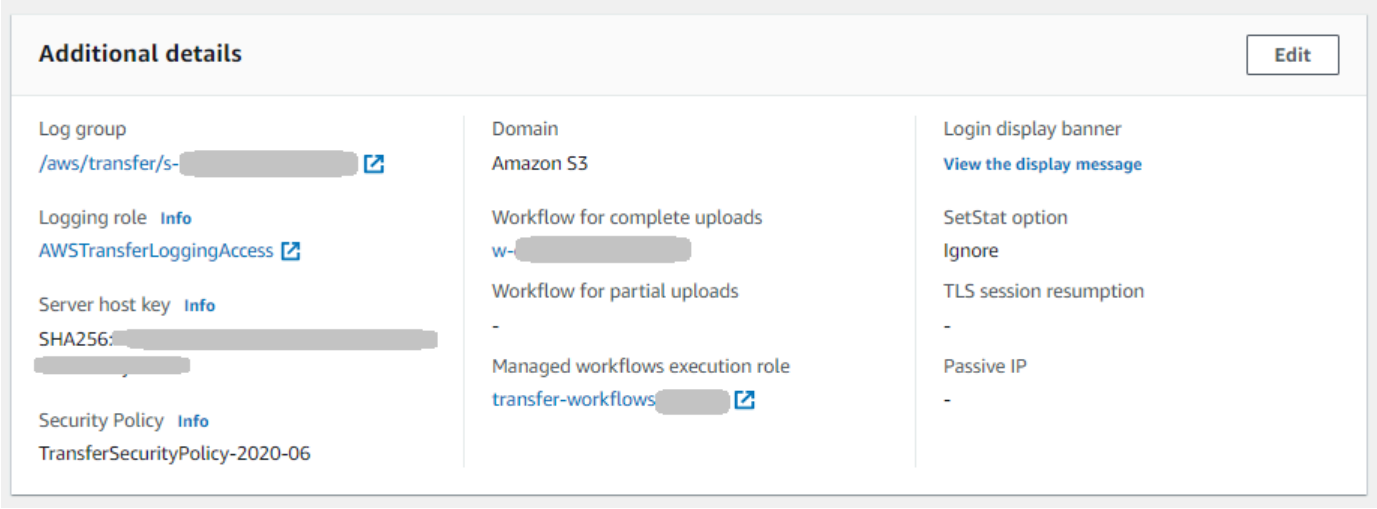
1. Abra la AWS Transfer Family consola en https://console.aws.amazon.com/transfer/.
2. En el panel de navegación, seleccione Servers (Servidores).
3. Elija el identificador en la columna ID de servidor para ver la página Detalles del servidor, que se muestra a continuación.

   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



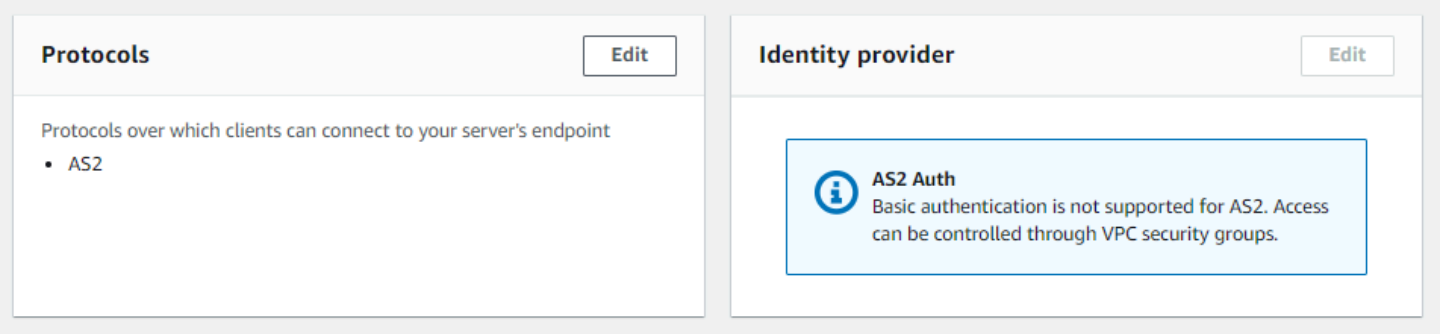
> **Note**
>
> Los valores de Descripción y Fecha de importación de la clave del host del servidor son nuevos a partir de septiembre de 2022. Estos valores se introdujeron para admitir la característica de claves de host múltiples. Esta característica requería la migración de

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.

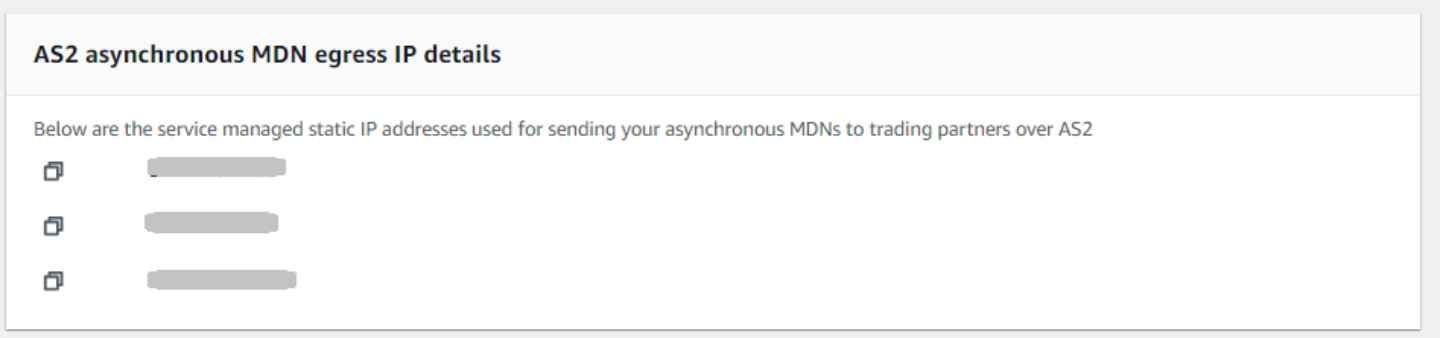


Vea los detalles del servidor AS2

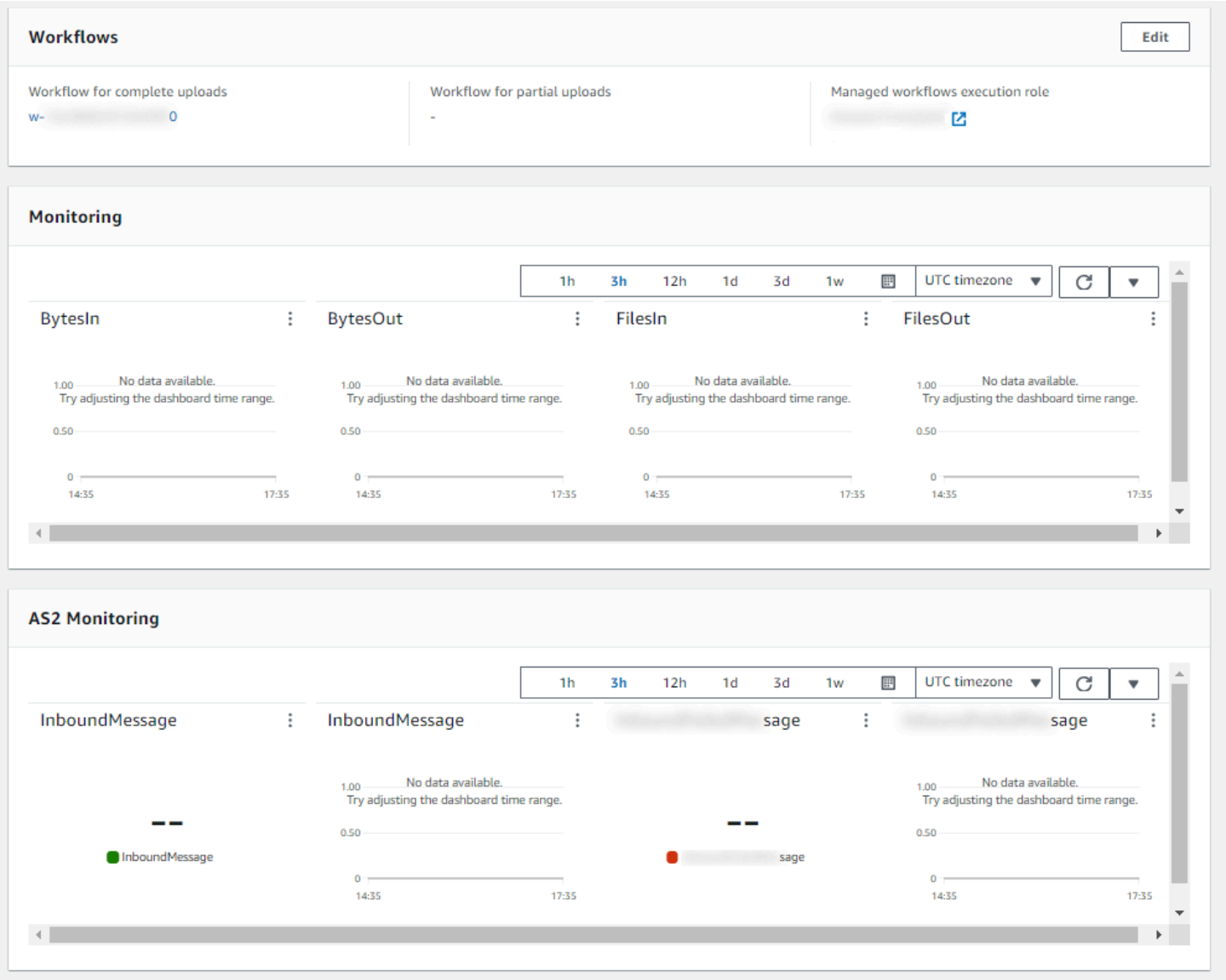
Puede encontrar una lista de detalles y propiedades de un AWS Transfer Family servidor individual. Las propiedades del servidor incluyen los protocolos, el estado y mucho más. En el caso de los servidores AS2, también puedes ver las direcciones IP de salida MDN asíncronas del AS2.



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.



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.



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 los parámetros personalizados del proveedor de identidad
- 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.

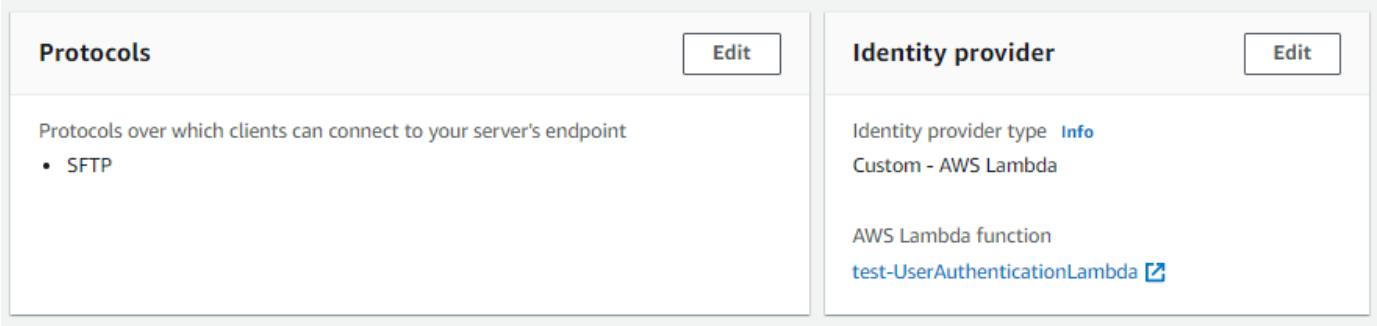
   Puede cambiar las propiedades del servidor en esta página al seleccionar Editar:

   - Para cambiar los protocolos, consulte Edite los protocolos de transferencia de archivos.
   - Para el proveedor de identidad, tenga en cuenta que una vez creado un servidor, no es posible cambiar el tipo de su proveedor de identidad. Para cambiar el proveedor de identidad debe eliminar servidor y crear uno nuevo con el proveedor de identidad que desee.

     > **Note**
     >
     > Si el servidor utiliza un proveedor de identidad personalizado, puede editar algunas propiedades. Para obtener más detalles, consulte Editar los parámetros personalizados del proveedor de identidad.

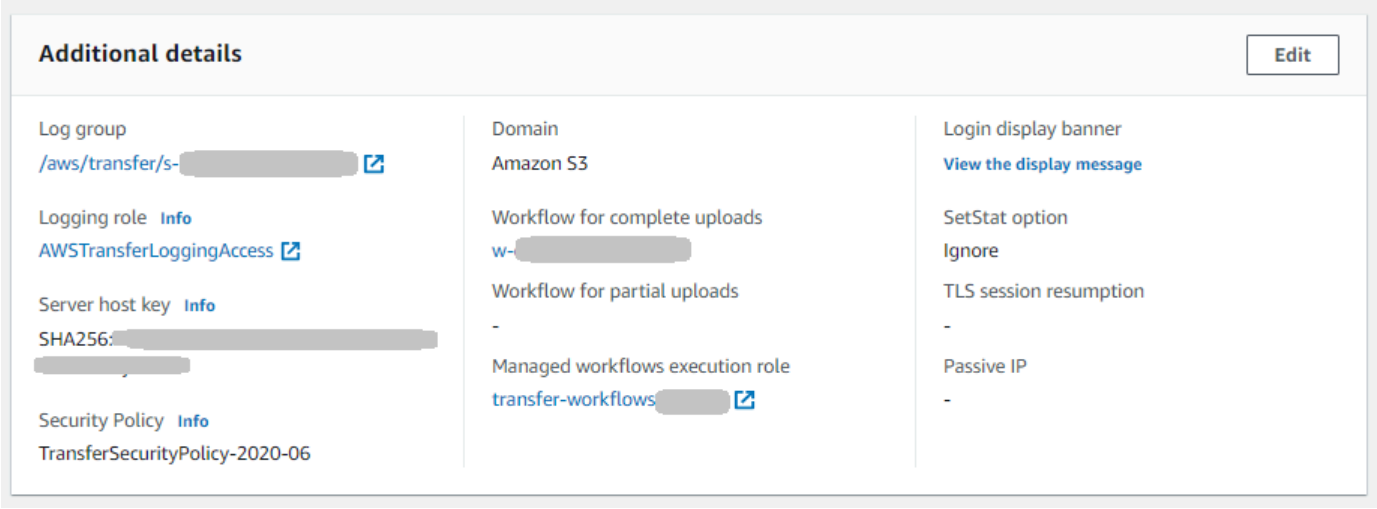
   - Para cambiar el tipo de punto de conexión o el nombre de host personalizado, consulte Editar el punto de conexión del servidor.
   - Para añadir un acuerdo, primero debe añadir AS2 como protocolo a su servidor. Para obtener más detalles, consulte Edite los protocolos de transferencia de archivos.
   - Para administrar las claves de host de su servidor, consulte Administración de las claves de host de su servidor habilitado para SFTP.
   - 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 Administración de las claves de host de su servidor habilitado para SFTP.

  - 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 ProtocolDetailstema.
  - 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 ProtocolDetailstema.
  - 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 ProtocolDetailstema.
- 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.



> **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.



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 Cree un servidor compatible con SFTP.

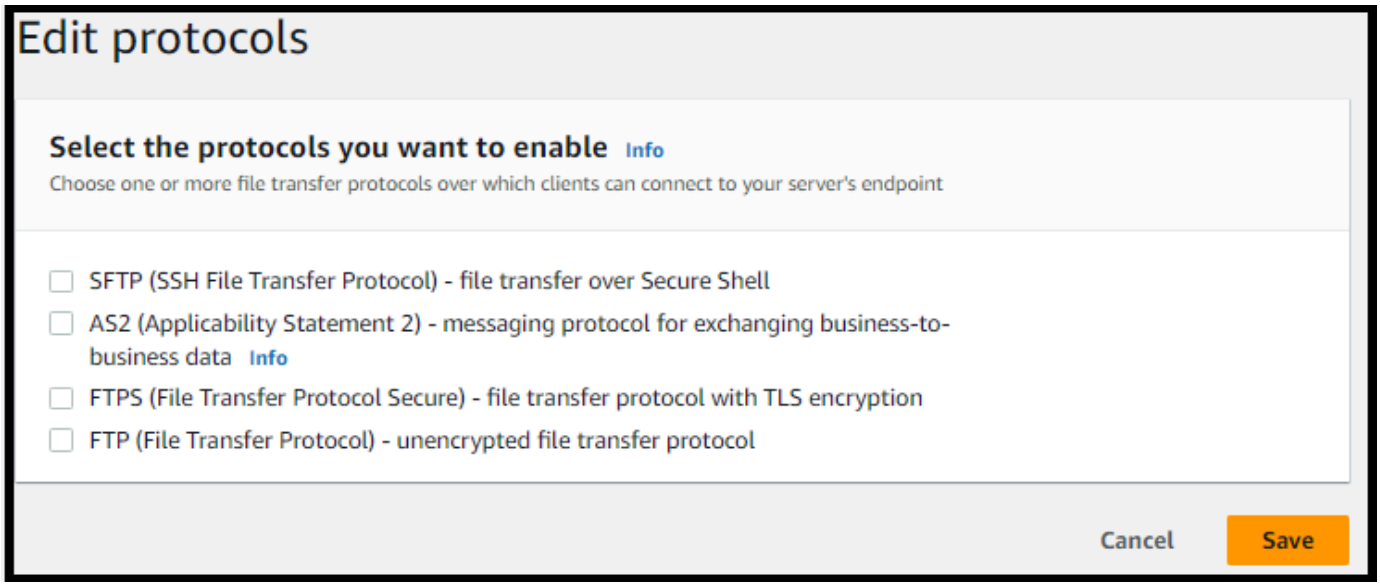
- Protocolo seguro de File Transfer (FTPS): transferencia de archivos con cifrado TLS

  Para obtener más información acerca de FTP, consulte Cree un servidor compatible con FTPS.

- Protocolo de File Transfer (FTP): transferencia de archivos sin cifrado

  Para obtener más información acerca de FTPS, consulte Cree un servidor compatible con FTP.

> **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.



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)

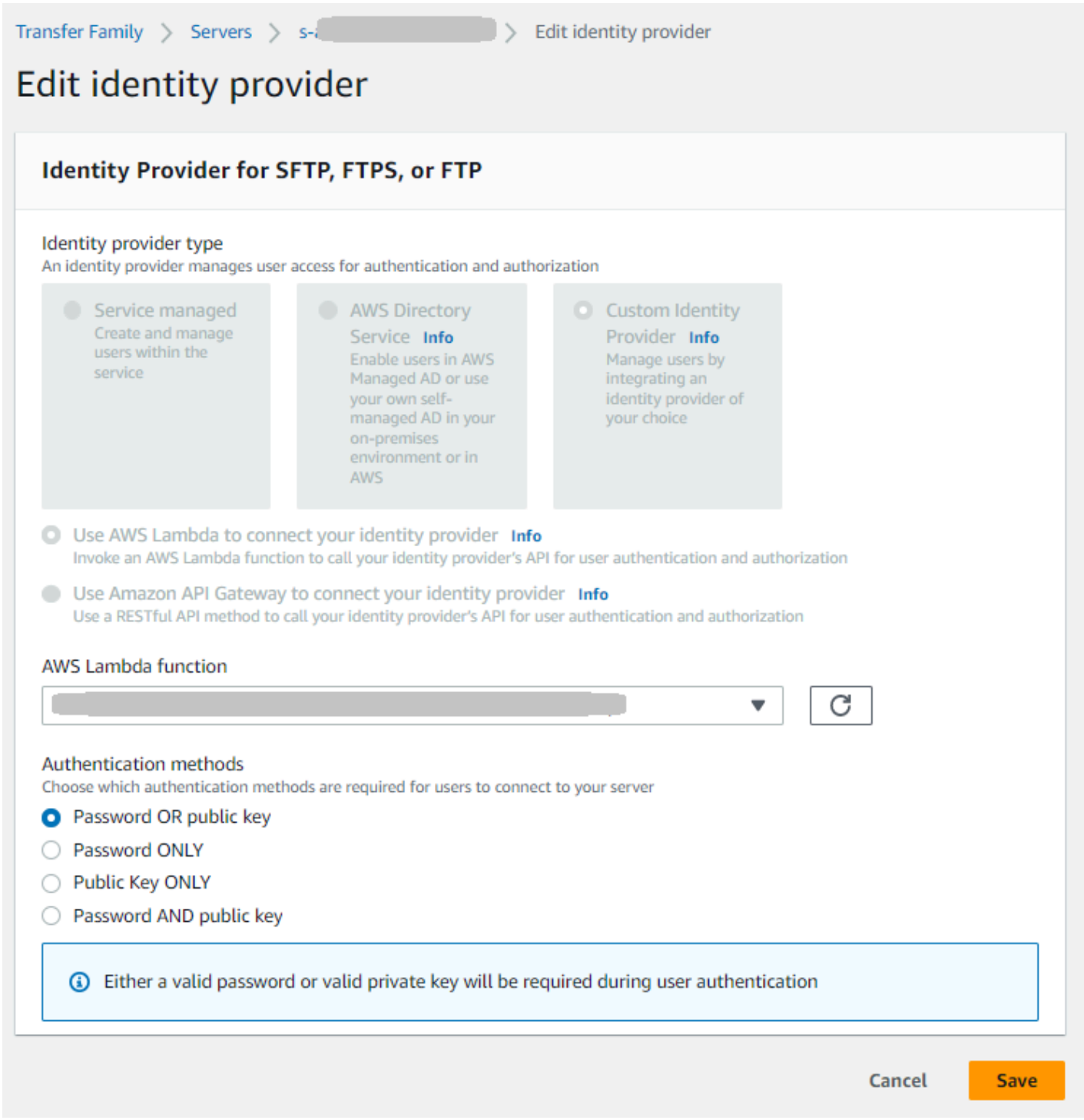
> **Note**
>
> El certificado debe ser un certificado SSL/TLS X.509 versión 3 válido con el FQDN o la dirección IP especificados y contener información sobre el emisor.

3. Seleccione Guardar. Regresará a la página de Detalles del servidor.

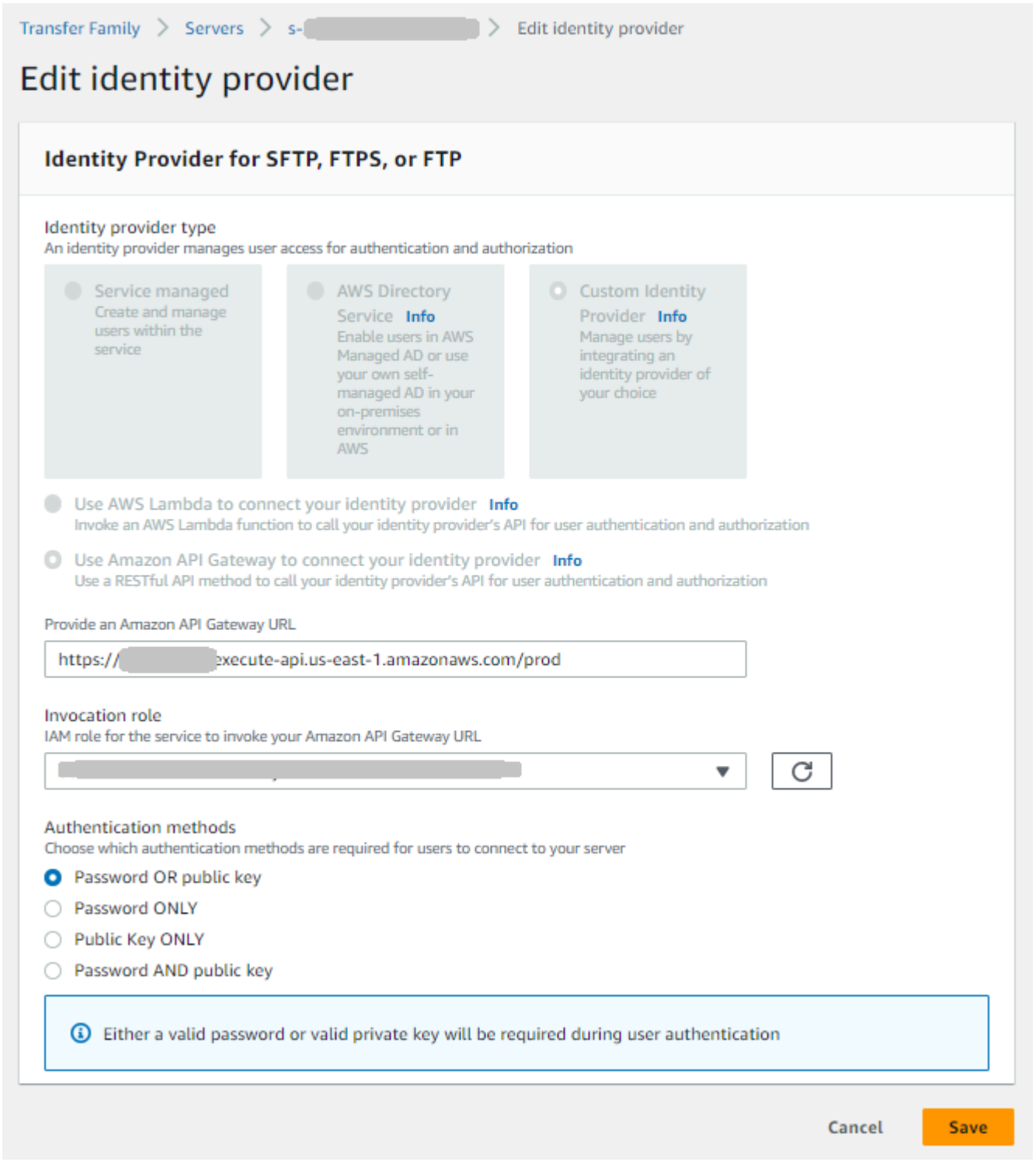
Editar los parámetros personalizados del proveedor de identidad

En la AWS Transfer Family consola, en el caso de los proveedores de identidades personalizados, puede cambiar algunos de los ajustes, en función de si utiliza una función Lambda o una API Gateway. En cualquier caso, si el servidor utiliza el protocolo SFTP, puede editar el método de autenticación.

- Si utiliza una Lambda como proveedor de identidad, puede cambiar la función de Lambda subyacente.



- Si utiliza una puerta de enlace API como proveedor de identidad, puede actualizar la URL de la puerta de enlace o el rol de invocación, o ambos.


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
Provide an Amazon API Gateway URL
https:// execute-api.us-east-1.amazonaws.com/prod
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

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:

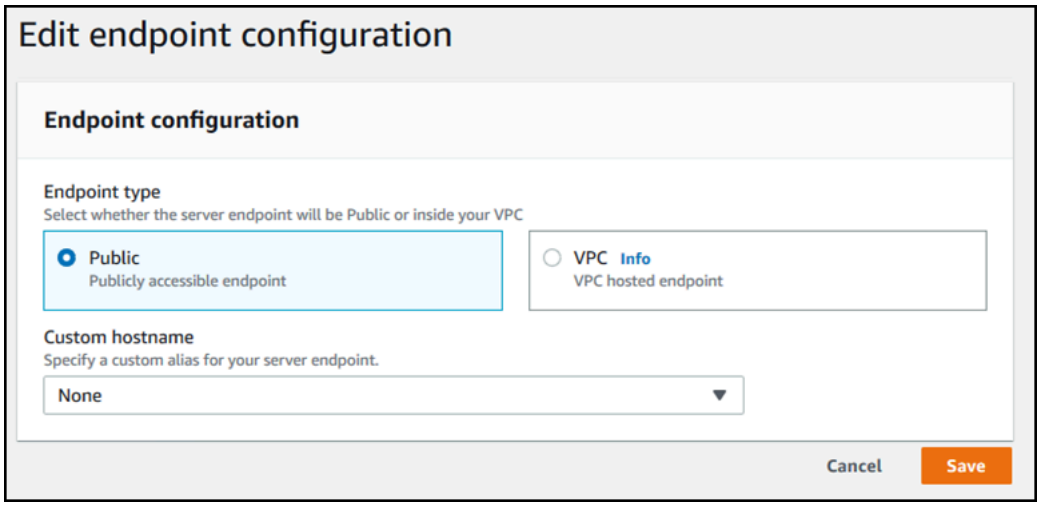
   - Ninguno: si no desea utilizar un dominio personalizado, seleccione None.

     Obtendrá un nombre de host del 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 Guardar. 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 terminal está habilitado para FIPS, 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 servidores AWS Transfer Family.
3. Seleccione Guardar.

   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 enPolíticas de seguridad para servidores AWS Transfer Family.

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.

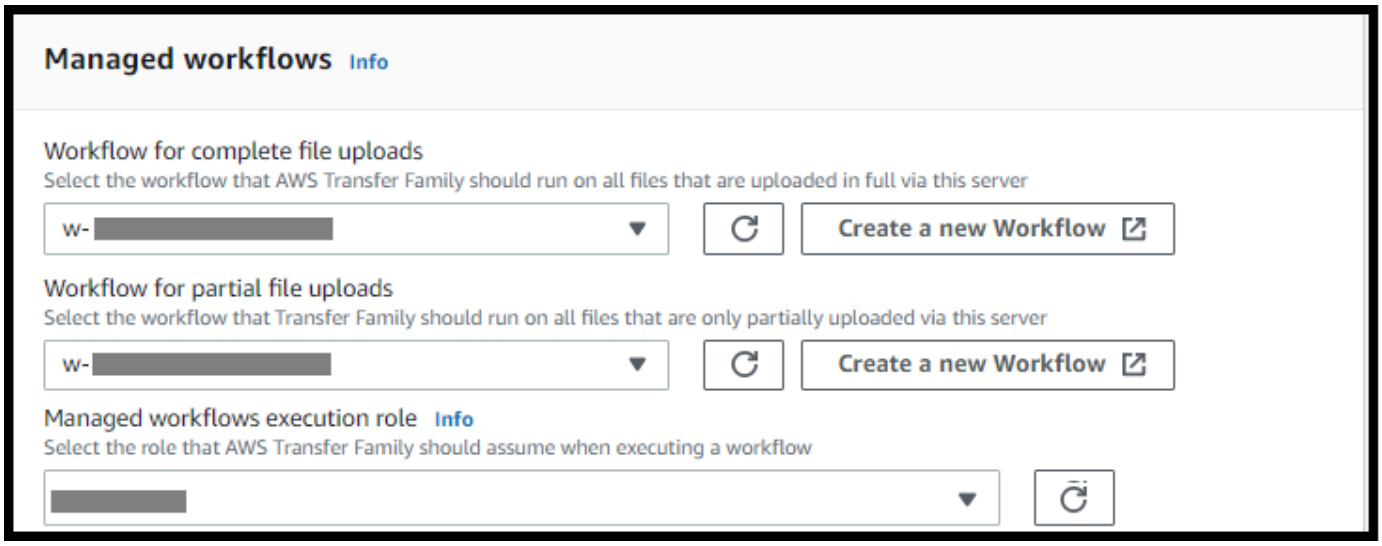
Cambio del flujo de trabajo administrado

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 (Guardar).



3. Seleccione Guardar. 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 Guardar. 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 `START_FAILED` de error`STOP_FAILED`, póngase en contacto con nosotros AWS Support para que le ayuden a resolver los problemas.

Administración de las claves de host de su servidor habilitado para SFTP

> **Important**
>
> Si no tiene pensado migrar los usuarios existentes de un servidor compatible con SFTP existente a un servidor compatible con SFTP nuevo, ignore esta sección.
> 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 proporciona una clave de host para el servidor habilitado para SFTP. Puede sustituir la clave de host predeterminada con una clave de host de otro servidor. Hágalo solo si tiene pensado mover usuarios existentes de un servidor compatible con SFTP existente al nuevo servidor compatible con SFTP.

Para evitar que sus usuarios reciban la soilicitud para verificar la autenticidad del servidor compatible con SFTP de nuevo, importe la clave de host del servidor en las instalaciones al servidor compatible con SFTP. De este modo, también se evita que los 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.

> **Note**
>
> Si bien la consola Transfer Family permite especificar y agregar claves de host de servidor para todos los servidores, estas claves solo son útiles para los servidores que utilizan el protocolo SFTP.

Temas

- Agregue una clave de host de servidor adicional
- Eliminar una clave de host
- Rotar las claves del host del servidor

- Información adicional sobre la clave del host del servidor

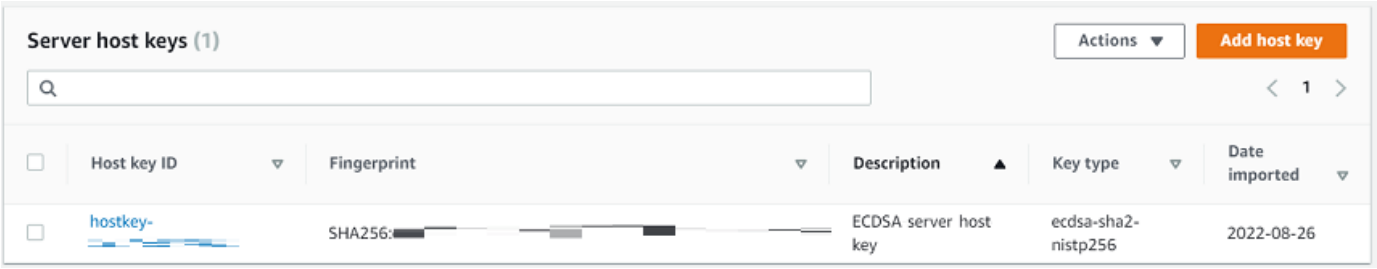
Agregue una clave de host de servidor adicional

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 conecta mediante la primera clave pública que tiene y que puede coincidir con una de las claves de servidor activas.

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.



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 utilizará para identificar el servidor cuando los clientes se conecten a él a través del servidor compatible con SFTP.

> **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 de the section called “ImportHostKey” API y proporcione la nueva clave de host. Si crea un nuevo servidor compatible con SFTP, proporcione su clave de host como un parámetro en la the section called “CreateServer” operación de API . También, puede utilizar el 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 servidor habilitado para SFTP especificado.

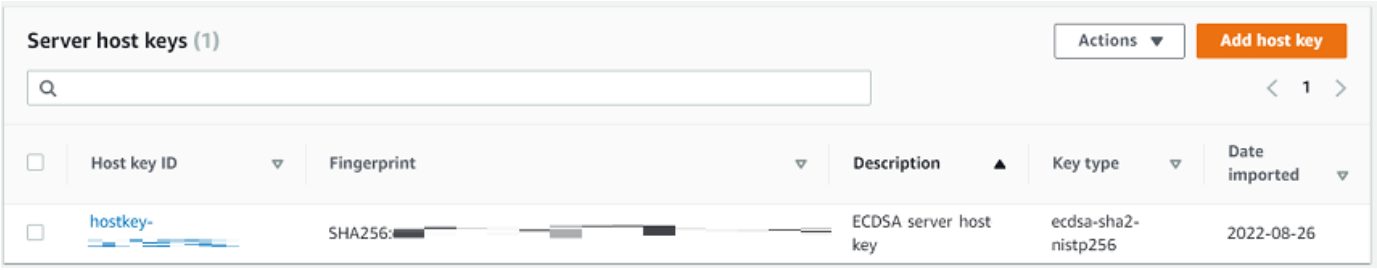
```
aws transfer import-host-key --description key-description --server-id your-server-id
 --host-key-body file://my-host-key
```

Eliminar una clave de host

En la AWS Transfer Family consola, puede eliminar la clave de host de un 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.



4. En la sección Claves de host del servidor, seleccione una clave y, a continuación, en Acciones, seleccione Eliminar.
5. 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 la AWS CLI, utilice la operación de the section called "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 servidor habilitado para SFTP 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.

Cómo elige el cliente una clave de host de 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

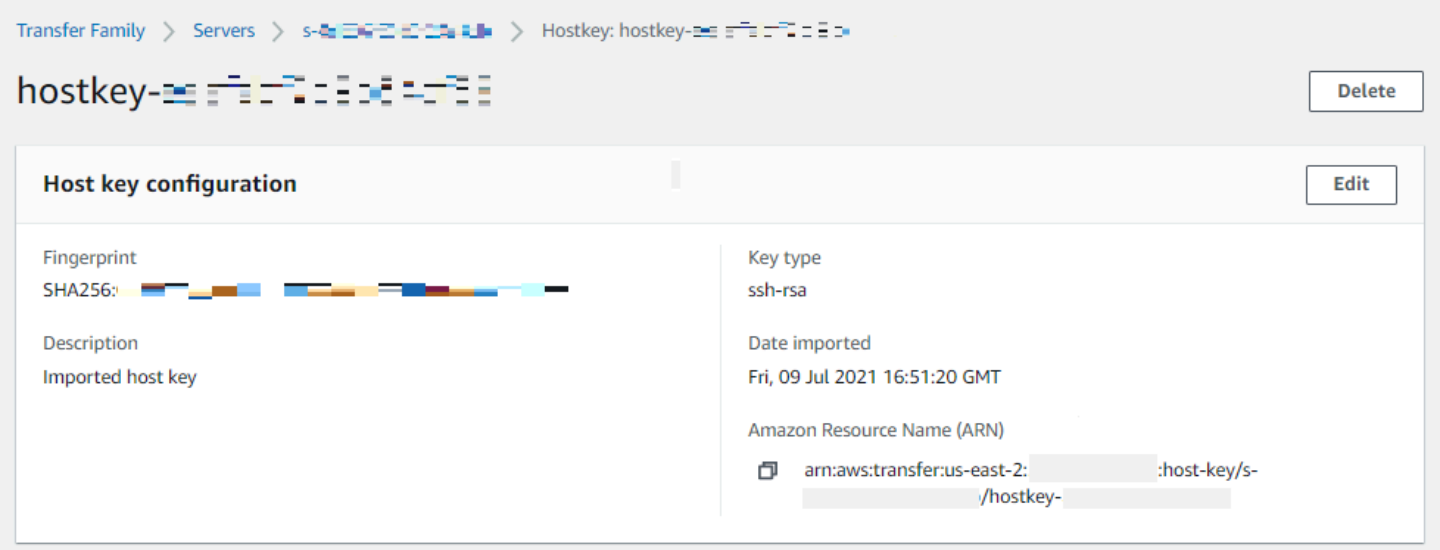
Tipo de clave de host	Fecha en que se añadió al servidor
RSA	1 de abril de 2020
ECDSA	1 de febrero de 2020
ED25519	1 de diciembre de 2019
RSA	1 de octubre de 2019
ECDSA	1 de junio de 2019
ED25519	1 de marzo de 2019

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 enCómo elige el cliente una clave de host de servidor.

Información adicional sobre la clave del host del servidor

Puede seleccionar una clave de host para mostrar los detalles de esa clave.



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.

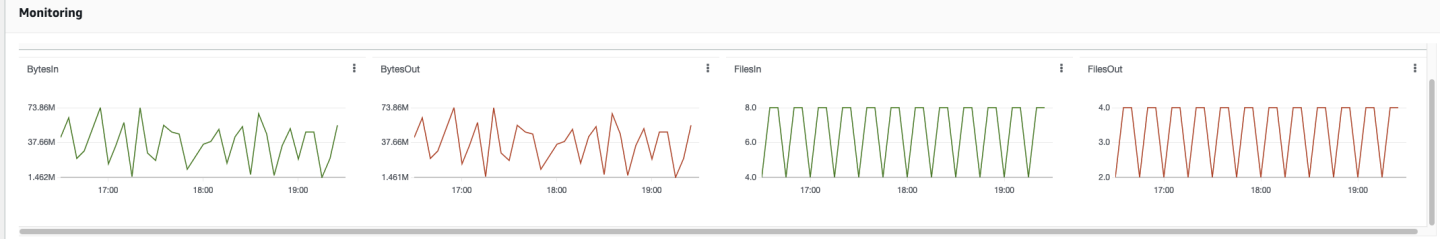
Monitoreo del uso en la consola

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 detalles, consulte Vea los detalles de los servidores SFTP, FTPS y FTP. En la siguiente tabla, se describen las métricas disponibles para Transfer Family.

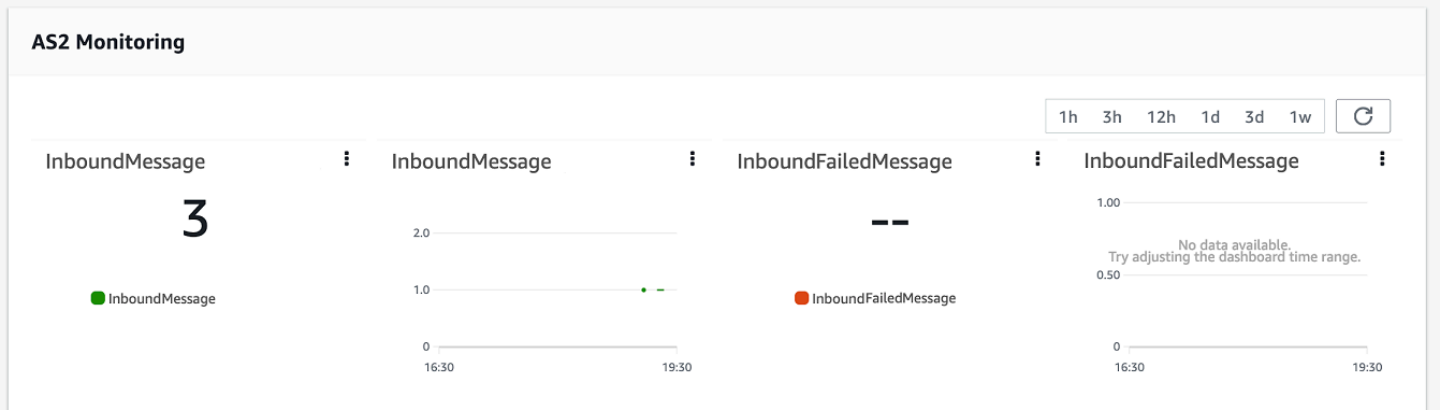
Espacio de nombres	Métrica	Descripción
`AWS/Transfer`	`BytesIn`	El número total de bytes transferidos al servidor. Unidades: recuento Periodo: 5 minutos
	`BytesOut`	El número total de bytes transferidos desde el servidor. Unidad: recuento Periodo: 5 minutos
	`FilesIn`	El número total de archivos transferidos al servidor. Para los servidores que utilizan el protocolo AS2, esta métrica representa la cantidad de mensajes recibidos. Unidades: recuento Periodo: 5 minutos
	`FilesOut`	El número total de archivos transferidos desde el servidor. Unidades: recuento Periodo: 5 minutos

Espacio de nombres	Métrica	Descripción
	`InboundMessage`	El número total de mensajes AS2 recibidos correctamente de un socio comercial. 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. Unidades: recuento Periodo: 5 minutos
	`OnUploadExecutionsStarted`	La cantidad total de ejecuciones de flujos de trabajo iniciadas en el servidor. Unidades: recuento Periodo: 1 minuto
	`OnUploadExecutionsSuccess`	La cantidad total de ejecuciones satisfactorias del flujo de trabajo en el servidor. Unidades: recuento Periodo: 1 minuto
	`OnUploadExecutionsFailed`	La cantidad total de ejecuciones de flujos de trabajo fallidas en el servidor. Unidades: recuento Periodo: 1 minuto

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 (de 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 para AWS Transfer Family que contenga la política de IAM y que tenga asociada una 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 detalles, 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 detalles, consulte Cifrado de datos en Amazon S3. 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
- Impedir que los usuarios ejecuten mkdir en un bucket de S3

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. La asignación de un rol de IAM con esta política de IAM a ese usuario le proporcionará acceso de lectura y escritura 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:::DOC-EXAMPLE-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:::DOC-EXAMPLE-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.

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 HomeDirectoryy. 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 AssumeRoleWith SAML y AssumeRoleWithWebIdentity 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 realice cambios a la política en la consola de IAM, tiene que volver a la consola de AWS Transfer Family y actualizar sus usuarios con los últimos contenidos de la política. Puede actualizar el usuario en la pestaña Información de la política en la sección Configuración de usuario.
> Si utiliza el 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)"
> ```

Impedir que los usuarios ejecuten **`mkdir`** en un bucket de S3

Puede limitar la capacidad de los usuarios para crear un directorio en un bucket de Amazon S3. Para hacerlo, cree una política de IAM que permita la acción `s3:PutObject`, pero que también la deniegue cuando la clave termine con una “/” (barra diagonal invertida). El siguiente ejemplo de política permite a los usuarios cargar archivos en un bucket de Amazon S3, pero deniega el comando mkdir en el bucket de Amazon S3.

```
{
   "Sid":"DenyMkdir",
   "Action":[
      "s3:PutObject"
   ],
   "Effect":"Deny",
   "Resource":[
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/",
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/*"
    ]
}
```

> **Note**
>
> La segunda línea de recursos impide a los usuarios crear subcarpetas mediante la ejecución de un comando como `put my-file DOC-EXAMPLE-BUCKET/new-folder/my-file`.

Registros en AWS Transfer Family

AWS Transfer Familyse integra tanto con Amazon AWS CloudTrail como con Amazon CloudWatch. CloudTrail y CloudWatch sirven para propósitos diferentes pero complementarios:

- CloudTrail es un AWS servicio que crea un registro de las acciones realizadas en su senoCuenta de AWS. Supervisa y registra continuamente las llamadas a la API para actividades como los inicios de sesión en la consola, los AWS Command Line Interface comandos y las llamadas al SDK/API. 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 es 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.

Temas

- AWS CloudTrailiniciar sesión para AWS Transfer Family
- Amazon CloudWatch inicia sesión para AWS Transfer Family

AWS CloudTrailiniciar sesión para AWS Transfer Family

AWS Transfer Familyestá integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, rol o AWS servicio enAWS Transfer Family. CloudTrail captura todas las llamadas a la API AWS Transfer Family como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de AWS Transfer Family y las llamadas desde el código a las operaciones de la API de AWS Transfer Family.

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud,

etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Para mantener un registro continuo de eventos en la cuenta de AWS, incluidos los eventos de AWS Transfer Family, cree un registro de seguimiento. 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. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. 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 `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 lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de AWS Identity and Access Management.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte 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 paraAWS 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 a AWS Transfer Family qué dirección IP se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Temas

- Habilitar AWS CloudTrail el registro
- Ejemplo de entrada de registro para crear un servidor

Habilitar AWS CloudTrail el registro

Puede monitorizar AWS Transfer Family las llamadas a la API con AWS CloudTrail. La monitorización de las llamadas a la API le permite obtener información operativa y de seguridad que puede ser muy útil. 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 acerca de los identificadores únicos del rol de AWS Identity and Access Management (IAM), consulte Identificadores únicos en la Guía del usuario de AWS Identity and Access Management.

> **Important**
>
> La longitud máxima de `RoleSessionName` son 64 caracteres. Si el `RoleSessionName` es más largo, se trunca el `server-id`.

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": "AAAA4FFF5HHHHH6NNWWWW: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": "AAAA4FFF5HHHHH6NNWWWW",
                "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"
}
```

Amazon CloudWatch inicia sesión para AWS Transfer Family

Amazon CloudWatch monitorea tus AWS Transfer Family recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede utilizarlas CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir para sus recursos y aplicaciones.

La página de CloudWatch inicio muestra automáticamente las métricas sobre Transfer Family y todos los demás AWS servicios que utilizas. También puede crear adicionalmente paneles personalizados para mostrar métricas sobre sus aplicaciones personalizadas, y mostrar colecciones personalizadas de métricas que elija.

Puede crear alarmas que vigilen métricas y enviar notificaciones o realizar cambios automáticamente en los recursos que está monitoreando cuando se infringe un umbral. Por ejemplo, puede supervisar los archivos que se transfieren a un servidor Transfer Family y utilizar esos datos para determinar si necesita implementar servidores adicionales para gestionar el aumento de carga. También puede usar estos datos para detener o eliminar instancias infrautilizadas y así ahorrar dinero.

Tipos de CloudWatch registro para Transfer Family

Transfer Family ofrece dos formas de registrar eventos en CloudWatch:

- Registro estructurado en 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": "arn:aws:logs:region-id:Cuenta de AWS:log-group:/aws/transfer/
*"
        }
    ]
}
```

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, consulteAdministrar el registro de los flujos de trabajo.

Temas

- Crear, actualizar y ver los registros de los servidores
- Administrar el registro de los flujos de trabajo
- Configura el rol de CloudWatch registro
- Visualización de las transmisiones de registros de Transfer Family
- Creación de CloudWatch alarmas de Amazon
- Registro de llamadas a la API de Amazon S3 a los registros de acceso de S3

- Ejemplos para limitar el problema del suplente confuso
- CloudWatch estructura de registro para Transfer Family
- Ejemplo de entradas de CloudWatch registro
- Uso de CloudWatch métricas para Transfer Family
- Utilizándolo AWS User Notifications con AWS Transfer Family
- Uso de consultas para filtrar las entradas de registro

Crear, actualizar y ver los registros de los servidores

Para todos los AWS Transfer Family servidores, puede elegir entre dos opciones de registro: `LoggingRole` (utilizada para registrar los flujos de trabajo que están conectados al servidor) o`StructuredLogDestinations`. Entre los beneficios de utilizar `StructuredLogDestinations` se incluyen los 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.

Las opciones para `LoggingRole` o `StructuredLogDestinations` se configuran y controlan por separado. Para cada servidor, puede configurar uno o ambos métodos de registro, o configurar el servidor para que no registre ningún tipo de registro (aunque no se recomienda).

Si crea un servidor mediante la consola de Transfer Family, el registro se habilita de forma predeterminada. Después de crear el servidor, puede utilizar la llamada a la `UpdateServer` API para cambiar la configuración de registro. Para obtener más información, consulte StructuredLog Destinos.

Actualmente, para los flujos de trabajo, si desea habilitar el registro, debe especificar un rol de registro:

- Si asocia un flujo de trabajo con un servidor mediante `CreateServer` o la llamada a la `UpdateServer` API, el sistema no crea automáticamente un rol 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`

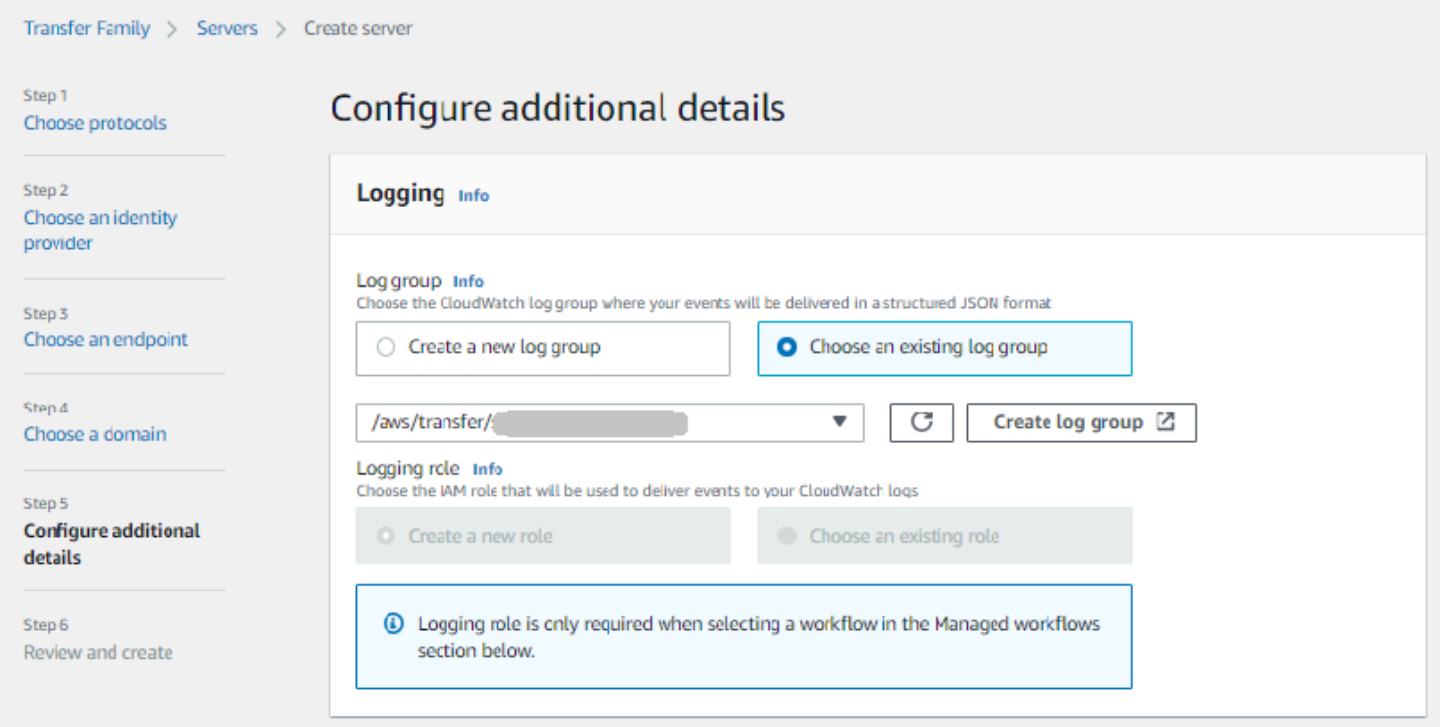
En la sección encontrará un ejemplo de políticaConfigura el rol de CloudWatch registro.

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.



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.

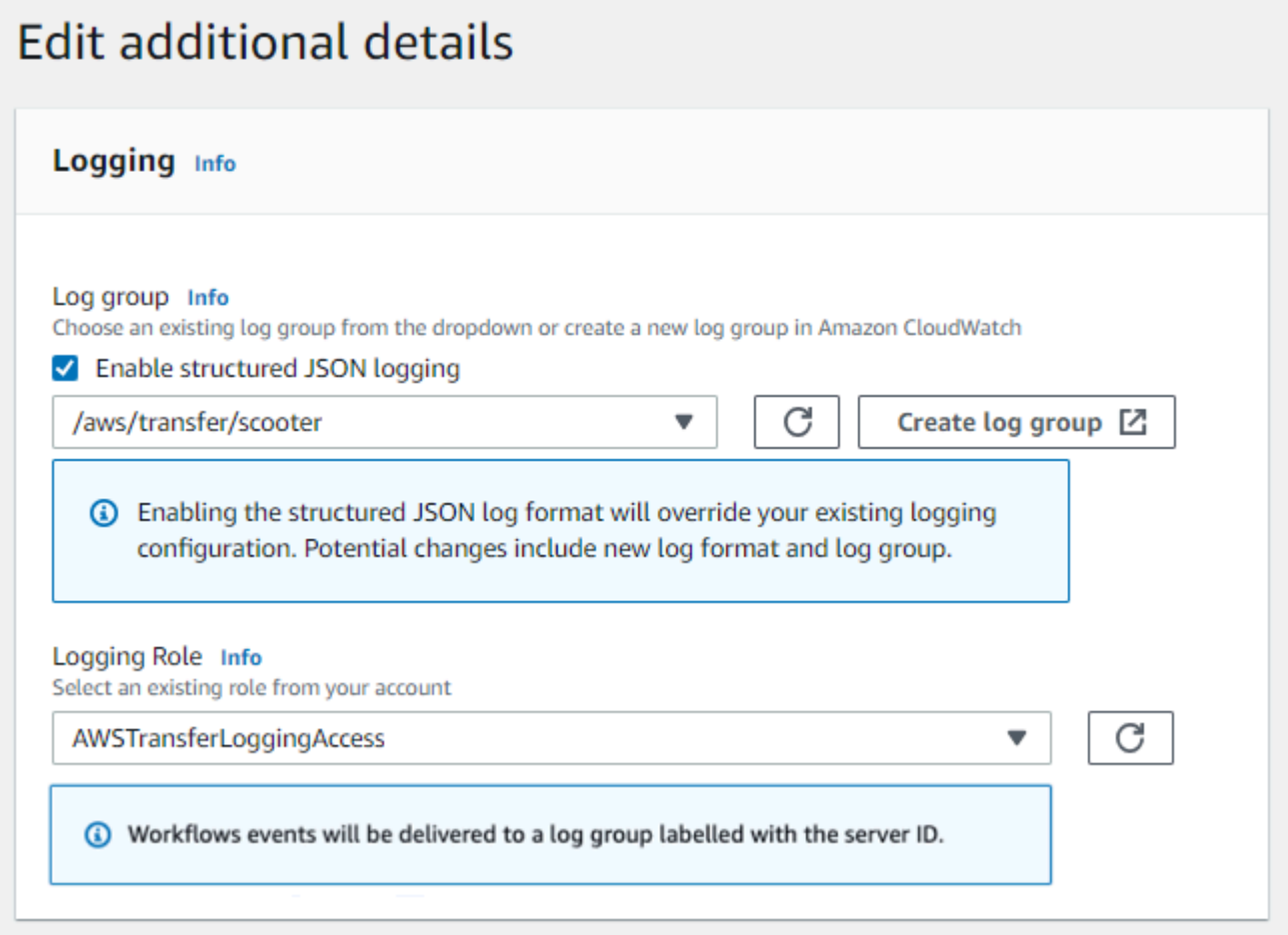
Actualización del registro de un servidor

Los detalles del registro dependen del escenario de la actualización.

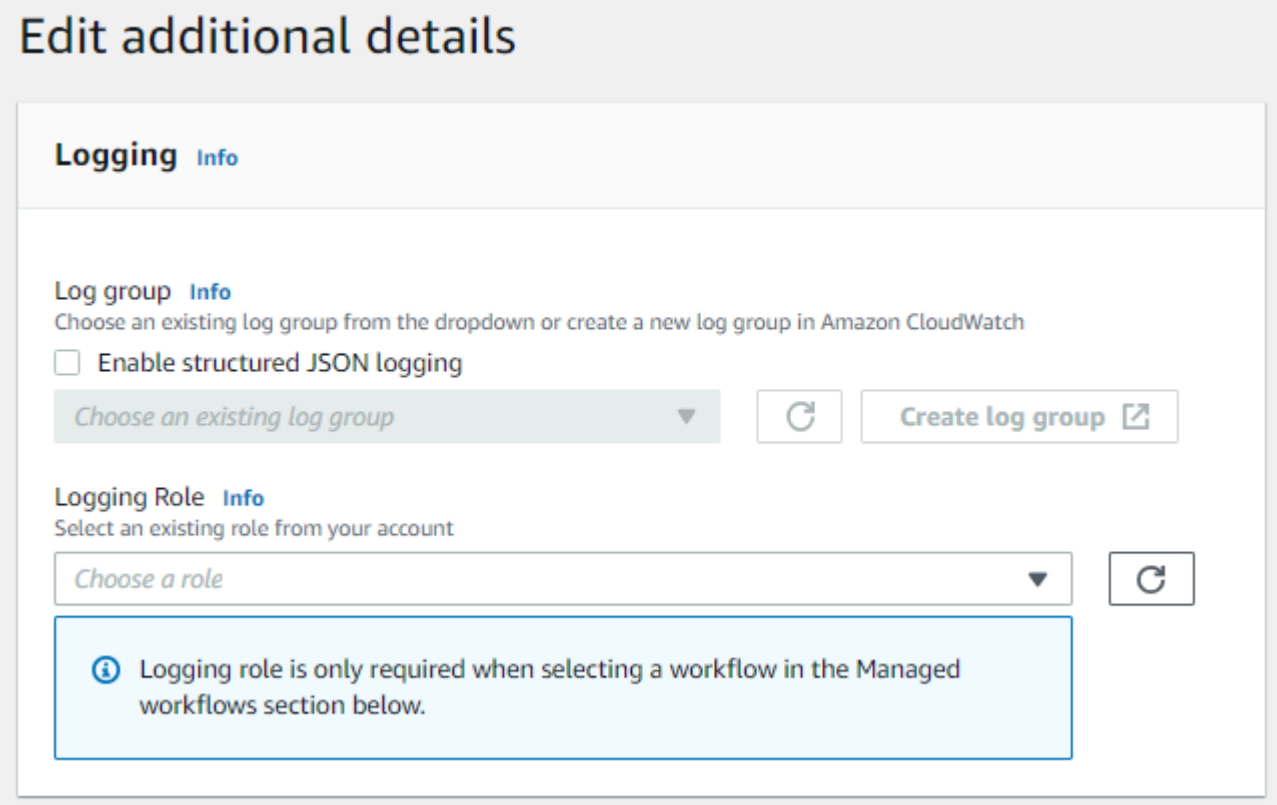
> **Note**
>
> Si opta por el registro JSON estructurado, es posible que, en raras ocasiones, se produzca un retraso donde Transfer Family deje de registrar en el formato anterior, pero demore cierto tiempo en empezar a registrar en el nuevo formato JSON. Esto puede provocar que los eventos no se registren. 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.

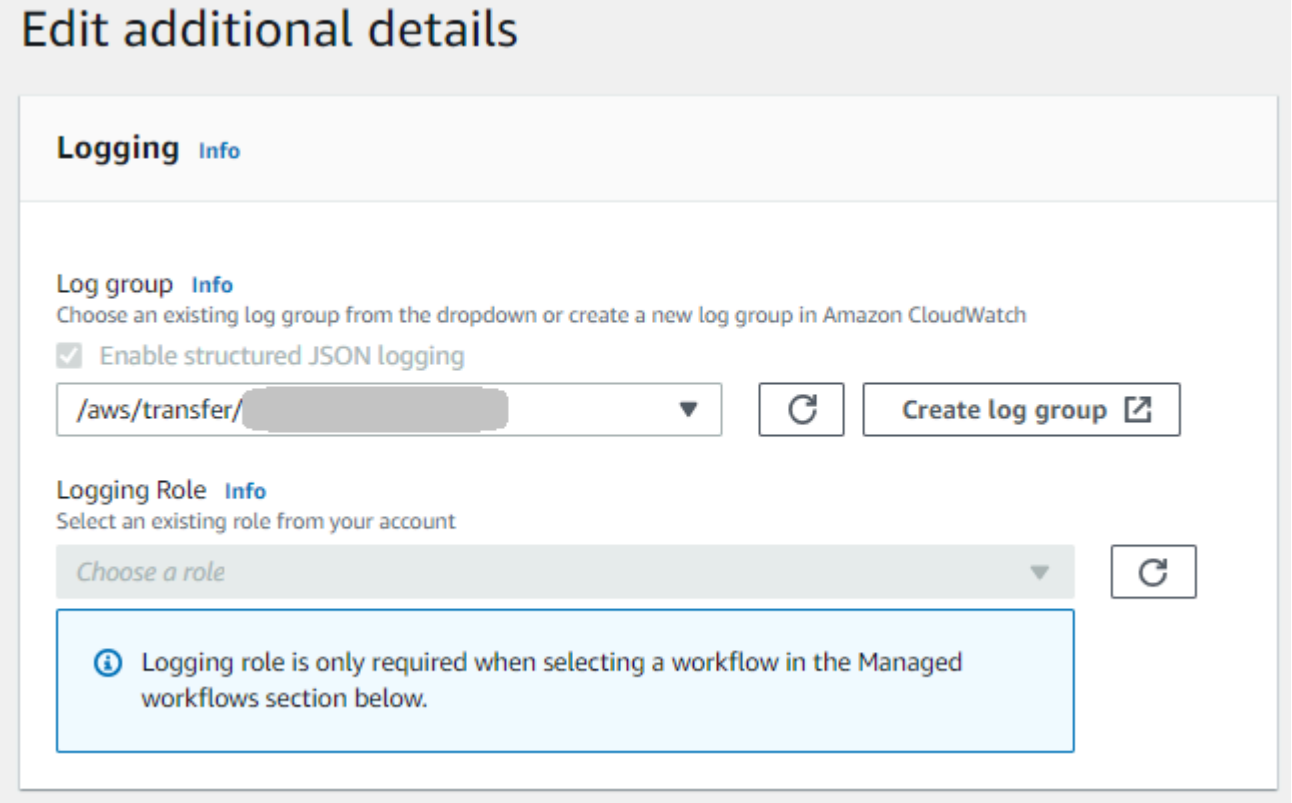
- El servidor ya tiene habilitado un rol de registro, pero no tiene activado el registro JSON estructurado.



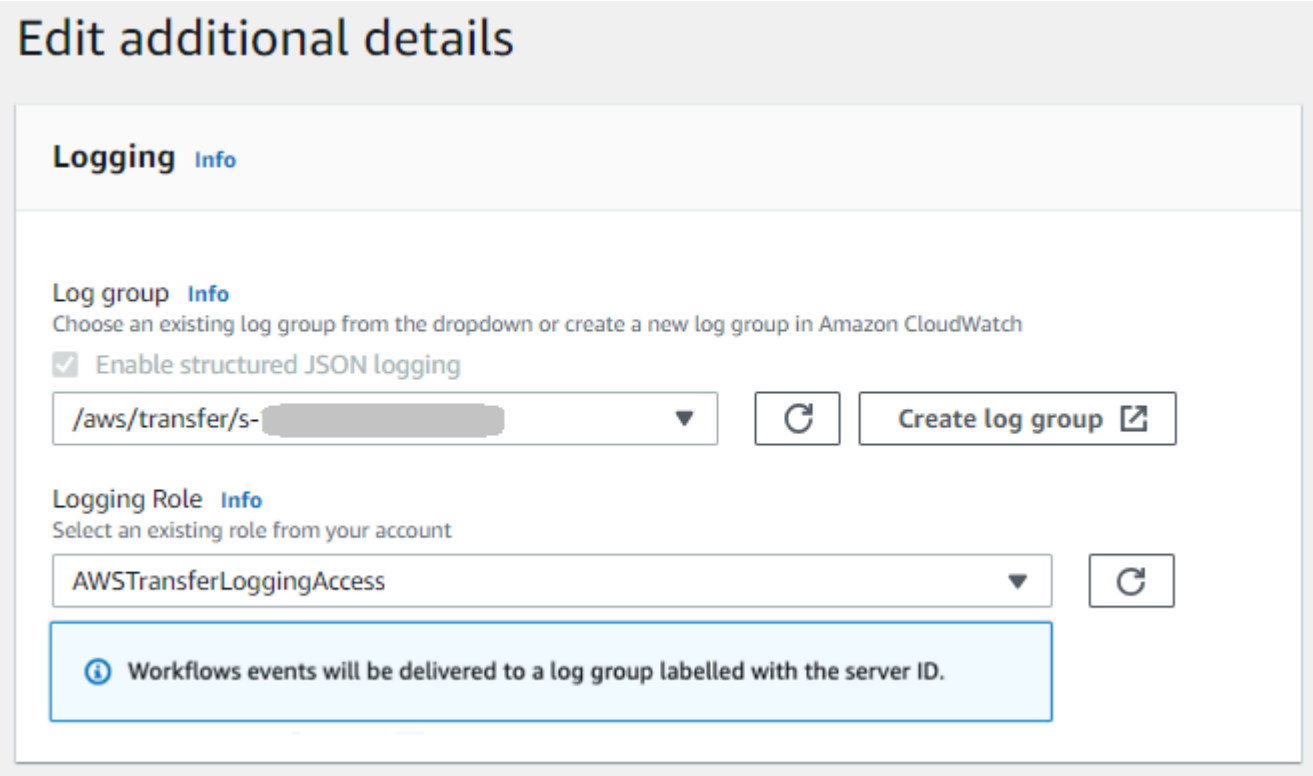
- El servidor no tiene activado ningún registro.



- El servidor ya tiene habilitado el registro JSON estructurado, pero no tiene un rol de registro especificado.



- El servidor ya tiene habilitado el registro JSON estructurado y tiene un rol de registro especificado.

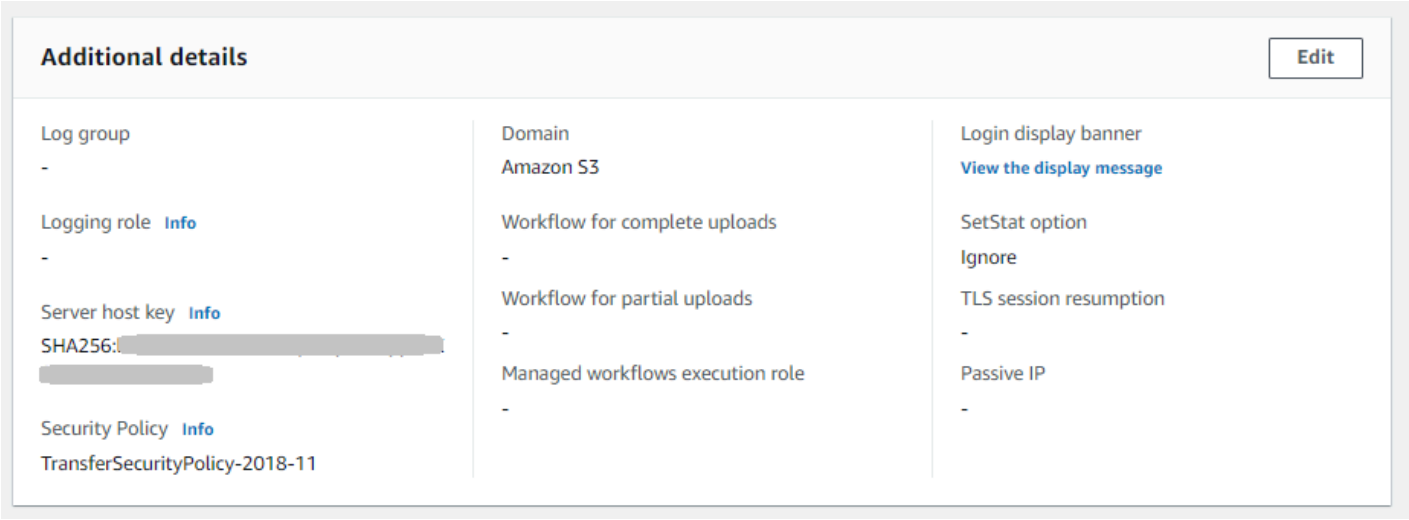


Vista de la configuración del servidor

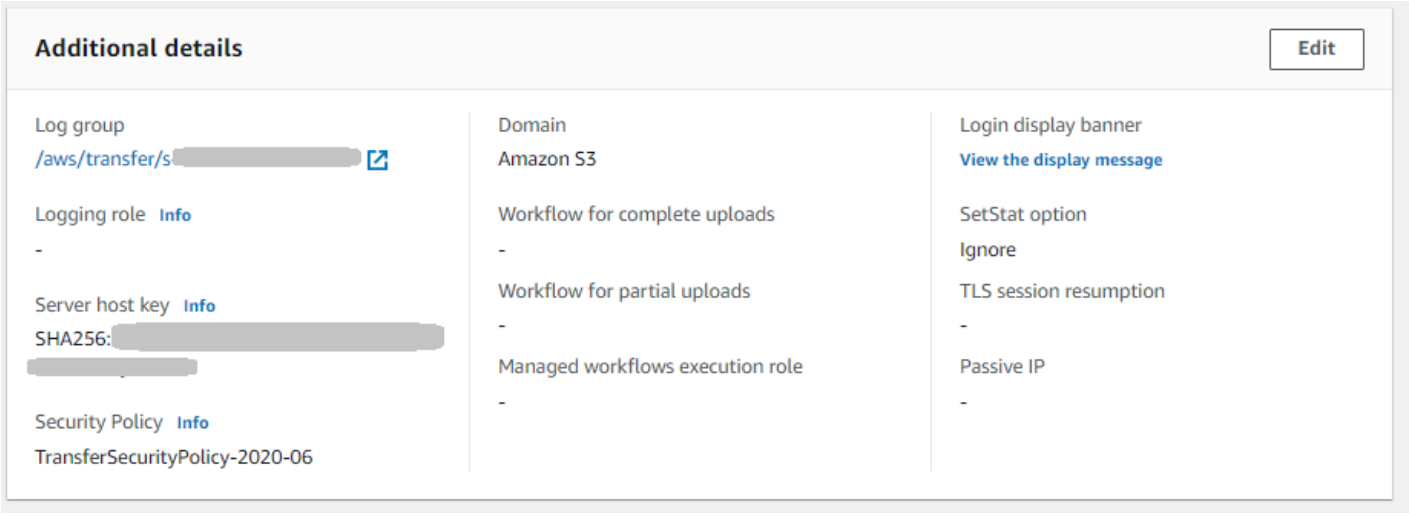
Los detalles de la página de configuración del servidor dependen del escenario:

Según el escenario, la página de configuración del servidor puede tener un aspecto similar a uno de los siguientes ejemplos:

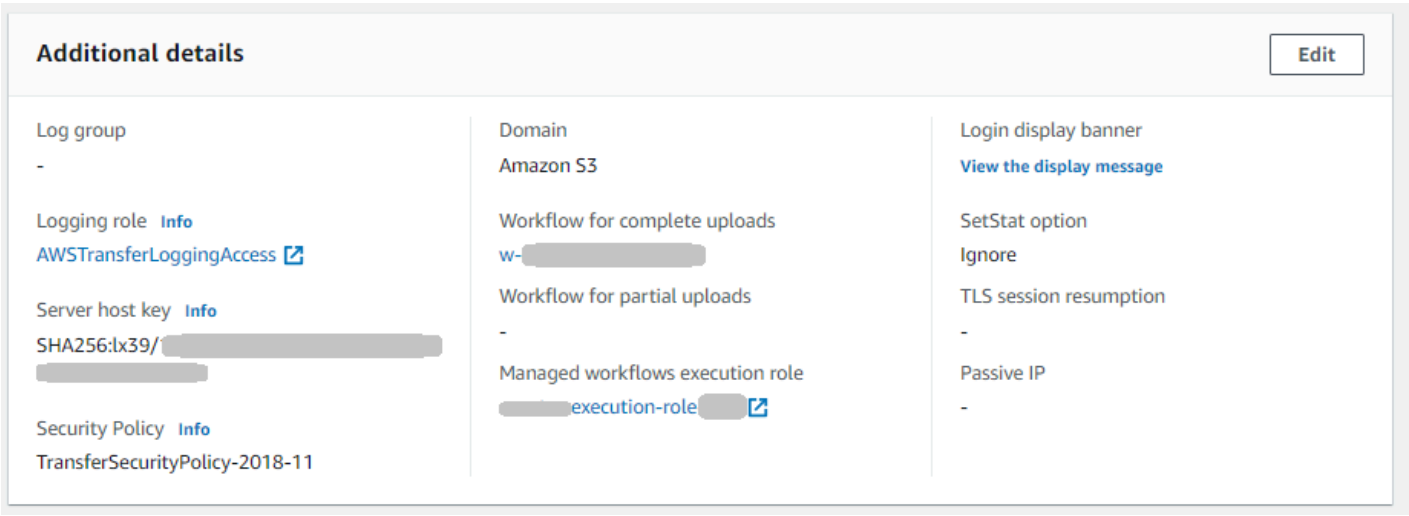
- No se ha habilitado ningún registro.



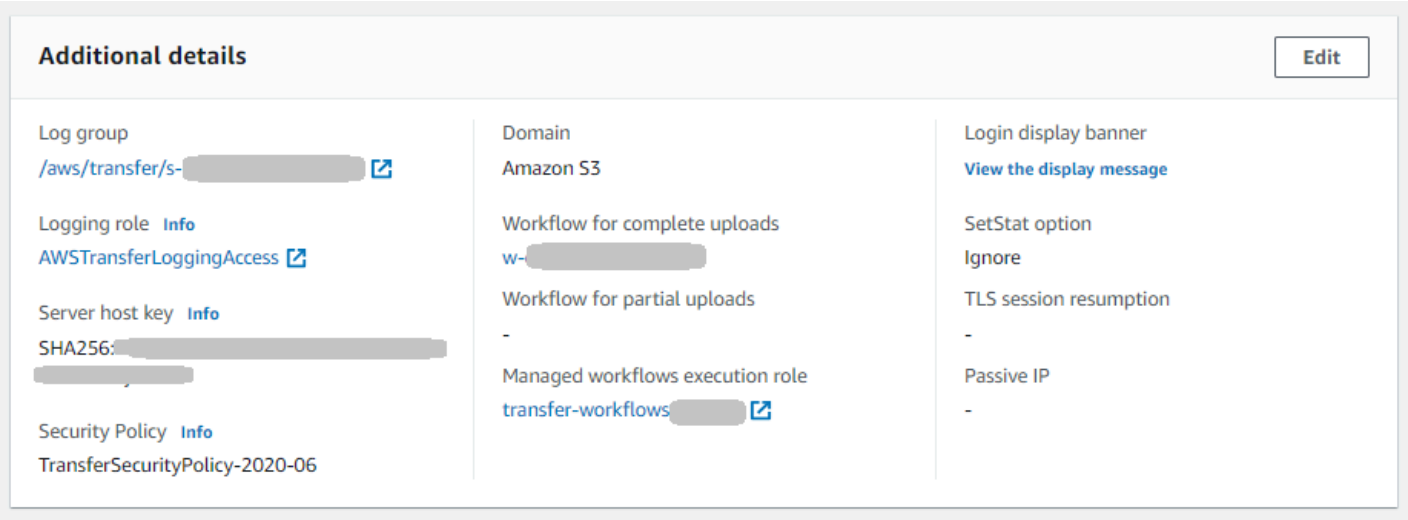
- El registro JSON estructurado está habilitado.



- El rol de registros está activado, pero el registro JSON estructurado no está activado.



- Ambos tipos de registro (rol de registro y registro JSON estructurado) están habilitados.



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 enUso de CloudWatch métricas para 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": "DOC-EXAMPLE-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":"DOC-EXAMPLE-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 asóciele 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": "arn:aws:logs:region-id:Cuenta de AWS:log-group:/aws/
transfer/*"
        }
    ]
}
```

En el ejemplo anterior de política, para el **Resource**, sustituya la *identificación de región* y *Cuenta de AWS* por 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 (Siguiente: 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

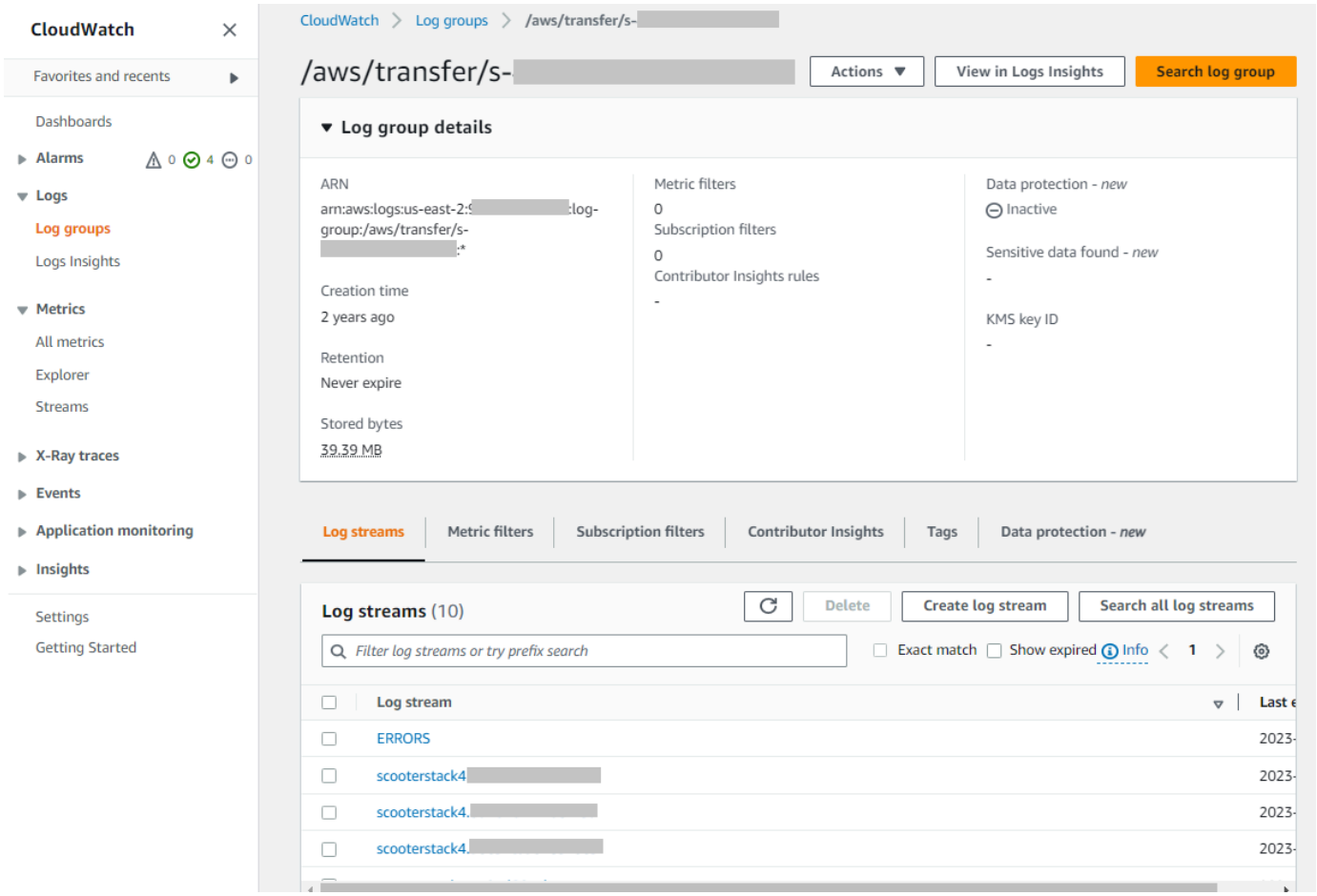
3. En la sección Adjuntar políticas de permisos, busque y elija la política de CloudWatch registros que acaba de crear y elija Siguiente: etiquetas.
4. (Opcional) Introduzca una clave y un valor de etiqueta y seleccione Siguiente: Revisión.
5. En la página Review (Revisión), escriba un nombre y una descripción 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 (`PUT`operaciones) y las descargas de datos (`GET`operaciones).

Visualización de las transmisiones de registros de Transfer Family

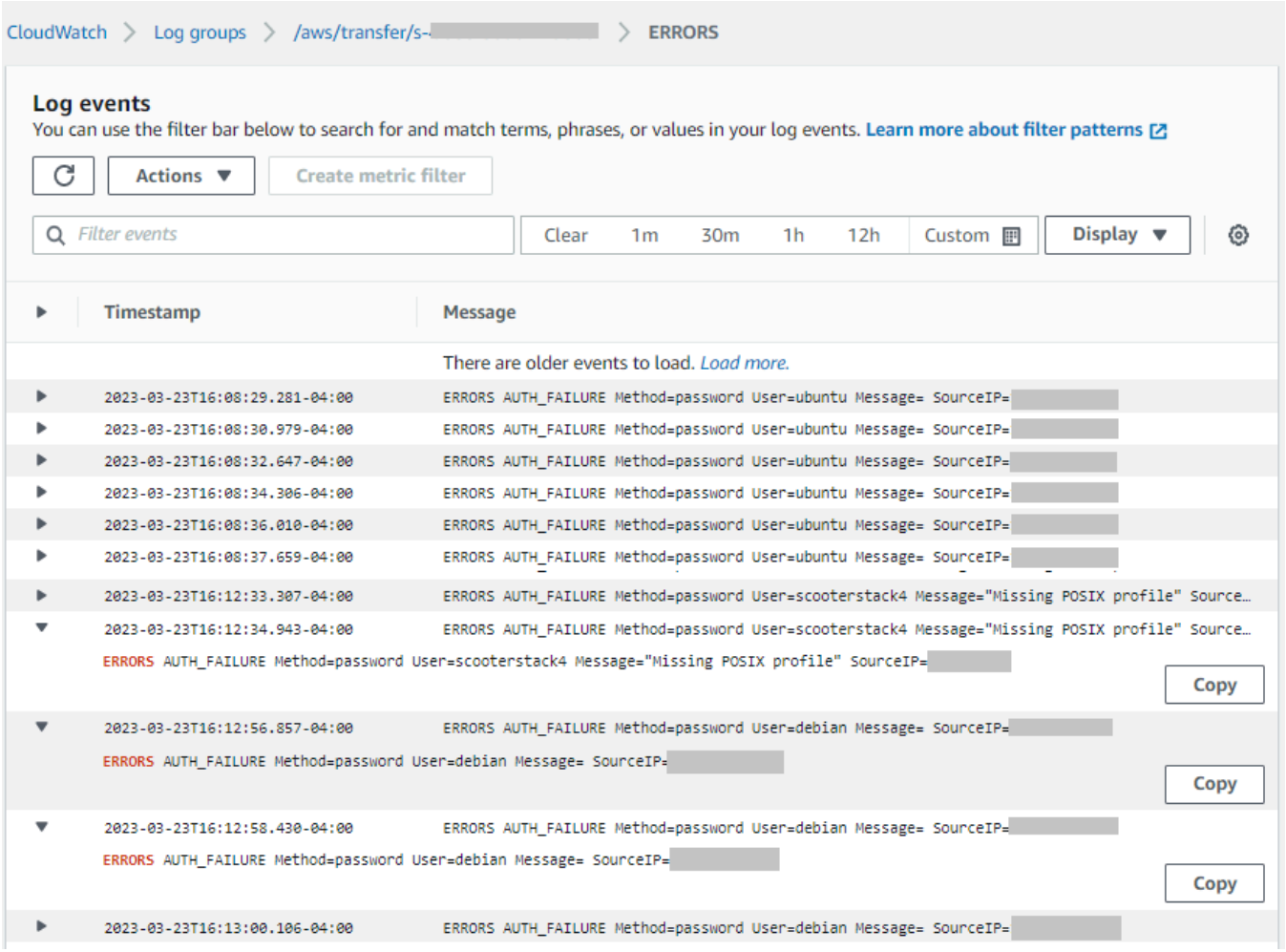
Visualización de los registros del servidor de Transfer Family

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.

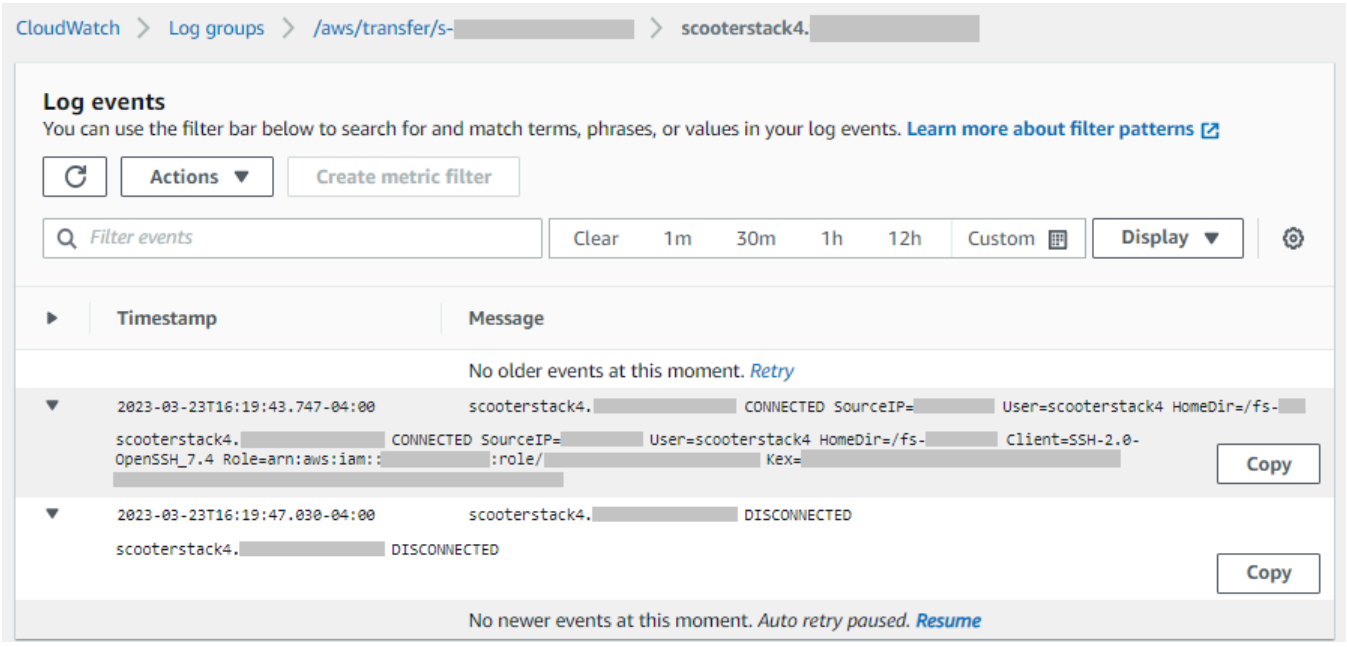


4. Puede seleccionar un flujo de registro para mostrar los detalles y las entradas individuales del flujo.

   - Si hay una lista de ERRORES, puede seleccionarla para ver los detalles de los errores más recientes del servidor.

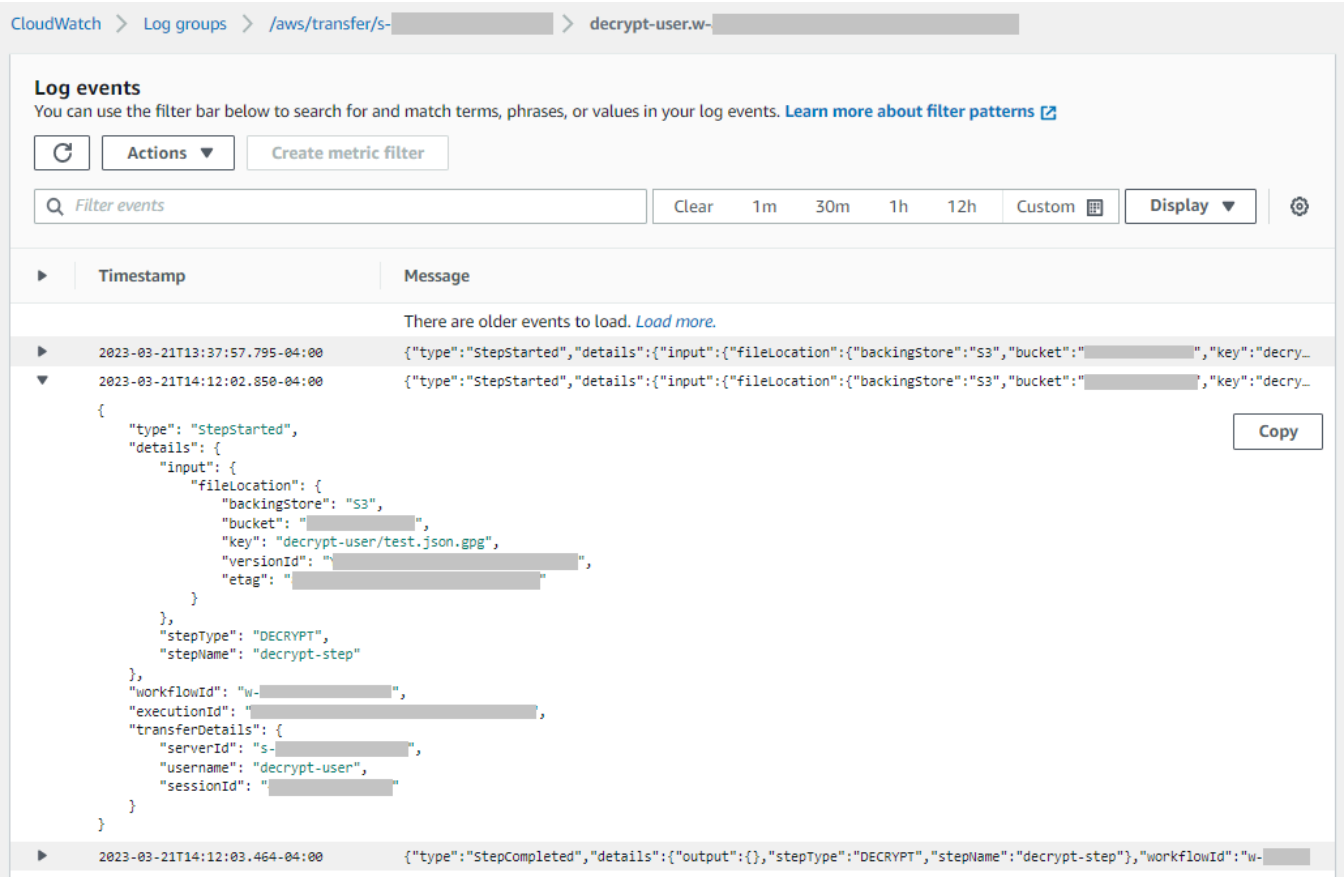


- Seleccione cualquier otra entrada para ver un ejemplo de flujo de registro.



- 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`**.



> **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-00000000000000000" },
  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,
});
```

AWS CloudFormation

```
Type: AWS::CloudWatch::Alarm
Properties:
  Namespace: AWS/Transfer
  MetricName: FilesIn
  Dimensions:
    - Name: ServerId
      Value: s-00000000000000000
  Statistic: Average
  Period: 60
  Threshold: 1000
  EvaluationPeriods: 10
  DatapointsToAlarm: 5
  ComparisonOperator: GreaterThanOrEqualToThreshold
```

Registro de llamadas a la API de Amazon S3 a los registros de acceso de S3

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 Prevención de la sustitución confusa entre servicios.

> **Note**
>
> En los ejemplos siguientes, reemplace cada *`marcador de posición del usuario`* con su 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 de política de registro e invocación 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": "account-id"
                },
                "ArnLike": {
                   "aws:SourceArn": [
                     "arn:aws:transfer:region:account-id:server/*",
                     "arn:aws:transfer:region:account-id:workflow/*"
                   ]
                }
            }
        }
    ]
}
```

El siguiente ejemplo de política de registro e invocación permite que un servidor (y un flujo de trabajo) específicos asuman la función.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSpecificServerWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
                "ArnEquals": {
```

```
                    "aws:SourceArn": [
                        "arn:aws:transfer:region:account-id:server/server-id",
                        "arn:aws:transfer:region:account-id: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 las acciones de SFTP/FTP/FTPS de Transfer Family, en el nuevo formato de registro estructurado JSON.

Campo	Descripción	Ejemplo de entrada
activity-type	The action by the user	ABRIR | CERRAR | CERRAR PARCIALMENTE | DESCONECTADO | CONECTADO
bytes-in	Number of bytes uploaded by the user	29238420042
bytes-out	Number of bytes downloaded by the user	23094032490328
ciphers	Specifies the SSH cipher negotiated for the connection	aes256-gcm@openssh.com

Campo	Descripción	Ejemplo de entrada
	(available ciphers are listed in Algoritmos criptográficos)	
client	The user's client software	SSH-2.0-OpenSSH_7.4
home-dir	The directory that the end user lands on when they connect to the endpoint if their home directory type is PATH: if they have a logical home directory, this value is always /	/user-home-bucket/test
kex	Specifies the negotiated SSH key exchange (KEX) for the connection (available KEX are listed in Algoritmos criptográficos)	diffie-hellman-group14-sha256
message	Provides more information related to the error	*<string>*
method	The authentication method	publickey
mode	Specifies how a client opens a file	CREATE | TRUNCATE | WRITE
operation	The client operation on a file	OPEN | CLOSE
path	Actual file path affected	/user-test-bucket/test-file-1.pdf
resource-arn	A system-assigned, unique identifier for a specific resource (for example, a server)	arn:aws:transfer:ap-northeast-1:12346789012:server/s-1234567890akeu2js2
role	The IAM role of the user	arn:aws:iam: :02938836 75:role/testuser-role

Campo	Descripción	Ejemplo de entrada
session-id	A system-assigned, unique identifier for a single session	9ca9a0e1cec6ad9d
source-ip	Client IP address	18.323.0.129
user	The end user's username	myname192
user-policy	The permissions specified for the end user: this field is populated if the user's policy is a session policy.	The JSON code for the session policy that is being used

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.

Acción de	Registros correspondientes en Amazon CloudWatch Logs
Errores de autenticación	ERRORS AUTH_FAILURE Method=publickey User=lhr Message="RSA SHA256:Lfz3R2nmLY4raK+b7Rb1rSvUIbAE+a+Hxg0c7l1JIZ0" SourceIP=3.8.172.211
COPIAR/ETIQUETAR/ELIMINAR/DESCIFRAR flujo de trabajo	{"type»:» StepStarted «, "details»: {"fileLocation»: {"BackingStore» :"EFS», "fileSyst

Acción de	Registros correspondientes en Amazon CloudWatch Logs
	emID» :"fs-12345678", "path»:» /lhr/regex.py «}}, "stepType» :"TAG», "stepName» :"successful_tag_step "}, "WorkflowID» :"w-1111aaaa2222bbbb3", "ExecutionID» :"81234abcd-1234-efgh-5678-ijklmnopqr90", "Transfer Details»: {"serverID» :"s-1234abcd5678efghi», "username» :"lhr», «ID de sesión» :"1234567890abcdef0"}}
Flujo de trabajo con pasos personalizados	{"type»:» CustomStepInvoked «, "details»: {"output»: {"token» :"MZM4MJG5YWUTYT EzMy 00 YjIz LWI3OG MtYz U4OGI2 ZjQyMz E5"}, "stepType» :"CUSTOM», "stepName » :"efs-s3_copy_2"}, "workflowID» :"w-9283e49d33297c3f7", Execute tionID» :"1234abcd-1234-efgh-5678-ijklmnopqr90", "Transfer Details»: {"serverID» :"s-zzzz1111aaaa22223", "username» :"lhr», "ID de sesión» :"1234567890abcdef0"}}
Eliminaciones	lhr.33a8fb495ffb383b DELETE Path=/bucket/user/123.jpg
Descargas	lhr.33a8fb495ffb383b OPEN Path=/bucket/user/123.jpg Mode=READ llhr.33a8fb495ffb383b CERRAR RUTA=/bucket/user/123.jpg BytesOut =3618546

Acción de	Registros correspondientes en Amazon CloudWatch Logs
Inicio de sesión/cierre de sesión	user.914984e553bcddb6 FUENTE CONECTADA IP = 1.22.111.222 Usuario=LHR =CLIENTE LÓGICO = SSH-2.0-opensSH_7.4 role=arn:aws: :iam: :123456789012:role/sftp-s3-access HomeDir user.914984e553bcddb6 DISCONNECTED
Cambio de nombre	lhr.33a8fb495ffb383b CAMBIAR NOMBRE DE RUTA=/bucket/user/lambo.png =/bucket/user/ferrari.png NewPath
Ejemplo de registro de errores de flujo de trabajo	{"type»:» StepErrored «, "details»: {"ErrorTy pe» :"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-567 8-ijklmnopqr90", "TransferDetails»: {"ServerI D» :"s-1234abcd5678efghi», "username» :"lhr», «ID de sesión» :"1234567890abcdef0"}}
Symlinks	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK LinkPath =/fs-12345678/lhr/pqr.jpg TargetPath =abc.jpg
Subidas	lhr.33a8fb495ffb383b OPEN Path=/bucket/user/123.jpg Mode=CREATE|TRUNCATE|WRITE lhr.33a8fb495ffb383b CERRAR RUTA=/bucket/user/123.jpg =3618546 BytesIn

Acción de	Registros correspondientes en Amazon CloudWatch Logs
Flujos de trabajo	{"type»:» ExecutionStarted «, "details»: {"input»: {"BackingStore» :"EFS», "FileSyst emID» :"fs-12345678", "path»:» /lhr/regex.py initialFileLocation «}}}, "WorkflowID» :"w-1111a aaa2222bbbb3", "ExecutionID» :"1234abc d-1234-efgh-56-78-78-ijklmnopqr90", "Transfer Details»: {"ServerID» :"s-zzzz1111aaaa22223", "username» :"lhr», "ID de sesión» :"1234567 890abcdef0"}} {"type»:» StepStarted «, "details»: {"fileLoc ation»: {"BackingStore» :"EFS», "fileSyst emID» :"fs-12345678", "path»:» /lhr/regex.py «}}, "stepType» :"CUSTOM», "stepName » :"efs-s3"copy_2"}, "WorkflowID» :w-9283e4 9d33297c3f7", "ExecutionID» :"1234abcd-1234- efgh-5678-ijklmnopqr90", "TransferDetails»: {"ServerID» :"s-18ca49dce5d842e0b», «username» :"lhr», "ID de sesión» :"1234567 890abcdeff 0"}}

Ejemplo de entradas de CloudWatch registro

En este tema se presentan ejemplos de entradas de registro.

Temas

- Ejemplo de entradas de registro de sesiones de transferencia
- Ejemplo de entradas de registro para conectores SFTP
- Ejemplos de entradas de registro de errores en el algoritmo de intercambio de claves

Ejemplo 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/scooter-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": "/scooter-test/log-me",
   "user": "log-me",
   "kex": "ecdh-sha2-nistp256",
   "session-id": "9ca9a0e1cec6ad9d"
}
```

La siguiente entrada de registro refleja que el usuario de SFTP ha subido un archivo a su bucket de Amazon S3.

```
{
   "mode": "CREATE|TRUNCATE|WRITE",
   "path": "/scooter-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": "/scooter-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"
}
```

Ejemplo de entradas de registro para conectores SFTP

Esta sección contiene registros de ejemplo de una transferencia correcta y otra incorrecta. Los registros se generan en un grupo de registros denominado`/aws/transfer/`*`connector-id`*, donde *`connector-id`* es el identificador del conector SFTP.

> **Note**
>
> Las entradas de registro para los conectores SFTP solo se generan cuando se ejecuta un comando. `StartFileTransfer`

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-1:480351544584:connector/connector-id",
    "local-directory-path": "/connectors-localbucket"
```

```
    "bytes": 514
}
```

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-1:480351544584:connector/connector-id",
    "local-directory-path": "/connectors-localbucket"
}
```

Esta entrada de registro corresponde a una operación de ENVÍO que se ha realizado 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": "/DOC-EXAMPLE-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-1:255443218509:connector/connector-id",
    "bytes": 275
}
```

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 llamada a la `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 de 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 en el que se produce un 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 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.

Espacio de nombres	Métrica	Descripción
`AWS/Transfer`	`BytesIn`	El número total de bytes transferidos al servidor. Unidades: recuento Periodo: 5 minutos
	`BytesOut`	El número total de bytes transferidos desde el servidor. Unidad: recuento 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. Unidades: recuento Periodo: 5 minutos

Espacio de nombres	Métrica	Descripción
	`FilesOut`	El número total de archivos transferidos desde el servidor. Unidades: recuento Periodo: 5 minutos
	`InboundMessage`	El número total de mensajes AS2 recibidos correctamente de un socio comercial. 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. Unidades: recuento Periodo: 5 minutos
	`OnUploadExecutionsStarted`	La cantidad total de ejecuciones de flujos de trabajo iniciadas en el servidor. Unidades: recuento Periodo: 1 minuto
	`OnUploadExecutionsSuccess`	La cantidad total de ejecuciones satisfactorias del flujo de trabajo en el servidor. Unidades: recuento Periodo: 1 minuto

Espacio de nombres	Métrica	Descripción
	`OnUploadExecutionsFailed`	La cantidad total de ejecuciones de flujos de trabajo fallidas en el servidor. Unidades: recuento Periodo: 1 minuto

Dimensiones de Transfer Family

Una dimensión es un par de nombre-valor 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 describe la CloudWatch dimensión de Transfer Family.

Dimensión	Descripción
`ServerId`	El ID exclusivo del usuario.

Utilizándolo AWS User Notifications con AWS Transfer Family

Para recibir notificaciones sobre AWS Transfer Family eventos, puedes AWS User Notificationsconfigurar 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 AWS Chatbot o notificaciones push 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 la CloudWatch consola AWS Management Console y ábrala 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"
}
```

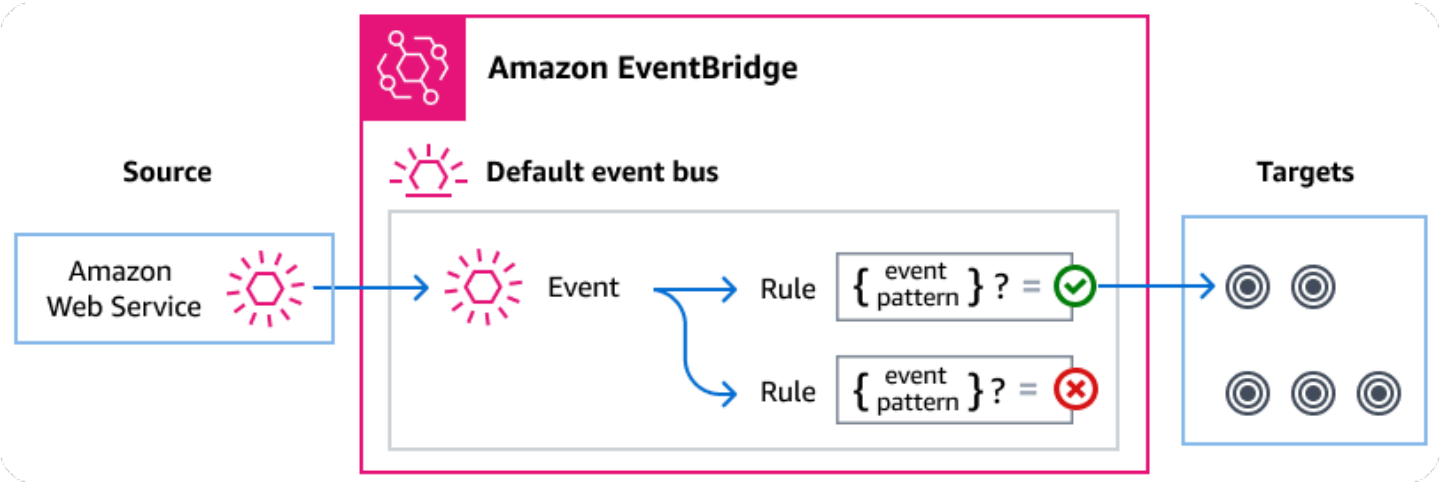
Ejecuta la siguiente consulta para ver las entradas de registro que indican que se ha abierto un archivo.

```
filter `activity-type` = 'OPEN'
| display @timestamp, @logStream, `session-id`, mode, path
```

Gestión de Transfer Family eventos mediante 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. La arquitectura basada en eventos 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 predeterminado. EventBridge 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
- Envío de Transfer Family eventos mediante reglas EventBridge
- Amazon EventBridge permisos
- EventBridge Recursos adicionales
- 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 haciendo todo lo posible; sin embargo, es posible que algunos eventos se entreguen fuera de orden.

Los siguientes eventos son generados por Transfer Family. Para obtener más información, consulte EventBridge los eventos en la Guía Amazon EventBridge del usuario.

Eventos de servidores SFTP, FTPS y FTP

Tipo de detalle del evento	Descripción
Se completó la descarga del servidor de archivos FTP	Se ha descargado correctamente un archivo para el protocolo FTP.
Falló la descarga del servidor de archivos FTP	Se produjo un error al intentar descargar un archivo para el protocolo FTP.
Se completó la carga del servidor de archivos FTP	Se ha cargado correctamente un archivo para el protocolo FTP.
Error al cargar el servidor de archivos FTP	Se produjo un error al intentar cargar un archivo para el protocolo FTP.
Se completó la descarga del servidor de archivos FTPS	Se ha descargado correctamente un archivo para el protocolo FTPS.
Falló la descarga del servidor de archivos FTPS	No se pudo descargar un archivo para el protocolo FTPS.
Se completó la carga del servidor de archivos FTPS	Se ha cargado correctamente un archivo para el protocolo FTPS.
Error al cargar el servidor de archivos FTPS	Se produjo un error al intentar cargar un archivo para el protocolo FTPS.

Tipo de detalle del evento	Descripción
Se completó la descarga del archivo del servidor SFTP	Se ha descargado correctamente un archivo para el protocolo SFTP.
Falló la descarga del archivo del servidor SFTP	No se pudo descargar un archivo para el protocolo SFTP.
Se completó la carga del archivo del servidor SFTP	Se ha cargado correctamente un archivo para el protocolo SFTP.
No se pudo cargar el archivo del servidor SFTP	Se produjo un error al intentar cargar un archivo para el protocolo SFTP.

Eventos del conector SFTP

Tipo de detalle del evento	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.

Eventos A2S

Tipo de detalle del evento	Descripción
Se completó la recepción de carga útil del 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.

Envío de Transfer Family eventos mediante reglas EventBridge

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.

Puede crear una regla siguiendo estos pasos generales:

1. Cree un patrón de eventos para la regla que especifique lo siguiente:
   - Transfer Family es el origen de los eventos que evalúa la regla.

- (Opcional) Cualquier otro dato de evento con el que compararlo.

  Para obtener más información, consulte ???.

2. (Opcional) Cree un transformador de entrada que personalice los datos del evento antes EventBridge de enviar la información al objetivo de la regla.

   Para obtener más información, consulte Transformación de entrada en la Guía del usuario de EventBridge .

3. Especifique los destinos a los que desea EventBridge entregar los eventos que coincidan con el patrón de eventos.

   Los objetivos pueden ser otros AWS servicios, aplicaciones de software como servicio (SaaS), destinos de API u otros puntos finales personalizados. Para más información, consulte Destinos en la Guía del usuario de EventBridge .

Para obtener instrucciones detalladas sobre cómo crear reglas de bus de eventos, consulte Creación de reglas que reaccionan a eventos en la Guía del usuario de EventBridge .

Crear patrones de eventos para eventos Transfer Family

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 correctas para el *nombre* de usuario:

```
{
  "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 .

Probar patrones de Transfer Family eventos para 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 entregar 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 .

EventBridge Recursos adicionales

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 File Server 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

A continuación se muestran los campos detallados de los eventos de los servidores SFTP, FTPS y FTP:

- Se completó la descarga del servidor de archivos FTP
- Falló la descarga del servidor de archivos FTP
- Se completó la carga del servidor de archivos FTP
- Error al cargar el servidor de archivos FTP
- Se completó la descarga del servidor de archivos FTPS
- Falló la descarga del servidor de archivos FTPS
- Se completó la carga del servidor de archivos FTPS
- Error al cargar el servidor de archivos FTPS
- Se completó la descarga del archivo del servidor SFTP
- Falló la descarga 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",
    "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.

`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 del servidor de archivos 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": "/DOC-EXAMPLE-BUCKET/test/1mb_file",
        "server-id": "s-1111aaaa2222bbbb3",
        "username": "test",
        "session-id": "event-ID",
        "start-timestamp": "2024-01-29T16:31:42.462088327Z"
    }
}
```

Eventos del conector SFTP

Los siguientes son los campos de detalle 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

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",
    "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 nombres de directorios o archivos 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 de la lista de archivos/directorios.

`listing-id`

Un identificador único para la llamada a la `StartDirectoryListing` API. Este identificador se puede utilizar para comprobar CloudWatch los registros y ver el estado de la solicitud de anuncio.

`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.

`failure-message`

En el caso de las transferencias fallidas, los detalles del motivo del 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.

`local-file-location`

Este parámetro contiene los detalles de la ubicación del archivo de AWS almacenamiento.

`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": "/DOC-EXAMPLE-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": "DOC-EXAMPLE-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": "/DOC-EXAMPLE-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": "DOC-EXAMPLE-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": "/DOC-EXAMPLE-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": "DOC-EXAMPLE-BUCKET",
            "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
        }
    }
}
```

Eventos AS2

Los siguientes son los campos de detalle de los eventos de AS2:

- Se completó la recepción de la carga útil del AS2
- Falló la recepción de la carga útil del AS2
- Se completó el envío de la carga útil del 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 del 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": "DOC-EXAMPLE-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": "DOC-EXAMPLE-BUCKET1",
          "file-key": "/as2Integ/TestOutboundWrongCert.dat",
          "file-bucket": "DOC-EXAMPLE-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. 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 AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar

la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).

- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

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

- Políticas de seguridad para servidores AWS Transfer Family
- Políticas AWS Transfer Family de seguridad para conectores SFTP
- Uso del intercambio de claves híbrido poscuántico con AWS Transfer Family
- Protección de datos en AWS Transfer Family
- Administración de identidad y acceso para AWS Transfer Family

- Validación de conformidad para AWS Transfer Family
- Resiliencia en AWS Transfer Family
- Seguridad de la infraestructura en AWS Transfer Family
- Agregue un cortafuegos de aplicaciones web
- Prevención de la sustitución confusa entre servicios
- AWS políticas gestionadas para AWS Transfer Family

Políticas de seguridad para servidores AWS Transfer Family

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) y conjuntos de cifrado) asociados a su servidor. 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 Algoritmos admitidos para las claves de usuario y del servidor.

> **Note**
>
> Le recomendamos encarecidamente que actualice sus servidores a nuestra política de seguridad más reciente. Nuestra política de seguridad más reciente es la predeterminada. A cualquier cliente que cree un servidor Transfer Family utilizando CloudFormation y aceptando la política de seguridad predeterminada se le asignará automáticamente la última política.
> 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, consulteEditar la política de seguridad.

Para obtener más información sobre la seguridad de Transfer Family, consulta la entrada del blog Cómo Transfer Family puede ayudarte a crear una solución de transferencia de archivos gestionada segura y compatible.

Temas

- Algoritmos criptográficos
- TransferSecurityPolítica-2024-01

- TransferSecurityPolítica-2023-05
- TransferSecurityPolítica-2022-03
- TransferSecurityPolítica-2020-06
- TransferSecurityPolítica-2018-11
- TransferSecurityPolítica-FIPS-2024-01/ Política-FIPS-2024-05 TransferSecurity
- TransferSecurityPolítica-FIPS-2023-05
- TransferSecurityPolítica: FIPS-2020-06
- Políticas de seguridad poscuánticas

> **Note**
>
> `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.

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`:

- TransferSecurityPolítica-2018-11
- TransferSecurityPolítica-2020-06
- TransferSecurityPolítica-FIPS-2020-06
- TransferSecurityPolítica-FIPS-2023-05

- TransferSecurityPolítica-FIPS-2024-01
- TransferSecurityPolítica-PQ-SSH-FIPS-Experimental-2023-04

> **Note**
>
> Es importante entender la diferencia entre el tipo de clave RSA (que siempre es así) y el algoritmo de clave de host RSA, que puede ser cualquiera de los algoritmos compatibles. `ssh-rsa`

La siguiente es una lista de los algoritmos criptográficos admitidos con cada política de seguridad.

> **Note**
>
> En la tabla y las políticas siguientes, anote el siguiente uso de los tipos de algoritmos.
>
> - Los servidores SFTP solo utilizan algoritmos en las SshMacssecciones SshCiphersSshKexs, y.
> - Los servidores FTPS solo utilizan los algoritmos de la TlsCipherssección.
> - Los servidores FTP, dado que no utilizan cifrado, no utilizan ninguno de estos algoritmos.
> - Las políticas de seguridad FIPS-2024-05 y FIPS-2024-01 son idénticas, excepto que FIPS-2024-05 no admite el algoritmo. `ssh-rsa`

Política de seguridad	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
SshCiphers								
aes128-ctr	♦			♦	♦		♦	♦
aes128-gc	♦	♦	♦	♦	♦	♦	♦	♦

Política de seguridad	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
m@openssh.com								
aes192-ctr	♦	♦	♦	♦	♦	♦	♦	♦
aes256-ctr	♦	♦	♦	♦	♦	♦	♦	♦
aes256-gcm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦
chacha20-poly1305@openssh.com				♦				♦
SshKexs								
curva25519-sha256	♦	♦	♦					♦
curve25519-sha256@libssh.org	♦	♦	♦					♦

Política de seguridad	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
diffie-hellman-group14-sha1								♦
diffie-hellman-group14-sha256				♦			♦	♦
diffie-hellman-group16-sha512	♦	♦	♦	♦	♦	♦	♦	♦
diffie-hellman-grupo18-sha512	♦	♦	♦	♦	♦	♦	♦	♦
diffie-hellman-group-exchange-sha256		♦	♦	♦		♦	♦	♦

Política de seguridad	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
ecdh-nist p256-kyber-512r3-sha256-d00 @openquantumsafe.org	♦				♦			
ecdh-nist p384-kyber-768r3-sha384-d00 @openquantumsafe.org	♦				♦			

Política de seguridad	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org	♦				♦			
ecdh-sha2-nistp256	♦			♦	♦		♦	♦
ecdh-sha2-nistp384	♦			♦	♦		♦	♦
ecdh-sha2-nistp521	♦			♦	♦		♦	♦
x25519-kyber-512r3-sha256-d00@amazon.com	♦							

Política de seguridad	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
SshMacs								
hmac-sha1								♦
hmac-sha1-etm@openssh.com								♦
hmac-sha2-256			♦	♦			♦	♦
hmac-sha2-256-etm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦
hmac-sha2-512			♦	♦			♦	♦
hmac-sha2-512-etm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦

Política de seguridad	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
umac-128-etm@openssh.com				♦				♦
umac-128@openssh.com				♦				♦
umac-64-etm@openssh.com								♦
umac-64@openssh.com								♦
TlsCiphers								
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256		♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256		♦	♦	♦	♦	♦	♦	♦

Política de seguridad	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	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	♦	♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	♦	♦	♦	♦	♦	♦	♦	♦

Política de seguridad	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	♦	♦	♦	♦	♦	♦	♦	♦
TLS_RSA_WITH_AES_128_CBC_SHA256								♦
TLS_RSA_WITH_AES_256_CBC_SHA256								♦

TransferSecurityPolítica-2024-01

A continuación se muestra la política de seguridad TransferSecurityPolicy -2024-01.

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-2024-01",
        "SshCiphers": [
            "aes128-gcm@openssh.com",
            "aes256-gcm@openssh.com",
            "aes128-ctr",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
```

```
            "x25519-kyber-512r3-sha256-d00@amazon.com",
            "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
            "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
            "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"
        ],
        "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"
        ]
    }
}
```

TransferSecurityPolítica-2023-05

A continuación se muestra la política de seguridad de TransferSecurityPolicy -2023-05.

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

TransferSecurityPolítica-2022-03

A continuación se muestra la política de seguridad del TransferSecurityPolicy -2022-03.

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

TransferSecurityPolítica-2020-06

A continuación se muestra la política de seguridad de la versión TransferSecurityPolicy -2020-06.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com",
      "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"
    ],
    "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"
    ]
  }
}
```

TransferSecurityPolítica-2018-11

A continuación se muestra la política de seguridad del modelo TransferSecurityPolicy -2018-11.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com",
      "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"
    ],
    "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"
    ]
  }
}
```

TransferSecurityPolítica-FIPS-2024-01/ Política-FIPS-2024-05 TransferSecurity

A continuación se muestran las políticas de seguridad -FIPS-2024-01 y TransferSecurityPolicy -FIPS-2024-05. TransferSecurityPolicy

> **Note**
>
> El punto final del servicio FIPS y las políticas de seguridad -FIPS-2024-01 y -FIPS-2024-05 solo están disponibles en algunas regiones. TransferSecurityPolicy TransferSecurityPolicy AWS 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 -FIPS-2024-01 es compatible con el algoritmo y -FIPS-2024-05 no. TransferSecurityPolicy `ssh-rsa` TransferSecurityPolicy


```
{
    "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-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
            "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
            "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
            "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"
        ],
        "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"
        ]
    }
}
```

TransferSecurityPolítica-FIPS-2023-05

Los detalles de la certificación FIPS se encuentran en AWS Transfer Family https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all

A continuación se muestra la política de seguridad TransferSecurityPolicy -FIPS-2023-05.

> **Note**
>
> El punto final del servicio FIPS y la política de seguridad TransferSecurityPolicy -FIPS-2023-05 solo están disponibles en algunas regiones. AWS 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"
        ],
        "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"
        ]
    }
}
```

TransferSecurityPolítica: FIPS-2020-06

Los detalles de la certificación FIPS se encuentran en AWS Transfer Family https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all

A continuación se muestra la política de seguridad TransferSecurityPolicy -FIPS-2020-06.

> **Note**
>
> El punto final del servicio FIPS y la política de seguridad TransferSecurityPolicy -FIPS-2020-06 solo están disponibles en algunas regiones. AWS 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"
    ],
    "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"
    ]
  }
}
```

Políticas de seguridad poscuánticas

En esta tabla, se enumeran los algoritmos de las políticas de seguridad poscuántica de Transfer Family. Estas políticas se describen en detalle en Uso del intercambio de claves híbrido poscuántico con AWS Transfer Family.

La lista de políticas sigue la tabla.

Política de seguridad	TransferSecurityPolítica-PQ-SSH-Experimental-2023-04	TransferSecurityPolítica-PQ-SSH-FIPS-Experimental-2023-04
SSH ciphers		
aes128-ctr		♦

Política de seguridad	TransferSecurityPolítica-PQ-SSH-Experimental-2023-04	TransferSecurityPolítica-PQ-SSH-FIPS-Experimental-2023-04
aes128-gcm@openssh.com	♦	♦
aes192-ctr	♦	♦
aes256-ctr	♦	♦
aes256-gcm@openssh.com	♦	♦
KEXs		
ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org	♦	♦
ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org	♦	♦
ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org	♦	♦
x25519-kyber-512r3-sha256-d00@amazon.com	♦	
diffie-hellman-group14-sha256		♦
diffie-hellman-group16-sha512	♦	♦
diffie-hellman-grupo18-sha512	♦	♦
ecdh-sha2-nistp384		♦
ecdh-sha2-nistp521		♦
diffie-hellman-group-exchange-sha256	♦	♦

Política de seguridad	TransferSecurityPolítica-PQ-SSH-Experimental-2023-04	TransferSecurityPolítica-PQ-SSH-FIPS-Experimental-2023-04
ecdh-sha2-nistp256		♦
curve25519-sha256@libssh.org	♦	
curva 25519-sha256	♦	
MACs		
hmac-sha2-256-etm@openssh.com	♦	♦
hmac-sha2-256	♦	♦
hmac-sha2-512-etm@openssh.com	♦	♦
hmac-sha2-512	♦	♦
TLS ciphers		
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	♦	♦
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	♦	♦

Política de seguridad	TransferSecurityPolítica-PQ-SSH-Experimental-2023-04	TransferSecurityPolítica-PQ-SSH-FIPS-Experimental-2023-04
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	♦	♦

TransferSecurityPolítica-PQ-SSH-Experimental-2023-04

A continuación se muestra la política de seguridad del -PQ-SSH-Experimental-2023-04. TransferSecurityPolicy

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-PQ-SSH-Experimental-2023-04",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
            "x25519-kyber-512r3-sha256-d00@amazon.com",
            "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
            "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
            "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"
        ],
        "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"
        ]
    }
}
```

TransferSecurityPolítica-PQ-SSH-FIPS-Experimental-2023-04

A continuación se muestra la política de seguridad del -PQ-SSH-FIPS-Experimental-2023-04. TransferSecurityPolicy

```
{
    "SecurityPolicy": {
        "Fips": true,
        "SecurityPolicyName": "TransferSecurityPolicy-PQ-SSH-FIPS-
Experimental-2023-04",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes256-ctr",
            "aes192-ctr",
            "aes128-ctr"
        ],
        "SshKexs": [
            "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
            "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
            "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.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"
        ],
        "SshMacs": [
            "hmac-sha2-512-etm@openssh.com",
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512",
            "hmac-sha2-256"
        ],
        "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"
        ]
    }
}
```

Políticas AWS Transfer Family de seguridad para 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 con 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.

Política de seguridad	Política de transferencias FTP: 2024-03 ConnectorSecurity	ConnectorSecurityPolítica de transferencias FTP - 2023-07
Ciphers		
aes128-ctr		♦
aes128-gcm@openssh.com	♦	♦
aes192-ctr	♦	♦
aes256-ctr	♦	♦
aes256-gcm@openssh.com	♦	♦
Kexs		
curva 25519-sha256	♦	♦
curve25519-sha256@libssh.org	♦	♦
diffie-hellman-group14-sha1		♦
diffie-hellman-group16-sha512	♦	♦
diffie-hellman-grupo18-sha512	♦	♦
diffie-hellman-group-exchange-sha256	♦	♦
Macs		
hmac-sha2-512-etm@openssh.com	♦	♦
hmac-sha2-256-etm@openssh.com	♦	♦
hmac-sha2-512	♦	♦
hmac-sha2-256	♦	♦

Política de seguridad	Política de transferencias FTP: 2024-03 ConnectorSecurity	ConnectorSecurityPolítica de transferencias FTP - 2023-07
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 de claves híbrido poscuántico con AWS Transfer Family

AWS Transfer Family admite una opción híbrida de establecimiento de claves poscuánticas para el protocolo Secure Shell (SSH). El establecimiento de claves poscuánticas es necesario porque ya es posible registrar el tráfico de la red y guardarlo para su descifrado en el futuro mediante una computadora cuántica, lo que se denomina ataque de almacenar ahora, recopilar después.

Puede utilizar esta opción cuando se conecte a Transfer Family para realizar transferencias de archivos seguras hacia y desde el almacenamiento de Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS). El establecimiento híbrido de claves poscuánticas en SSH introduce mecanismos de establecimiento de claves poscuánticas, 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 la criptografía poscuántica.

Contenido

- Acerca del intercambio de claves híbrido poscuántico en SSH
- Cómo funciona el establecimiento de claves híbrido poscuántico en Transfer Family
  - ¿Por qué Kyber?
  - Requisitos criptográficos y de intercambio de claves híbrido poscuántico SSH (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 clásico algoritmo de intercambio de claves Elliptic Curve Diffie-Hellman (ECDH, curva elíptica de Diffie-Hellman) como CRYSTALS Kyber. Kyber es un algoritmo de cifrado y establecimiento de claves públicas poscuántico que el National Institute for Standards and Technology (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 su compatibilidad con el intercambio de claves poscuánticas en las transferencias de archivos SFTP en. AWS Transfer Family Transfer Family escala de forma segura las transferencias de business-to-business archivos a los servicios de AWS 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.

La compatibilidad del intercambio de claves híbrido poscuántico SFTP de Transfer Family incluye la combinación de los algoritmos poscuánticos Kyber-512, Kyber-768 y Kyber-1024, con ECDH sobre las curvas P256, P384, P521 o Curve25519. Los siguientes métodos de intercambio de claves SSH correspondientes se especifican en el borrador del intercambio de claves híbrido poscuántico SSH.

- `ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org`
- `ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org`
- `ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org`
- `x25519-kyber-512r3-sha256-d00@amazon.com`

> **Note**
>
> Estos nuevos métodos de intercambio de claves pueden cambiar a medida que el borrador avance hacia la estandarización o cuando el NIST ratifique el algoritmo Kyber.

¿Por qué Kyber?

AWS se compromete a respaldar algoritmos estandarizados e interoperables. Kyber es el primer algoritmo de cifrado poscuántico seleccionado para su estandarización por el proyecto de criptografía

poscuántica del NIST. Algunos organismos de normalización ya están integrando Kyber en los protocolos. AWS ya es compatible con Kyber en TLS en algunos AWS puntos finales de API.

Como parte de este compromiso, AWS ha presentado un borrador de propuesta al IETF para la criptografía poscuántica que combina Kyber con curvas aprobadas por el NIST, 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.

Estos nuevos métodos de intercambio de claves (en la sección Cómo funciona el establecimiento de claves híbrido poscuántico en Transfer Family) pueden cambiar a medida que el borrador avance hacia la estandarización o cuando el NIST ratifique el algoritmo Kyber.

> **Note**
>
> Actualmente, se admite el uso de algoritmos poscuánticos para el intercambio de claves híbridas poscuánticas en TLS AWS KMS (consulte Uso del TLS poscuántico híbrido con) y puntos finales de API. AWS KMSAWS Certificate Manager AWS Secrets Manager

Requisitos criptográficos y de intercambio de claves híbrido poscuántico SSH (FIPS 140)

Para los clientes que requieren el cumplimiento de FIPS, Transfer Family proporciona criptografía aprobada por FIPS en SSH mediante la biblioteca criptográfica de código abierto con certificación AWS FIPS 140, -LC. AWSLos métodos de intercambio de claves híbridos poscuánticos compatibles con el TransferSecurityPolicy -PQ-SSH-FIPS-Experimental-2023-04 de 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

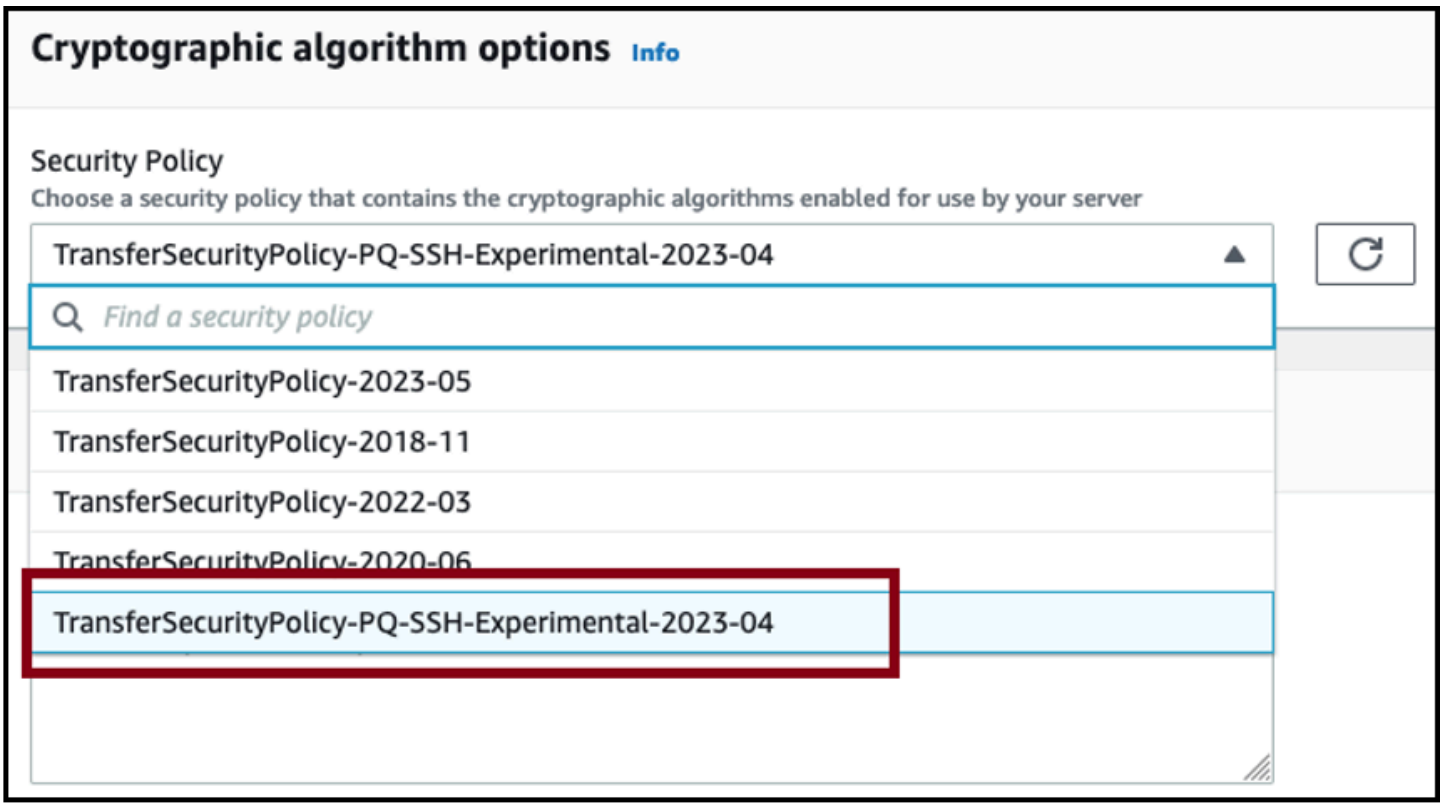
En esta sección, se describen los pasos que debe seguir para probar el intercambio de claves híbrido poscuántico.

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 de la AWS Management Console dónde actualiza la política SSH.



Los nombres de las políticas de SSH que admiten el intercambio de claves poscuántico son Policy-PQ-SSH-Experimental-2023-04 TransferSecurity TransferSecurityy Policy-PQ-SSH-FIPS-Experimental-2023-04. Para obtener más información sobre las políticas de Transfer Family, consulte Políticas de seguridad para servidores AWS Transfer Family.

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. Utilice un cliente SFTP (por ejemplo, OQS OpenSSH) que admita el intercambio de claves híbrido poscuántico siguiendo las instrucciones de la especificación del borrador mencionado anteriormente.

Open Quantum Safe (OQS) OpenSSH es una ramificación de código abierto de OpenSSH que añade criptografía de seguridad cuántica a SSH mediante el uso de `liboqs`. `liboqs` es una biblioteca C de código abierto que implementa algoritmos criptográficos resistentes a la información cuántica. OQS OpenSSH y `liboqs` forman parte del proyecto Open Quantum Safe (OQS).

Para probar el intercambio de claves híbrido poscuántico SFTP en Transfer Family con OQS OpenSSH, debe compilar OQS OpenSSH como se explica en el README del proyecto. Después de crear OQS OpenSSH, puede ejecutar el cliente SFTP de ejemplo para conectarse a su punto de conexión SFTP (por ejemplo, `s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com`) mediante los métodos de intercambio de claves híbrido poscuántico, como se muestra en el siguiente comando.

```
./sftp -S ./ssh -v -o \
   KexAlgorithms=ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org \
   -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:

- Reemplace *username_private_key_PEM_file* por el archivo de clave privada codificado en Privacy Enhanced Mail (PEM, correo de privacidad mejorada) del usuario SFTP
- Sustituya *nombre de usuario* por el nombre de usuario de SFTP
- Reemplace el *server-id* por el ID de servidor de Transfer Family
- Reemplace el *region-id* 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 Open Quantum Safe OpenSSH, la salida debería tener un aspecto similar al siguiente (se omite información irrelevante por motivos de brevedad):

```
$./sftp -S ./ssh -v -o KexAlgorithms=ecdh-nistp384-kyber-768r3-sha384-
d00@openquantumsafe.org -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_8.9-2022-01_p1, Open Quantum Safe 2022-08, OpenSSL 3.0.2 15 Mar 2022
debug1: Reading configuration data /home/lab/openssh/oqs-test/tmp/ssh_config
debug1: Authenticator provider $SSH_SK_PROVIDER did not resolve; disabling
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
 [xx.yy.zz..12] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_8.9-2022-01_
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 /home/lab/.ssh/known_hosts2: No such file or directory
[...]
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes192-ctr MAC: hmac-sha2-256-etm@openssh.com
 compression: none
debug1: kex: client->server cipher: aes192-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:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649
[...]
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 AWS.Tranfer.PQ.SFTP.test-endpoint.aws.com ([xx.yy.zz..12]:22) using
 "publickey".s
debug1: channel 0: new [client-session]
```

```
[...]
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 `ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org` y que se estableció correctamente una sesión SFTP.

Protección de datos en AWS Transfer Family

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. Usted es 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 AWS Identity and Access Management (IAM). 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:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS 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.

Temas

- Cifrado de datos en Amazon S3
- Administración de claves SSH y PGP en Transfer Family

Cifrado de datos en Amazon S3

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 (SSE-KMS AWS 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"
 ],
 "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 de claves de AWS KMS debe permitir el rol raíz o el rol de IAM que se utiliza para el usuario. Para obtener información sobre la política de AWS KMS claves, consulte Uso de políticas clave en AWS KMS en la Guía para AWS Key Management Service desarrolladores.

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 A AWS Transfer Family y AWS Lambda.

> **Note**
>
> AWS Transfer Family acepta claves RSA, ECDSA y ED25519.

En esta sección también se explica cómo generar y administrar las claves Pretty Good Privacy (PGP).

Temas

- Algoritmos admitidos para las claves de usuario y del servidor
- Genere claves SSH para los usuarios administrados por el servicio
- Rotar claves SSH
- Genere y administre claves PGP
- Clientes PGP admitidos

Algoritmos admitidos para las claves de usuario y del servidor

Los siguientes algoritmos clave son admitidos con los pares de claves de usuario y de servidor dentro de AWS Transfer Family.

> **Note**
>
> Para ver los algoritmos que se pueden usar con el descifrado PGP en los flujos de trabajo, consulte Algoritmos admitidos con los pares de claves PGP.

- Para ED25519: `ssh-ed25519`
- Para RSA (Rivest, Shamir y Adleman):
  - `rsa-sha2-256`
  - `rsa-sha2-512`
- Para ECDSA:
  - `ecdsa-sha2-nistp256`
  - `ecdsa-sha2-nistp384`
  - `ecdsa-sha2-nistp521`

> **Note**
>
> Admitimos `ssh-rsa` con SHA1 para nuestras políticas de seguridad más antiguas. Para obtener más detalles, consulte Algoritmos criptográficos.

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 bien. AWS Directory Service for Microsoft Active Directory Para obtener más información, consulte Uso de proveedores de identidad personalizados o Uso del proveedor de identidad de AWS Directory Service.

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
- Convierta una clave pública SSH2 a formato PEM

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.

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 claves con formato RSA, ECDSA y ED25519. Elija el comando apropiado en función del tipo de par de claves que esté generando.

> **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.

- 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
```

> **Note**
>
> *key_name* es el nombre del archivo del par de claves SSH.

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:
SHA256:8tDDwPmanTFcEzjTwPGETVWOGW1nVz+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]-----+
```

> **Note**
>
> Al ejecutar `ssh-keygen` como se ha mostrado, el comando 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.

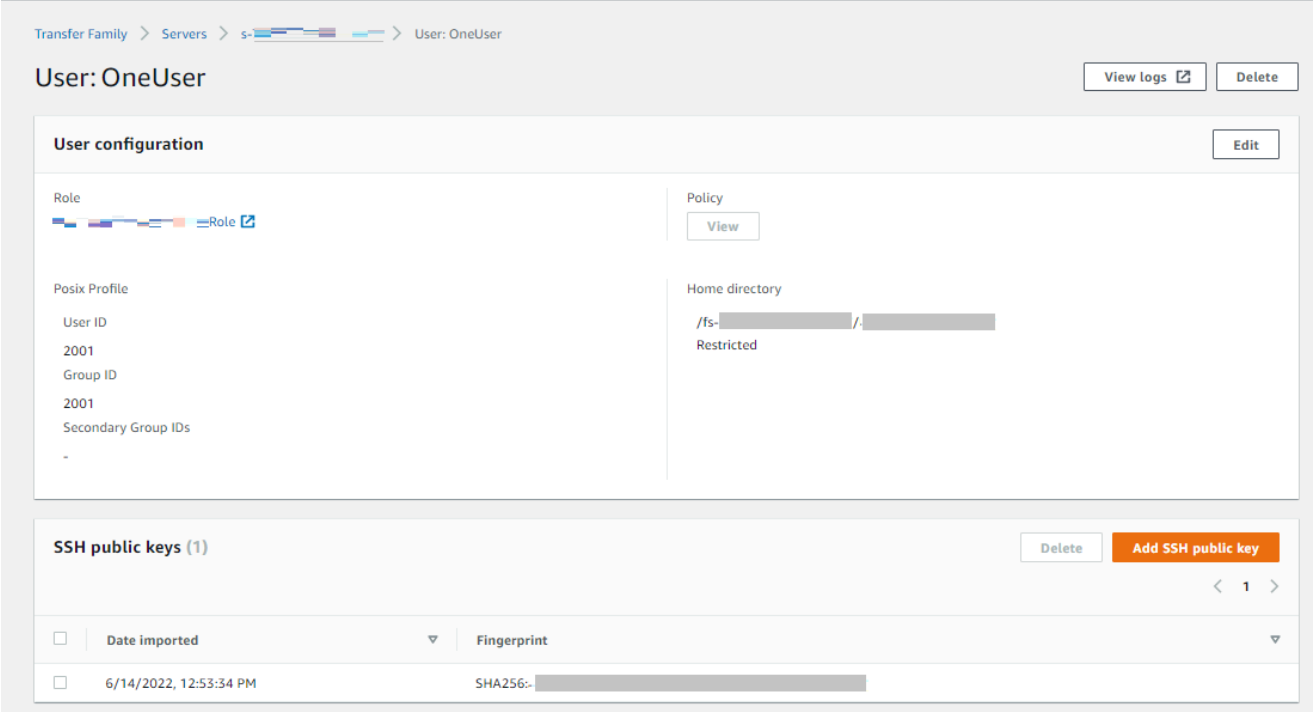
3. Desplácese hasta el archivo *`key_name`*`.pub` y ábralo.
4. Copie el texto y péguelo en la clave pública SSH del usuario administrado por el servicio.

   a. Abra la AWS Transfer Family consola en https://console.aws.amazon.com/transfer/ y, a continuación, seleccione Servidores en el panel de navegación.

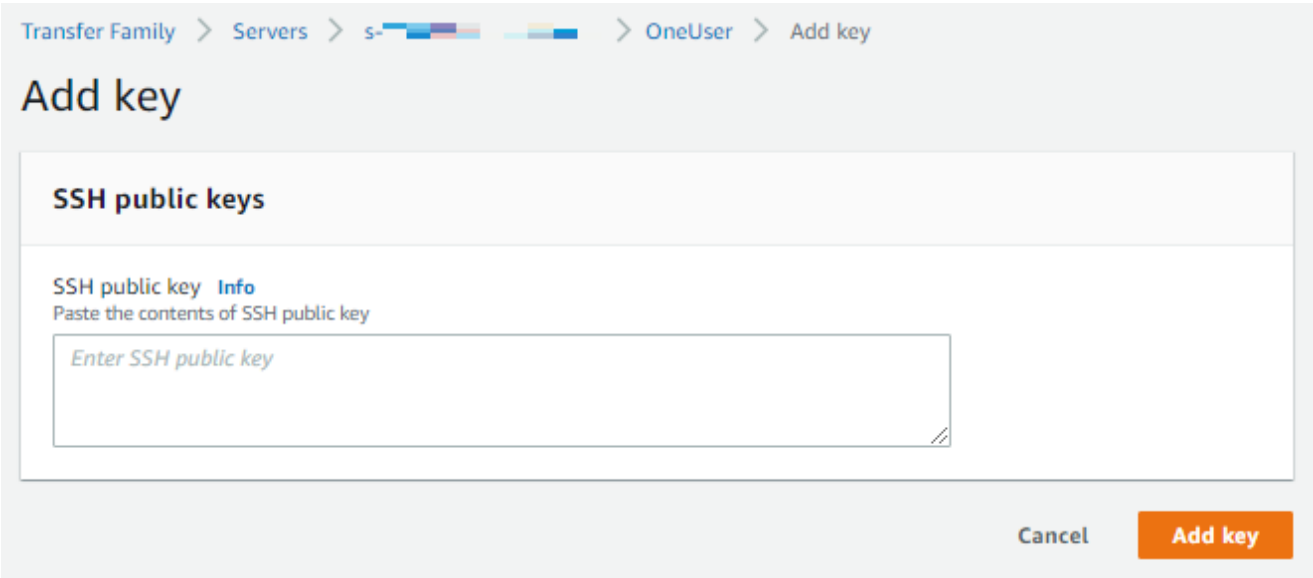
b. En la página Servidores, seleccione el ID de servidor para el servidor que contiene el usuario que desea actualizar.

c. Seleccione el usuario para el que va a añadir una clave pública.

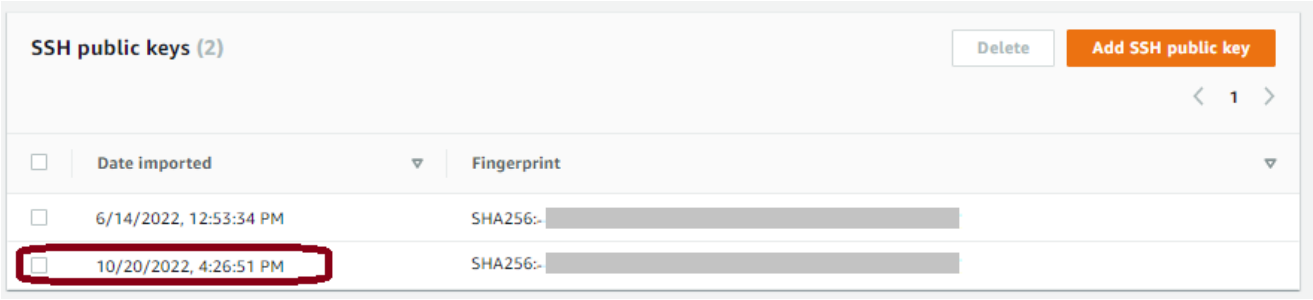
d. En el panel de claves públicas SSH, seleccione Añadir clave pública SSH.



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.



Creación de claves SSH en Microsoft Windows

Windows utiliza un formato ligeramente distinto para el par de claves SSH. La clave pública debe tener el formato PUB, mientras que la clave privada debe tener el formato PPK. En Windows, puede utilizar PuTTYgen para crear un par de claves SSH con los formatos correctos. También puede utilizar PuTTYgen para convertir una clave privada generada con `ssh-keygen` en un archivo `.ppk`.

> **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 la creación de claves SSH con PuTTYgen en Windows, consulte el sitio web SSH.com.

Convierta una clave pública SSH2 a formato PEM

AWS Transfer Family solo acepta claves públicas con formato PEM. Si tiene una clave pública SSH2, debe convertirla. Una clave pública SSH2 tiene el siguiente formato:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20160402"
AAAAB3NzaC1yc2EAAAABJQAAAgEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI
:
:
---- END SSH2 PUBLIC KEY ----
```

Una clave pública PEM tiene el siguiente formato:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

Ejecute el siguiente comando para convertir una clave pública con formato SSH2 en una clave pública con formato PEM. Reemplace *ssh2-key* por el nombre de su clave SSH2, y la *clave PEM* por el nombre de su clave PEM.

```
ssh-keygen -i -f ssh2-key.pub > PEM-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.

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 DeleteSshPublicKeyAPI para eliminar la clave pública de Secure Shell (SSH) de un usuario y la ImportSshPublicKeyAPI 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.

Genere y administre 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.

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

Generar claves PGP

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, puede descargar lo que necesite desde 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). Sin embargo, si elige ECC, asegúrese de seleccionar una NIST o BrainPool para la curva elíptica. No seleccione Curve 25519.

Algoritmos admitidos con los pares de claves PGP

Admitimos los siguientes algoritmos para los pares de claves PGP:

- RSA
- ElGamal
- ECC:
  - NIST
  - BrainPool

> **Note**
>
> No admitimos las claves CCurve25519.

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 claves PGP que no utilice un algoritmo de cifrado Curve 25519.

   - Si utiliza la versión 2.3.0 de **GnuPG** o posterior, ejecute el siguiente comando:

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

     Puede elegir **RSA** o, si elige **ECC**, puede elegir **NIST** o **BrainPool** para la curva elíptica. Si ejecuta `gpg --gen-key` en su lugar, cree un par de claves que utilice el algoritmo de cifrado ECC Curve 25519, que, actualmente, no admitimos para las claves PGP.

   - 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 frase de contraseña cuando introduzca los detalles de la clave en AWS Secrets Manager más adelante en 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. Se usa AWS Secrets Manager para almacenar la clave PGP.

   a. Inicie sesión AWS Management Console 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 Pares clave-valor, seleccione la pestaña Clave/valor.

      - 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-----`.

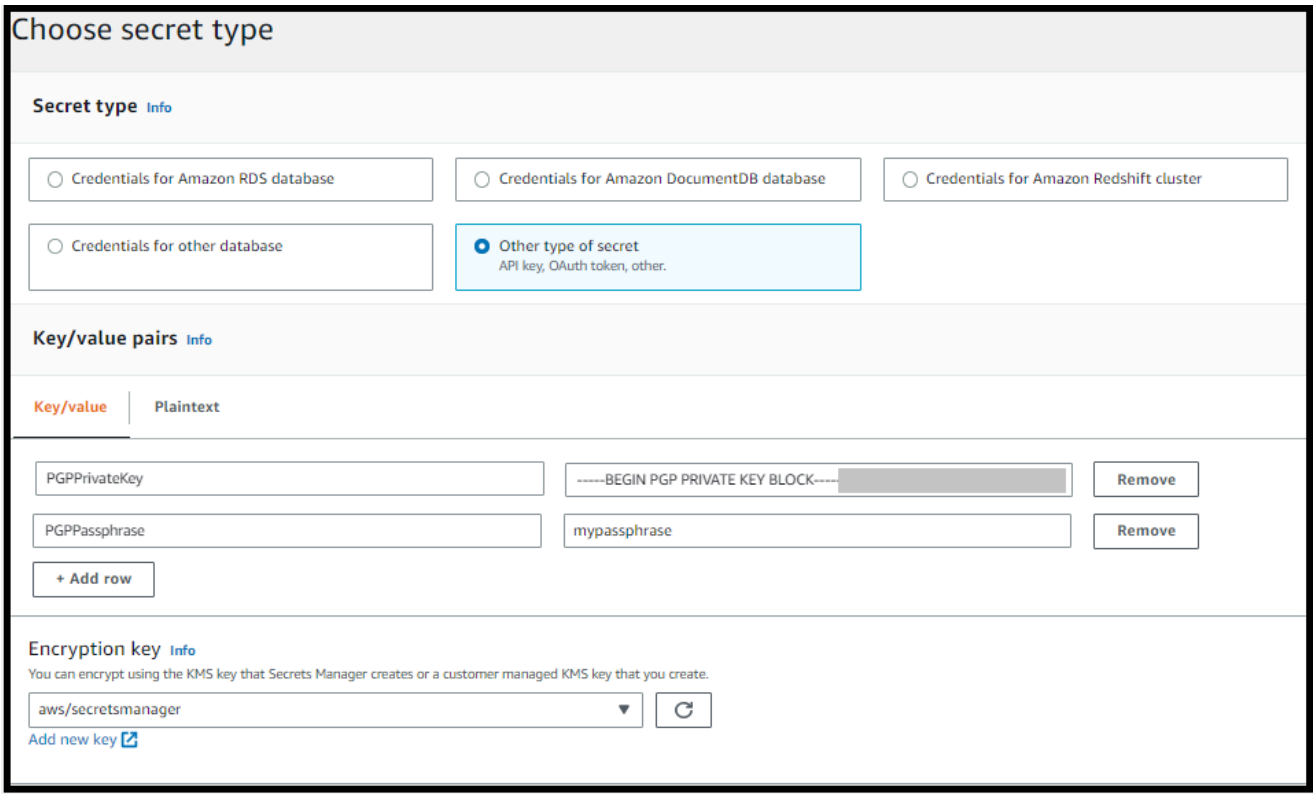
        > **Note**
        >
        > Asegúrese de que el bloque de texto contenga solo la clave privada y que no contenga también la clave pública.

   f. Seleccione Agregar fila y en la sección Pares clave/valor, seleccione la pestaña Clave/valor.

      - 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.



> **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.

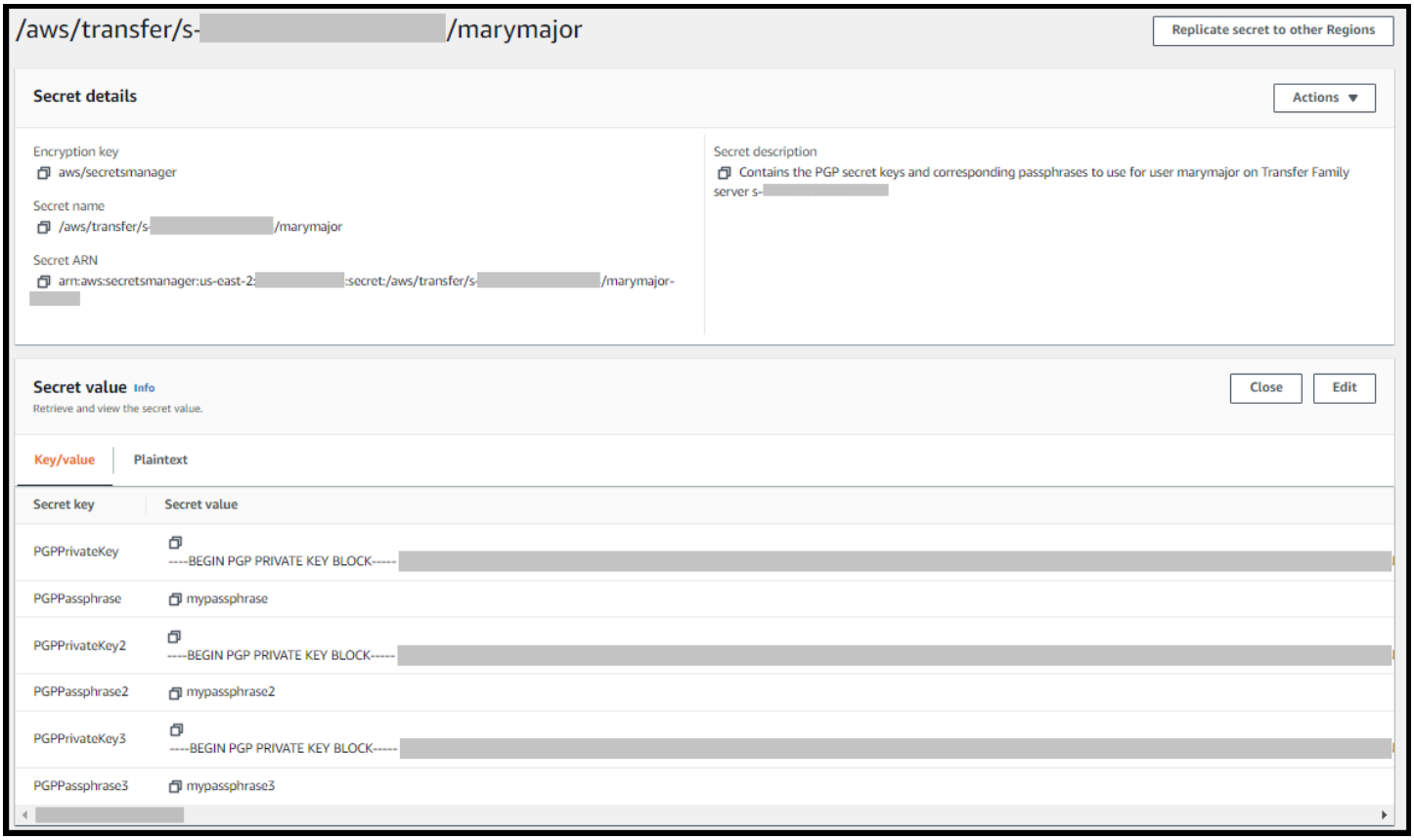
h. En la página Configurar secreto, introduzca un nombre y una descripción para el secreto.

- 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.

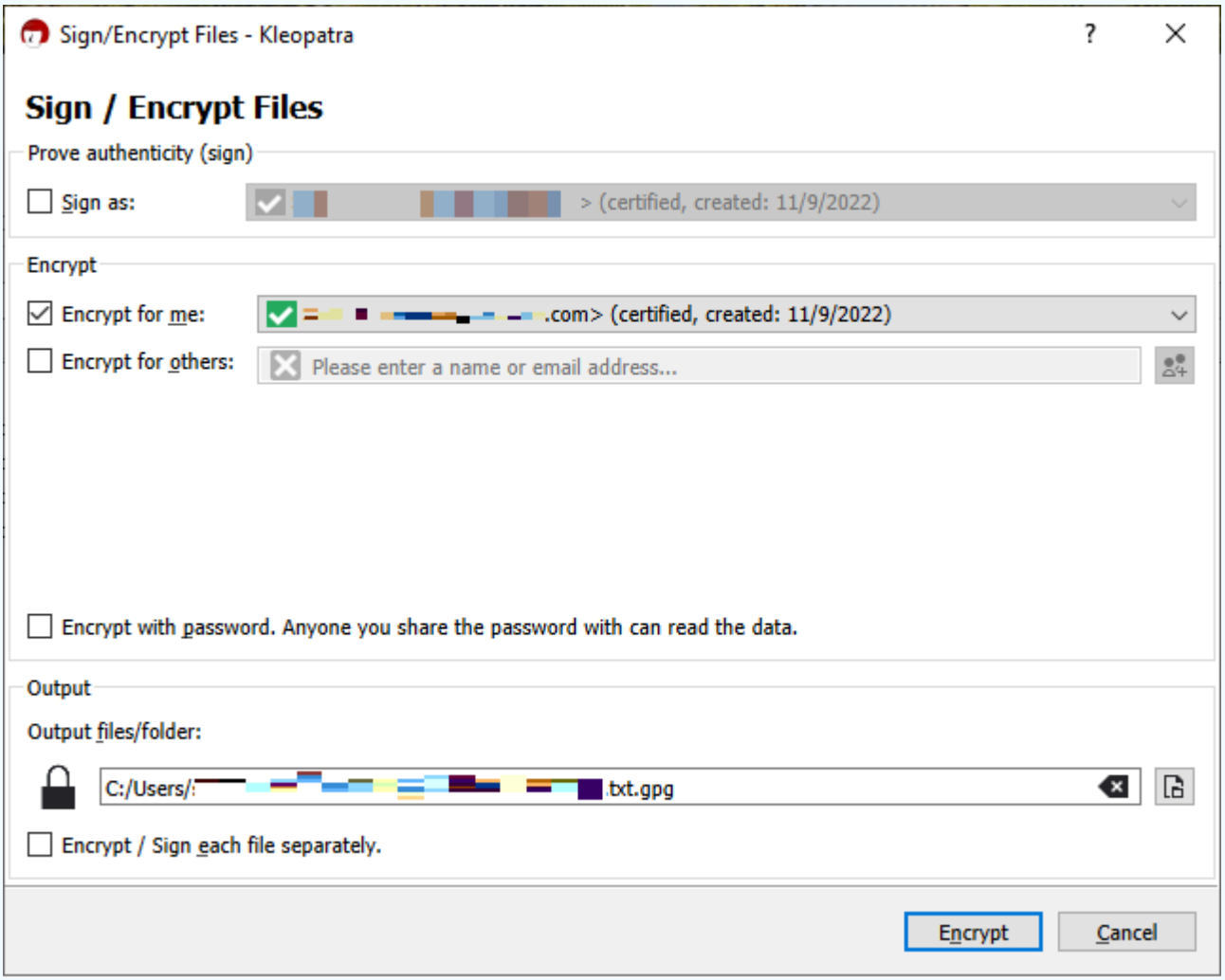


Clientes PGP admitidos

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 de acceso mediante políticas
- ¿Cómo AWS Transfer Family funciona con IAM
- AWS Transfer Family ejemplos de políticas basadas en la identidad
- AWS Transfer Family ejemplos de políticas basadas en etiquetas
- Solución de problemas AWS Transfer Family de identidad y acceso

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS Transfer Family

Usuario del servicio: si utiliza el AWS Transfer Family servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS Transfer Family funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en AWS Transfer Family, consulte Solución de problemas AWS Transfer Family de identidad y acceso.

Administrador de servicios: si estás a cargo de AWS Transfer Family los recursos de tu empresa, probablemente tengas acceso total a ellos AWS Transfer Family. Su trabajo consiste en determinar

a qué AWS Transfer Family funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM AWS Transfer Family, consulte¿Cómo AWS Transfer Family funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS. Para ver ejemplos de políticas AWS Transfer Family basadas en la identidad que puede utilizar en IAM, consulte. AWS Transfer Family ejemplos de políticas basadas en la identidad

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Usuario raíz de la cuenta de AWS

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos de Servicios de AWS la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como 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, incluidos los que requieren acceso de administrador, 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 de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. 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 propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener

información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

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.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una

política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son 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. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas 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 y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites

de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para 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 AWS determinar 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 usar AWS Identity and Access Management (IAM) para administrar el acceso AWS Transfer Family, debe comprender con qué funciones de IAM está disponible. 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

- Políticas de AWS Transfer Family basadas en identidades
- Políticas de AWS Transfer Family basadas en recursos
- Autorización basada en etiquetas de AWS Transfer Family

- AWS Transfer Family Funciones de IAM

Políticas de AWS Transfer Family basadas en identidades

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. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, 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` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una sola clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. 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 la identidad

Políticas de AWS Transfer Family basadas en recursos

Las políticas basadas en recursos son documentos de políticas de JSON que especifican qué acciones puede realizar un director específico en el AWS Transfer Family recurso y en qué condiciones. Amazon S3 admite políticas de permisos basadas en recursos para *buckets* de Amazon S3. Las políticas basadas en recursos le permiten otorgar permiso de uso a otras cuentas por recurso. *También puede usar una política basada en recursos para permitir que un AWS servicio acceda a sus buckets de Amazon S3.*

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 de Amazon S3 solo admite un tipo de política basada en recursos denominada política de *bucket*, que se adjunta a un *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 etiquetas de AWS Transfer Family

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, consulteAWS Transfer Family ejemplos de políticas basadas en etiquetas.

AWS Transfer Family Funciones 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 la AWS STS API, como AssumeRoleo GetFederationToken.

AWS Transfer Family admite el uso de credenciales temporales.

AWS Transfer Family ejemplos de políticas basadas en la identidad

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 API AWS Management Console AWS CLI, o AWS . 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

- Mediante la consola de AWS Transfer Family
- Permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad 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 trabajo 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 AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice 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 Política de validación de Analizador de acceso de IAM en la Guía de 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 solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de AWS Transfer Family

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 los recursos de AWS Transfer Family

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 los recursos, consulte Etiquetar AWS los 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"
                ]
            }
        }
    }
]
}
```

Solución de problemas AWS Transfer Family de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales 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 accedan a mis AWS Transfer Family recursos

No estoy autorizado a realizar ninguna acción en AWS Transfer Family

Si AWS Management Console 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 `mateojackson` de IAM, intenta utilizar la consola para ver detalles sobre un *`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.

Algunas 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 el rol 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 administrador. AWS 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.

```
{
   "Version": "2012-10-17",
   "Statement": [
      { "Action": "iam:PassRole",
        "Resource": "arn:aws::iam::123456789012:role/*",
        "Effect": "Allow"
      }
   ]
}
```

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis AWS Transfer Family recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. 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 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 obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Validación de conformidad para AWS Transfer Family

Los auditores externos evalúan la seguridad y el cumplimiento AWS Transfer Family como parte de varios programas de AWS cumplimiento. 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 para la seguridad y el cumplimiento de la HIPAA: este documento técnico describe cómo las empresas pueden utilizar para crear aplicaciones que cumplan con la HIPAA. AWS
- 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— 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.

Tenga en cuenta lo siguiente:

- Para puntos de conexión públicos:
  - La redundancia de nivel de zona de disponibilidad está integrada en el servicio
  - Hay flotas redundantes para cada zona de disponibilidad.
  - Esta redundancia se proporciona de forma automática
- Para más información sobre los puntos de conexión en una nube privada virtual (VPC), consulte Creación de un servidor en una nube privada virtual (VPC).

Véase también

- 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 crear una mayor redundancia y minimizar la latencia de la red mediante el enrutamiento basado en la latencia, consulte la entrada del blog Minimice la latencia de la red con sus servidores. AWS Transfer Family

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.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

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. Seleccione Guardar cambios.
8. Elija Recursos.
9. Para Acciones, elija Implementar API.

Para obtener información sobre el grado de seguridad AWS Transfer Family con el firewall de aplicaciones AWS web, consulte Protección AWS Transfer Family con el firewall de AWS aplicaciones y Amazon API Gateway en el blog sobre AWS almacenamiento.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio 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`y 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 ejemplos siguientes, reemplace cada *`marcador de posición del usuario`* con 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": "account-id"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:region:account-id: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": "account-id"
                },
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:transfer:region:account-id: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:region:account-id: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": "account-id"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:region:account-id: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:region:account-
id:workflow/workflow-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 de política de registro e invocación 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": "account-id"
                },
                "ArnLike": {
                   "aws:SourceArn": [
                     "arn:aws:transfer:region:account-id:server/*",
                     "arn:aws:transfer:region:account-id:workflow/*"
                   ]
                }
            }
        }
    ]
}
```

El siguiente ejemplo de política de registro e invocación permite que un servidor (y un flujo de trabajo) específicos asuman la función.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSpecificServerWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
                "ArnEquals": {
                   "aws:SourceArn": [
                       "arn:aws:transfer:region:account-id:server/server-id",
                       "arn:aws:transfer:region:account-id:workflow/workflow-id"
                   ]
                }
            }
        }
    ]
}
```

AWS políticas gestionadas 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 acerca de 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 por 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 por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos 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.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `acm:ListCertificates`: otorga permiso para recuperar una lista de los Nombres de recurso de Amazon (ARN) certificados y el nombre de dominio para cada ARN.
- `ec2:DescribeAddresses`: concede permiso para describir una o varias direcciones IP elásticas.
- `ec2:DescribeAvailabilityZones`: concede permiso para describir una o varias de las zonas de disponibilidad que tiene a su disposición.
- `ec2:DescribeNetworkInterfaces`: concede permiso para describir una o varias interfaces de red elásticas.
- `ec2:DescribeSecurityGroups`: concede permiso para describir uno o varios grupos de seguridad.
- `ec2:DescribeSubnets`: concede permiso para describir una o varias subredes.
- `ec2:DescribeVpcs`: concede permiso para describir una o varias nubes privadas virtuales (VPC).
- `ec2:DescribeVpcEndpoints`: concede permiso para describir uno o varios puntos de conexión de VPC.
- `health:DescribeEventAggregates`: devuelve el número de eventos de cada tipo de evento (problema, cambio programado y notificación de cuenta).

- `iam:GetPolicyVersion`: concede permiso para recuperar información sobre una versión de la política administrada especificada, incluido el documento de política.
- `iam:ListPolicies`: concede permiso para obtener una lista de todas las políticas administradas.
- `iam:ListRoles`: concede permiso para obtener una lista de los roles de IAM con el prefijo de ruta especificado.
- `iam:PassRole`: concede permiso para transferir un rol de IAM a Transfer Family. Para obtener más información, consulte Otorgar permisos a un usuario para transferir un rol a un Servicio de AWS.
- `route53:ListHostedZones`: otorga permiso para obtener una lista de las zonas alojadas públicas y privadas asociadas a la actual Cuenta de AWS.
- `s3:ListAllMyBuckets`: concede permiso para enumerar todos los buckets propiedad del remitente autenticado de la solicitud.
- `transfer:*`: concede acceso a los recursos de Transfer Family. El asterisco (*) concede acceso a todos los recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "transfer.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "acm:ListCertificates",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeVpcs",
                "ec2:DescribeVpcEndpoints",
                "health:DescribeEventAggregates",
                "iam:GetPolicyVersion",
                "iam:ListPolicies",
                "iam:ListRoles",
                "route53:ListHostedZones",
                "s3:ListAllMyBuckets",
                "transfer:*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AWSTransferFullAccess

La política de `AWSTransferFullAccess` proporciona acceso completo a los servicios de Transfer Family.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `transfer:*`: concede permiso para acceder a los recursos de Transfer Family. El asterisco (*) concede acceso a todos los recursos.
- `iam:PassRole`: concede permiso para transferir un rol de IAM a Transfer Family. Para obtener más información, consulte Otorgar permisos a un usuario para transferir un rol a un Servicio de AWS.
- `ec2:DescribeAddresses`: concede permiso para describir una o varias direcciones IP elásticas.
- `ec2:DescribeNetworkInterfaces`: concede permiso para describir una o varias interfaces de red.
- `ec2:DescribeVpcEndpoints`: concede permiso para describir uno o varios puntos de conexión de VPC.

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

```
            "Effect": "Allow",
            "Action": "transfer:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "transfer.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

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.

Detalles de los permisos

Esta política incluye los siguientes permisos para Amazon CloudWatch Logs.

- `CreateLogStream`: concede permisos a las entidades principales para crear un flujo de registro.
- `DescribeLogStreams`: concede permisos a las entidades principales para que enumeren los flujos de registros del grupo de registros.
- `CreateLogGroup`: concede permisos a las entidades principales para crear grupos de registros.
- `PutLogEvents`: concede permisos a las entidades principales para cargar un lote de eventos de registro en un flujo de registros.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AWSTransferReadOnlyAccess

La política de `AWSTransferReadOnlyAccess` proporciona acceso de solo lectura a los servicios de Transfer Family.

Detalles de los permisos

Esta política incluye los siguientes permisos para Transfer Family.

- `DescribeUser`: concede permisos a las entidades principales para ver las descripciones de los usuarios.
- `DescribeServer`: concede permisos a las entidades principales para ver las descripciones de los servidores.
- `ListUsers`: concede permisos a las entidades principales para enumerar los usuarios de un servidor.
- `ListServers`: concede permisos a las entidades principales para enumerar los usuarios de una cuenta.
- `TestIdentityProvider`: concede permisos a las entidades principales para comprobar si el proveedor de identidades configurado está configurado correctamente.
- `ListTagsForResource`: concede permiso a las entidades principales para enumerar las etiquetas de un recurso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "transfer:DescribeUser",
                "transfer:DescribeServer",
                "transfer:ListUsers",
                "transfer:ListServers",
                "transfer:TestIdentityProvider",
                "transfer:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Transfiere las actualizaciones de Family a las políticas AWS gestionadas

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, suscríbase 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

Cambio	Descripción	Fecha
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

Solución de problemas AWS Transfer Family

Utilice la siguiente información para ayudarle a diagnosticar y solucionar problemas comunes que puedan surgir al trabajar con ellos AWS Transfer Family.

Si tiene problemas con IAM en Transfer Family, consulte Solución de problemas AWS Transfer Family de identidad y acceso.

Temas

- Solución de los problemas de los usuarios administrados por el servicio
- Solución de problemas de Amazon API Gateway
- Solución de problemas de políticas para buckets de Amazon S3 cifrados
- Solución de problemas de autenticación
- Solución de problemas de flujos de trabajo administrados
- Solución de los problemas de descifrado del flujo de trabajo
- Solución de problemas de Amazon EFS
- Solución de los problemas al probar su proveedor de identidad
- Solución de los problemas al agregar claves de host confiables para su conector SFTP
- Solución de los problemas de carga de archivos
- Solución de los problemas con la excepción ResourceNotFound
- Solución de los problemas con el conector SFTP
- Solución de los problemas de AS2

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 los problemas de los usuarios administrados por el servicio de Amazon EFS
- Solución de problemas con cuerpo de la clave pública demasiado largo
- Solución de problemas no pudo agregar la clave pública SSH

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 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 está basada en RSA, puede convertirla al formato PEM. Por ejemplo, Ubuntu proporciona una herramienta de conversión aquí: https://manpages.ubuntu.com/manpages/xenial/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 esté intentando importar una clave pública con formato SSH2 y que AWS Transfer Family no admita claves públicas con formato SSH2 para los usuarios gestionados por el servicio.

Solución

Debe convertir la clave al formato OpenSSH. Este proceso se describe en Convierta una clave pública SSH2 a formato PEM.

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. Abre la AWS 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. UserRoleArnSustitúyalo 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 página Revisar ***pila***, 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 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 detalles, consulte Cifrado de datos en Amazon S3.

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
- Varios problemas de autenticación

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).

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, `/DOC-EXAMPLE-BUCKET/images` es aceptable, pero `DOC-EXAMPLE-BUCKET/images` no `/DOC-EXAMPLE-BUCKET/images/` lo es.

Solución de problemas de flujos de trabajo administrados

En esta sección se describen las posibles soluciones para los siguientes problemas de 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 ExecutionErroredmensaje. Para obtener más información, consulte Procesamiento de datos de registro en tiempo real 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

- Solucionar el error del archivo de cifrado firmado
- Solucione el error de un algoritmo FIPS

Solucionar 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 Amazon EFS

En esta sección se describen las posibles soluciones para los siguientes problemas de Amazon EFS.

Temas

- Solución de los problemas del perfil POSIX faltante

- Solución de los problemas de directorios lógicos con Amazon EFS

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.

Solución de los problemas al probar su proveedor de identidad

Descripción

Si prueba su proveedor de identidad mediante la consola o la llamada a 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.

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...==
```

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 caracteres UTF-8. Como resultado, algunos caracteres no se representan correctamente.

Solución

Para solucionar este problema, revise la aplicación cliente para comprobar la codificación de caracteres de los nombres de archivo y asegúrese de que está configurada en UTF-8.

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 ResourceNotFoundExceptionmensaje. 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
```

Solución de los problemas con el conector SFTP

En esta sección se describen las posibles soluciones para los siguientes problemas con el conector SFTP.

Temas

- La negociación de claves falla

- Problemas varios con el conector SFTP

La negociación de claves 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 AWS Transfer Family de seguridad para conectores SFTP.

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: consultePrueba 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 Ejemplo 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.

Solución de los problemas de AS2

Los mensajes de error y las sugerencias de solución de problemas para los servidores compatibles con la Declaración de Aplicabilidad 2 (AS2) se describen aquí: Códigos de error de AS2.

Referencia de la API

En las siguientes secciones se documentan las llamadas al servicio de la AWS Transfer Family API, los tipos de datos, los parámetros y los errores.

Temas

- Bienvenido a la AWS Transfer Family API
- Acciones
- Data Types
- Realizar solicitudes a la API
- Parámetros comunes
- Errores comunes

Bienvenido a la AWS Transfer Family API

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

Para utilizar el AWS Transfer Family servicio, debe crear una instancia de un servidor en la AWS región que elija. Puede crear el servidor, ver una lista de los servidores disponibles, y actualizar servidores o eliminarlos. El servidor es la entidad desde la que se solicitan las operaciones con los archivos. AWS Transfer Family Los servidores tienen algunas propiedades muy importantes. El servidor es una instancia con nombre reconocible por un identificador `ServerId` asignado por el

sistema. Si lo desea, puede asignar un nombre de host o incluso un nombre personalizado a un servidor. El servicio se factura por los servidores instanciados (incluso aquellos `OFFLINE`) y por el volumen de los datos transferidos.

Los usuarios deben ser conocidos por el servidor que solicita operaciones con archivos. Los usuarios, identificados por su nombre de usuario, se asignan a un servidor. Los nombres de usuario se utilizan para autenticar las solicitudes. Un mismo servidor solo puede tener un método de autenticación: `AWS_DIRECTORY_SERVICE`, `SERVICE_MANAGED`, `AWS_LAMBDA` o `API_GATEWAY`.

Puede usar cualquiera de los siguientes tipos de proveedores de identidad para autenticar a los usuarios:

- Con `SERVICE_MANAGED` se almacena una clave SSH pública con las propiedades del usuario en un servidor. Cada usuario puede tener una o más claves SSH públicas en el archivo para el método de autenticación `SERVICE_MANAGED`. Cuando un cliente solicita una operación con archivos mediante el método `SERVICE_MANAGED`, debe proporcionar el nombre de usuario y la clave SSH privada, que entonces se autentica para conceder el acceso.
- Puede administrar la autenticación y el acceso de los usuarios con sus grupos de Microsoft Active Directory seleccionando el método de autenticación `AWS_DIRECTORY_SERVICE`.
- Puede conectarse a un proveedor de identidad personalizado mediante AWS Lambda. Elija el método de autenticación `AWS_LAMBDA`.
- Las solicitudes de los usuarios también pueden procesarse mediante un método de autenticación personalizado que ofrezca al mismo tiempo la autenticación del usuario y el 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. El método se denomina `API_GATEWAY` en las llamadas a la API y Custom en la consola. Puede utilizar este método personalizado para autenticar usuarios en un servicio de directorio, en una base de datos de nombres y contraseñas o en algún otro mecanismo.

A los usuarios se les asigna una política con una relación de confianza entre ellos y un bucket de Amazon S3. El acceso puede ser a todo un bucket o a parte de él. Para que un servidor actúe en nombre de un usuario, el servidor debe heredar del usuario su relación de confianza. Para ello se crea un rol de AWS Identity and Access Management (IAM) que contiene la relación de confianza y que se le asigna una acción `AssumeRole`. Así el servidor puede llevar a cabo operaciones con archivos como si fuera el usuario.

Los usuarios que tengan establecida una propiedad de directorio home podrán hacer que ese directorio (o carpeta) actúe como destino u origen de las operaciones con archivos. Si no hay establecido un directorio home, la ubicación inicial es el directorio `root` del bucket.

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 ID 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.transfer.`*`region`*`.amazonaws.com`.

Para obtener una lista de los puntos de enlace de Transfer Family por AWS región, consulte los AWS Transfer Family puntos de enlace y las cuotas en. Referencia general de AWS

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 Data 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.

Acciones

Se admiten las siguientes acciones:

- CreateAccess
- CreateAgreement
- CreateConnector
- CreateProfile
- CreateServer
- CreateUser
- CreateWorkflow
- DeleteAccess
- DeleteAgreement
- DeleteCertificate

- DeleteConnector
- DeleteHostKey
- DeleteProfile
- DeleteServer
- DeleteSshPublicKey
- DeleteUser
- DeleteWorkflow
- DescribeAccess
- DescribeAgreement
- DescribeCertificate
- DescribeConnector
- DescribeExecution
- DescribeHostKey
- DescribeProfile
- DescribeSecurityPolicy
- DescribeServer
- DescribeUser
- DescribeWorkflow
- ImportCertificate
- ImportHostKey
- ImportSshPublicKey
- ListAccesses
- ListAgreements
- ListCertificates
- ListConnectors
- ListExecutions
- ListHostKeys
- ListProfiles
- ListSecurityPolicies
- ListServers

- ListTagsForResource
- ListUsers
- ListWorkflows
- SendWorkflowStepState
- StartDirectoryListing
- StartFileTransfer
- StartServer
- StopServer
- TagResource
- TestConnection
- TestIdentityProvider
- UntagResource
- UpdateAccess
- UpdateAgreement
- UpdateCertificate
- UpdateConnector
- UpdateHostKey
- UpdateProfile
- UpdateServer
- UpdateUser

CreateAccess

Utilizado por los administradores para elegir qué grupos del directorio deben tener acceso para cargar y descargar archivos a través de los protocolos habilitados que utilizan AWS Transfer Family. Por ejemplo, un Active Directory de Microsoft puede contener 50 000 usuarios, pero es posible que solo una pequeña fracción necesite la capacidad de transferir archivos al servidor. Un administrador puede utilizar `CreateAccess` para limitar el acceso al conjunto correcto de usuarios que necesiten esta capacidad.

Sintaxis de la solicitud

```
{
   "ExternalId": "string",
   "HomeDirectory": "string",
   "HomeDirectoryMappings": [
      {
         "Entry": "string",
         "Target": "string",
         "Type": "string"
      }
   ],
   "HomeDirectoryType": "string",
   "Policy": "string",
   "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "Role": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ExternalId

Un identificador único que se requiere para identificar grupos específicos dentro de su directorio. Los usuarios del grupo que asocie tienen acceso a sus recursos de Amazon S3 o Amazon EFS a través de los protocolos habilitados que utilizan AWS Transfer Family. Si conoce el nombre del grupo, puede ver los valores del SID ejecutando el siguiente comando en Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

En ese comando, YourGroupNamesustitúyalo por el nombre del grupo de Active Directory.

La expresión regular utilizada para validar este parámetro es una cadena de caracteres compuesta de caracteres alfanuméricos en mayúscula y minúscula, sin espacios. También puede incluir guiones bajos y cualquiera de los siguientes caracteres: =,.@:/-

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `S-1-[\d-]+`

Obligatorio: sí

HomeDirectory

Directorio de destino (carpeta) de un usuario cuando inicia sesión en el servidor a través del cliente.

Un ejemplo de `HomeDirectory` es `/bucket_name/home/mydirectory`.

> **Note**
>
> El parámetro `HomeDirectory` solo se utiliza si `HomeDirectoryType` está establecido en `PATH`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

HomeDirectoryMappings

Los mapeos de directorio lógico que especifican qué rutas de acceso y claves de Amazon S3 o Amazon EFS 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. Si solo especifica un destino, se muestra tal cual. También debe asegurarse de que su función AWS Identity and Access Management (de IAM) proporcione acceso a las rutas de entrada. `Target` Este valor solo se puede establecer si `HomeDirectoryType` está establecido en LOGICAL.

Lo siguiente es un ejemplo del par `Entry` y `Target`.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

En la mayoría de los casos, puede utilizar este valor en lugar de la política de sesión para limitar al usuario al directorio de inicio designado (“`chroot`”). Para ello, puede establecer `Entry` en `/`, y `Target` al valor del parámetro `HomeDirectory`.

A continuación, se muestra un ejemplo del par `Entry` y `Target` para `chroot`.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Tipo: Matriz de HomeDirectoryMapEntry objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50000 artículos.

Obligatorio: no

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 la ruta absoluta 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 `HomeDirectoryMappings` que correspondan con la forma en que quiere que las rutas de acceso de Amazon S3 o de Amazon EFS sean visibles para sus usuarios.

> **Note**
>
> Si `HomeDirectoryType` es `LOGICAL`, debe proporcionar las asignaciones mediante el parámetro `HomeDirectoryMappings`. Si, por el contrario, `HomeDirectoryType` es `PATH`, se proporciona una ruta absoluta mediante el parámetro `HomeDirectory`. No puede tener `HomeDirectory` y `HomeDirectoryMappings` en su plantilla.

Tipo: cadena

Valores válidos: `PATH | LOGICAL`

Obligatorio: no

Policy

Una política de sesión para su usuario, de modo que pueda usar el mismo rol AWS Identity and Access Management (IAM) en varios usuarios. Esta política reduce el ámbito de acceso de un usuario a partes de su bucket de Amazon S3. Entre las variables que puede utilizar dentro de esta política se incluyen `${Transfer:UserName}`, `${Transfer:HomeDirectory}` y `${Transfer:HomeBucket}`.

> **Note**
>
> Esta política se aplica solo cuando el dominio de `ServerId` es Amazon S3. Amazon EFS no utiliza políticas de sesión.
>
> En el caso de las políticas de sesión, AWS Transfer Family almacena la política como un blob de JSON, en lugar del nombre de recurso de Amazon (ARN) de la política. Puede guardar la política como un blob JSON y pasarlo en el argumento `Policy`.
>
> Para ver un ejemplo de una política de sesión, consulte Example session policy (Ejemplo de política de sesión).
>
> Para obtener más información, consulte la referencia AssumeRolede la AWS Security Token Service API.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: no

PosixProfile

La identidad POSIX completa, incluido el ID de usuario (`Uid`), el ID de grupo (`Gid`) y cualquier ID de grupo secundario (`SecondaryGids`) 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.

Tipo: objeto PosixProfile

Obligatorio: no

Role

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que controla el acceso de los usuarios al bucket de Amazon S3 o al sistema de archivos Amazon 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.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: sí

ServerId

Identificador único asignado por el sistema para una instancia del servidor. Este es el servidor específico al que ha agregado el usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ExternalId

El identificador externo del grupo cuyos usuarios tienen acceso a sus recursos de Amazon S3 o Amazon EFS a través de los protocolos habilitados que utilizan AWS Transfer Family.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `S-1-[\d-]+`

ServerId

El ID del servidor al que se asocia el usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateAgreement

Crea un acuerdo. Un acuerdo es un acuerdo bilateral de socios comerciales, o asociación, entre un AWS Transfer Family servidor y un proceso AS2. El acuerdo define la relación de transferencia de archivos y mensajes entre el servidor y el proceso AS2. Para definir un acuerdo, Transfer Family combina un servidor, un perfil local, un perfil de socio, un certificado y otros atributos.

El socio se identifica con el `PartnerProfileId` y el proceso AS2 se identifica con el `LocalProfileId`.

Sintaxis de la solicitud

```
{
   "AccessRole": "string",
   "BaseDirectory": "string",
   "Description": "string",
   "LocalProfileId": "string",
   "PartnerProfileId": "string",
   "ServerId": "string",
   "Status": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

AccessRole

Los conectores se utilizan para enviar archivos mediante el protocolo AS2 o SFTP. Para la función de acceso, proporcione el nombre de recurso de Amazon (ARN) de la AWS Identity and Access Management función que se va a utilizar.

Para conectores AS2

Con AS2, puede enviar archivos llamando a `StartFileTransfer` y especificando las rutas de los archivos en el parámetro de solicitud, `SendFilePaths`. Utilizamos el directorio principal del archivo (por ejemplo, para `--send-file-paths /bucket/dir/file.txt`, el directorio principal es `/bucket/dir/`) para almacenar temporalmente un archivo de mensajes AS2 procesado, almacenar el MDN cuando lo recibimos del socio y escribir un archivo JSON final que contenga los metadatos relevantes de la transmisión. Por lo tanto, `AccessRole` debe proporcionar acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`. Además, debe proporcionar acceso de lectura y escritura al directorio principal de los archivos que desea enviar con `StartFileTransfer`.

Si utiliza la autenticación básica para el conector AS2, el rol de acceso requiere el permiso `secretsmanager:GetSecretValue` para el secreto. Si el secreto se cifra con una clave gestionada por el cliente en lugar de la clave AWS gestionada en Secrets Manager, el rol también necesitará el `kms:Decrypt` permiso para esa clave.

Para conectores SFTP

Asegúrese de que el acceso al 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 otorgue `secretsmanager:GetSecretValue` permiso a. AWS Secrets Manager

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: sí

BaseDirectory

El directorio de destino (carpeta) de los archivos que se transfieren a través del protocolo AS2.

Un ejemplo de `BaseDirectory` es `/DOC-EXAMPLE-BUCKET/home/mydirectory`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: sí

Description

El nombre o la descripción breve que se utilizan para identificar el acuerdo.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Graph}]+`

Obligatorio: no

LocalProfileId

Un identificador único para el perfil local de AS2.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: sí

PartnerProfileId

Un identificador único para el perfil de socio utilizado en el acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: sí

ServerId

Identificador único asignado por el sistema para una instancia del servidor. Este identificador indica el servidor específico que utiliza el acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Status

El estado del acuerdo. El acuerdo puede ser `ACTIVE` o `INACTIVE`.

Tipo: cadena

Valores válidos: `ACTIVE | INACTIVE`

Obligatorio: no

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar acuerdos.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "AgreementId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AgreementId

El identificador único para el acuerdo. Use este ID para eliminar o actualizar un acuerdo, así como en cualquier otra llamada a la API que requiera que especifique el ID del acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `a-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo, se crea un acuerdo y se devuelve el identificador del acuerdo.

```
aws transfer create-agreement --server-id s-021345abcdef6789 --local-profile-
id p-1234567890abcdef0 --partner-profile-id p-abcdef01234567890 --base-folder /DOC-
EXAMPLE-BUCKET/AS2-files --access-role arn:aws:iam::111122223333:role/AS2-role
```

Respuesta de ejemplo

La llamada a la API devuelve el identificador del nuevo acuerdo.

```
{
    "AgreementId": "a-11112222333344444"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateConnector

Crea el conector, que captura los parámetros de una conexión de salida para el protocolo AS2 o SFTP. Para AS2, el conector es necesario para enviar archivos a un servidor AS2 alojado externamente. En el caso del SFTP, el conector es necesario para enviar archivos a un servidor SFTP o recibir archivos desde un servidor SFTP. Para obtener más información sobre los conectores, consulte Configurar conectores AS2 y Crear conectores SFTP.

> **Note**
>
> Debe especificar exactamente un objeto de configuración, ya sea para AS2 (`As2Config`) o para SFTP (`SftpConfig`).

Sintaxis de la solicitud

```
{
   "AccessRole": "string",
   "As2Config": {
      "BasicAuthSecretId": "string",
      "Compression": "string",
      "EncryptionAlgorithm": "string",
      "LocalProfileId": "string",
      "MdnResponse": "string",
      "MdnSigningAlgorithm": "string",
      "MessageSubject": "string",
      "PartnerProfileId": "string",
      "SigningAlgorithm": "string"
   },
   "LoggingRole": "string",
   "SecurityPolicyName": "string",
   "SftpConfig": {
      "TrustedHostKeys": [ "string" ],
      "UserSecretId": "string"
   },
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
```

```
    "Url": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

AccessRole

Los conectores se utilizan para enviar archivos mediante el protocolo AS2 o SFTP. Para la función de acceso, proporcione el nombre de recurso de Amazon (ARN) de la AWS Identity and Access Management función que se va a utilizar.

Para conectores AS2

Con AS2, puede enviar archivos llamando a `StartFileTransfer` y especificando las rutas de los archivos en el parámetro de solicitud, `SendFilePaths`. Utilizamos el directorio principal del archivo (por ejemplo, para `--send-file-paths /bucket/dir/file.txt`, el directorio principal es `/bucket/dir/`) para almacenar temporalmente un archivo de mensajes AS2 procesado, almacenar el MDN cuando lo recibimos del socio y escribir un archivo JSON final que contenga los metadatos relevantes de la transmisión. Por lo tanto, `AccessRole` debe proporcionar acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`. Además, debe proporcionar acceso de lectura y escritura al directorio principal de los archivos que desea enviar con `StartFileTransfer`.

Si utiliza la autenticación básica para el conector AS2, el rol de acceso requiere el permiso `secretsmanager:GetSecretValue` para el secreto. Si el secreto se cifra con una clave gestionada por el cliente en lugar de la clave AWS gestionada en Secrets Manager, el rol también necesitará el `kms:Decrypt` permiso para esa clave.

Para conectores SFTP

Asegúrese de que el acceso al 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 otorgue `secretsmanager:GetSecretValue` permiso a. AWS Secrets Manager

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: sí

As2Config

Una estructura que contiene los parámetros de un objeto de conexión AS2.

Tipo: objeto As2ConnectorConfig

Obligatorio: no

LoggingRole

El nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que permite a un conector activar el CloudWatch registro de los eventos de Amazon S3. Cuando esté configurado, podrá ver la actividad del conector en sus CloudWatch registros.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

SecurityPolicyName

Especifica el nombre de la política de seguridad del conector.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 100 caracteres.

Patrón: `TransferSFTPConnectorSecurityPolicy-[A-Za-z0-9-]+`

Obligatorio: no

SftpConfig

Una estructura que contiene los parámetros de un objeto de conexión SFTP.

Tipo: objeto SftpConnectorConfig

Obligatorio: no

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar conectores. Las etiquetas son metadatos asociados a conectores para cualquier fin.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Url

La URL del punto de conexión de AS2 o SFTP del socio.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 255 caracteres.

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ConnectorId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ConnectorId

El identificador único del conector, que se devuelve una vez que la llamada a la API se realiza correctamente.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo se crea un conector AS2. En el comando, sustituya los siguientes elementos:

- `url`: proporcione la URL del servidor AS2 del socio comercial.
- `your-IAM-role-for-bucket-access`: un rol de IAM que tiene acceso al bucket de Amazon S3 que está utilizando para almacenar sus archivos.
- Usa el ARN para tu función de registro, que incluye tu Cuenta de AWS ID.
- Proporcione una ruta a un archivo que contenga los parámetros de configuración del conector AS2. El objeto de configuración del conector AS2 se describe en As2. ConnectorConfig

```
// Listing for testAs2Config.json
{
  "LocalProfileId": "your-profile-id",
  "PartnerProfileId": "partner-profile-id",
  "MdnResponse": "SYNC",
  "Compression": "ZLIB",
  "EncryptionAlgorithm": "AES256_CBC",
  "SigningAlgorithm": "SHA256",
  "MdnSigningAlgorithm": "DEFAULT",
  "MessageSubject": "Your Message Subject"
}
```

```
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
```

Ejemplo

En el siguiente ejemplo, se crea un conector SFTP. En el comando, sustituya los siguientes elementos:

- `sftp-server-url`: proporcione la URL del servidor SFTP con el que está intercambiando archivos.
- `your-IAM-role-for-bucket-access`: un rol de IAM que tiene acceso al bucket de Amazon S3 que está utilizando para almacenar sus archivos.
- Usa el ARN para tu función de registro, que incluye tu Cuenta de AWS ID.

- Proporcione una ruta a un archivo que contenga los parámetros de configuración del conector SFTP. El objeto de configuración del conector SFTP se describe en SftpConnectorConfig.

```
// 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="
   ]
}
```

```
aws transfer create-connector --url "sftp://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
```

Ejemplo

La llamada a la API devuelve el ID del conector nuevo.

Respuesta de ejemplo

```
{
    "ConnectorId": "a-11112222333344444"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2

- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateProfile

Crea el perfil local o de socio que se utilizará para las transferencias de AS2.

Sintaxis de la solicitud

```
{
   "As2Id": "string",
   "CertificateIds": [ "string" ],
   "ProfileType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

As2Id

El `As2Id` es el nombre AS2, tal como se define en RFC 4130. Para las transferencias entrantes, este es el encabezado `AS2-From` de los mensajes AS2 enviados por el socio. Para los conectores de salida, este es el encabezado `AS2-To` de los mensajes AS2 enviados al socio mediante la operación `StartFileTransfer` de la API. Este ID no puede incluir espacios.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `[\p{Print}\s]*`

Obligatorio: sí

CertificateIds

Una matriz de identificadores de los certificados importados. Este identificador se utiliza para trabajar con perfiles y perfiles de socios.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Obligatorio: no

ProfileType

Determina el tipo de perfil que se va a crear:

- Especifique `LOCAL` para crear un perfil local. Un perfil local representa la organización o entidad del servidor de Transfer Family habilitado para AS2.
- Especifique `PARTNER` para crear un perfil de socio. Un perfil de socio representa una organización remota, externa a Transfer Family.

Tipo: cadena

Valores válidos: `LOCAL | PARTNER`

Obligatorio: sí

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar perfiles AS2.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "ProfileId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ProfileId

El identificador único del perfil de AS2, que se devuelve después de que la llamada a la API se realiza correctamente.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo, se crea un perfil y se devuelve el identificador del perfil.

Los identificadores del certificado se crean cuando ejecuta `import-certificate`, uno para el certificado de firma y otro para el certificado de cifrado.

```
aws transfer create-profile --as2-id MYCORP --certificate-ids c-abcdefg123456hijk
              c-987654aaaa321bbbb
```

Respuesta de ejemplo

La llamada a la API devuelve el ID del perfil para el perfil nuevo.

```
{
    "ProfileId": "p-11112222333344444"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateServer

Crea una instancia de servidor virtual de escalado automático en función del protocolo de transferencia de archivos seleccionado en AWS. Cuando actualice su servidor habilitado por protocoles de transferencia de archivos o cuando trabaje con usuarios, use la propiedad `ServerId` generada por el servicio, la cual se asigna al servidor creado recientemente.

Sintaxis de la solicitud

```
{
   "Certificate": "string",
   "Domain": "string",
   "EndpointDetails": {
      "AddressAllocationIds": [ "string" ],
      "SecurityGroupIds": [ "string" ],
      "SubnetIds": [ "string" ],
      "VpcEndpointId": "string",
      "VpcId": "string"
   },
   "EndpointType": "string",
   "HostKey": "string",
   "IdentityProviderDetails": {
      "DirectoryId": "string",
      "Function": "string",
      "InvocationRole": "string",
      "SftpAuthenticationMethods": "string",
      "Url": "string"
   },
   "IdentityProviderType": "string",
   "LoggingRole": "string",
   "PostAuthenticationLoginBanner": "string",
   "PreAuthenticationLoginBanner": "string",
   "ProtocolDetails": {
      "As2Transports": [ "string" ],
      "PassiveIp": "string",
      "SetStatOption": "string",
      "TlsSessionResumptionMode": "string"
   },
   "Protocols": [ "string" ],
   "S3StorageOptions": {
      "DirectoryListingOptimization": "string"
   },
   "SecurityPolicyName": "string",
```

```
   "StructuredLogDestinations": [ "string" ],
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "WorkflowDetails": {
      "OnPartialUpload": [
         {
            "ExecutionRole": "string",
            "WorkflowId": "string"
         }
      ],
      "OnUpload": [
         {
            "ExecutionRole": "string",
            "WorkflowId": "string"
         }
      ]
   }
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Certificate

El nombre de recurso de Amazon (ARN) del certificado AWS Certificate Manager (ACM). Necesario cuando `Protocols` se establece en `FTPS`.

Para solicitar un certificado público nuevo, consulte Solicitar un certificado público en la Guía del AWS Certificate Manager usuario.

Para importar un certificado existente a ACM, consulte Importación de certificados a ACM en la Guía del AWS Certificate Manager usuario.

Para solicitar un certificado privado para usar FTPS a través de direcciones IP privadas, consulte Solicitar un certificado privado en la Guía del AWS Certificate Manager usuario.

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 SSL/TLS X.509 versión 3 válido con FQDN o dirección IP especificada e información sobre el emisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1600 caracteres.

Obligatorio: no

Domain

El dominio del sistema de almacenamiento que se utiliza para las transferencias de archivos. Hay dos dominios disponibles: Amazon Simple Storage Service (Amazon S3) y Amazon Elastic File System (Amazon EFS). El valor predeterminado es S3.

> **Note**
>
> Después de crear el servidor, el dominio no se puede cambiar.

Tipo: cadena

Valores válidos: `S3 | EFS`

Obligatorio: no

EndpointDetails

Los ajustes del punto de conexión de la nube privada virtual (VPC) que está configurado para su servidor. Cuando aloja el punto de conexión dentro de la VPC, puede hacer que sea accesible solo para los recursos de la VPC, o puede adjuntar direcciones IP elásticas y hacer que sea

accesible para los clientes a través de Internet. Los grupos de seguridad predeterminados de su VPC se asignan automáticamente a su punto de conexión.

Tipo: objeto EndpointDetails

Obligatorio: no

EndpointType

El tipo de punto de conexión que desea que use el servidor. Puede optar por hacer que el punto de conexión de su servidor sea de acceso público (PUBLIC) o alojarlo dentro de su VPC. Con un punto de conexión alojado en una VPC, puede restringir el acceso al servidor y a los recursos solo dentro de su VPC o elegir que esté orientado a Internet al adjuntarle direcciones IP elásticas directamente.

> **Note**
>
> Después del 19 de mayo de 2021, no podrás crear un servidor con `EndpointType=VPC_ENDPOINT` tu cuenta Cuenta de AWS si no lo ha hecho antes del 19 de mayo de 2021. Si ya has creado servidores `EndpointType=VPC_ENDPOINT` en tu cuenta Cuenta de AWS el 19 de mayo de 2021 o antes, no te afectará. Después de esta fecha, use `EndpointType=VPC`.
> Para obtener más información, consulte Suspender el uso de VPC_ENDPOINT.
> Se recomienda que utilice `VPC` como `EndpointType`. Con este tipo de punto de conexión, tiene la opción de asociar directamente hasta tres direcciones IPv4 Elastic (IP BYO incluida) con el punto de conexión del servidor y utilizar grupos de seguridad de VPC para restringir el tráfico de la dirección IP pública del cliente. Esto no es posible si se establece `EndpointType` en `VPC_ENDPOINT`.

Tipo: cadena

Valores válidos: `PUBLIC | VPC | VPC_ENDPOINT`

Obligatorio: no

HostKey

La clave privada RSA, ECDSA o ED25519 que se utilizará en el servidor habilitado para SFTP. Puede agregar varias claves de host, en caso de que desee rotar las claves, o tener un conjunto de claves activas que utilicen algoritmos diferentes.

Use el siguiente comando para generar una clave RSA de 2048 bits sin contraseña:

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

Utilice un valor mínimo de 2048 para la opción `-b`. Puede crear una clave más fuerte utilizando 3072 o 4096.

Utilice el siguiente comando para generar una clave ECDSA de 256 bits sin contraseña:

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

Los valores válidos para la opción `-b` de ECDSA son 256, 384 y 521.

Utilice el siguiente comando para generar una clave ED25519 sin contraseña:

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

Puedes reemplazar todos estos comandos por my-new-server-keyla cadena que prefieras.

> **Important**
>
> Si no planea migrar los usuarios existentes de un servidor compatible con SFTP a un servidor nuevo, no actualice la clave de host. El cambio accidental de la clave de host de un servidor puede ser disruptivo.

Para obtener más información, consulte Actualizar las claves de host de un servidor con SFTP en la AWS Transfer Family Guía del usuario.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 4096 caracteres.

Obligatorio: no

IdentityProviderDetails

Obligatorio cuando `IdentityProviderType` se establece en `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`. Acepta una matriz que contiene toda la información necesaria para usar un directorio en `AWS_DIRECTORY_SERVICE` o invocar a una API de autenticación proporcionada por el cliente, incluida la URL de API Gateway. No es necesario cuando `IdentityProviderType` se establece en `SERVICE_MANAGED`.

Tipo: objeto IdentityProviderDetails

Obligatorio: no

IdentityProviderType

El modo de autenticación de un servidor. El valor predeterminado es`SERVICE_MANAGED`, que le permite almacenar las credenciales de usuario y acceder a ellas dentro del servicio. AWS Transfer Family

Úselo `AWS_DIRECTORY_SERVICE` para proporcionar acceso a los grupos de Active Directory AWS Directory Service for Microsoft Active Directory o a Microsoft Active Directory en su entorno local o AWS mediante AD Connector. Esta opción también requiere que se especifique el ID del directorio mediante el parámetro `IdentityProviderDetails`.

Utilice el valor `API_GATEWAY` para la integración con un proveedor de identidades de su elección. La configuración de `API_GATEWAY` requiere que proporcione un punto de conexión de Amazon API Gateway para solicitar la autenticación mediante el parámetro `IdentityProviderDetails`.

Usa el `AWS_LAMBDA` valor para usar directamente una AWS Lambda función como proveedor de identidades. Si elige este valor, debe especificar el ARN de la función de Lambda en el parámetro `Function` para el tipo de datos de `IdentityProviderDetails`.

Tipo: cadena

Valores válidos: `SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA`

Obligatorio: no

LoggingRole

El nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que permite a un servidor activar el CloudWatch registro de Amazon para Amazon S3 o Amazon EFSEvents. Cuando esté configurado, podrá ver la actividad de los usuarios en sus registros. CloudWatch

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Patrón: `(|arn:.*role/\S+)`

Obligatorio: no

PostAuthenticationLoginBanner

Especifica una cadena para que se muestre cuando los usuarios se conecten a un servidor. Esta cadena se muestra después de que el usuario se autentique.

> **Note**
>
> El protocolo SFTP no admite banners de visualización posteriores a la autenticación.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 4 096 caracteres.

Patrón: `[\x09-\x0D\x20-\x7E]*`

Obligatorio: no

PreAuthenticationLoginBanner

Especifica una cadena para que se muestre cuando los usuarios se conecten a un servidor. Esta cadena se muestra antes de que el usuario se autentique. Por ejemplo, el siguiente banner muestra detalles sobre el uso del sistema:

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 4 096 caracteres.

Patrón: `[\x09-\x0D\x20-\x7E]*`

Obligatorio: no

ProtocolDetails

La configuración de protocolo configurados para su servidor.

- Use el parámetro `PassiveIp` para indicar el modo pasivo (para los protocolos FTP y FTPS). Ingrese una sola dirección IPv4 de cuatro puntos, como la dirección IP externa de un firewall, un enrutador o un equilibrador de carga.
- Utilice el parámetro `SetStatOption` para ignorar el error que se genera cuando el cliente intenta usar el comando `SETSTAT` en un archivo que esté cargando en un bucket de Amazon S3. Para que el AWS Transfer Family servidor ignore el `SETSTAT` comando y cargue archivos sin necesidad de realizar ningún cambio en el cliente SFTP, defina `ENABLE_NO_OP` el valor en. Si estableces el `SetStatOption` parámetro en`ENABLE_NO_OP`, Transfer Family generará una entrada de registro en Amazon CloudWatch Logs para que puedas determinar cuándo el cliente está realizando una `SETSTAT` llamada.
- Para determinar si su AWS Transfer Family servidor reanuda las sesiones negociadas recientes mediante un identificador de sesión único, utilice el `TlsSessionResumptionMode` parámetro.
- `As2Transports` indica el método de transporte de los mensajes de AS2. Actualmente, solo se admite HTTP.

Tipo: objeto ProtocolDetails

Obligatorio: no

Protocols

Especifica el protocolo o los protocolos de File Transfer a través de los cuales el cliente de protocolo de File Transfer puede conectarse al punto de enlace del servidor. Los protocolos disponibles son:

- `SFTP` (Protocolo de File Transfer Secure Shell (SSH)): transferencia de archivos a través de SSH
- `FTPS` (Protocolo de File Transfer seguro): transferencia de archivos con cifrado TLS
- `FTP` (Protocolo de File Transfer): transferencia de archivos sin cifrar
- `AS2`(Declaración de aplicabilidad 2): se utiliza para transportar datos estructurados business-to-business

> **Note**
>
> - Si lo seleccionaFTPS, debe elegir un certificado almacenado en AWS Certificate Manager (ACM) que se utilice para identificar el servidor cuando los clientes se conecten a él a través de FTPS.

- Si el `Protocol` incluye `FTP` o `FTPS`, el `EndpointType` debe ser `VPC` y el `IdentityProviderType` debe ser `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
- Si `Protocol` incluye `FTP`, entonces `AddressAllocationIds` no se puede asociar.
- Si el `Protocol` se establece solo en `SFTP`, se puede establecer el `EndpointType` como `PUBLIC` y el `IdentityProviderType` se puede configurar como cualquiera de los tipos de identidad admitidos: `SERVICE_MANAGED`, `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
- Si `Protocol` incluye `AS2`, `EndpointType` debe ser `VPC` y el dominio debe ser Amazon S3.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Valores válidos: `SFTP | FTP | FTPS | AS2`

Obligatorio: no

S3StorageOptions

Especifica si el rendimiento de los directorios de Amazon S3 está optimizado o no. Esta opción está deshabilitada de forma predeterminada.

De forma predeterminada, las asignaciones de los directorios principales tienen un `TYPE` valor de. `DIRECTORY` Si habilita esta opción, tendrá que establecerla de forma explícita `FILE` si `HomeDirectoryMapEntry` `Type` desea que la asignación tenga un destino de archivo.

Tipo: objeto S3StorageOptions

Obligatorio: no

SecurityPolicyName

Especifica el nombre de la política de seguridad del servidor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 100 caracteres.

Patrón: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Obligatorio: no

StructuredLogDestinations

Especifica los grupos de registro a los que se envían los registros de su servidor.

Para especificar un grupo de registros, debe proporcionar el ARN de un grupo de registros existente. En este caso, el formato del grupo de registros es el siguiente:

`arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*`

Por ejemplo, `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

Si ha especificado previamente un grupo de registros para un servidor, puede borrarlo y desactivar el registro estructurado proporcionando un valor vacío para este parámetro en una llamada `update-server`. Por ejemplo:

```
update-server --server-id s-1234567890abcdef0 --structured-log-
destinations
```

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: no

Tags

Pares clave-valor que se puede utilizar para agrupar y buscar servidores.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

WorkflowDetails

Especifica el ID del flujo de trabajo que se va a asignar y el rol de ejecución que se utiliza para ejecutar el flujo de trabajo.

Además de un flujo de trabajo que se ejecuta cuando un archivo se carga por completo, `WorkflowDetails` también puede contener un ID de flujo de trabajo (y un rol de ejecución) para que un flujo de trabajo se ejecute en una carga parcial. Se produce una carga parcial si la sesión de servidor se desconecta mientras se está cargando el archivo.

Tipo: objeto WorkflowDetails

Obligatorio: no

Sintaxis de la respuesta

```
{
   "ServerId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ServerId

El identificador asignado al servicio del servidor que se crea.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo se crea un nuevo usuario usando un `VPC_ENDPOINT`.

Solicitud de muestra

```
{
   "EndpointType": "VPC",
```

```
   "EndpointDetails":...,
   "HostKey": "Your RSA private key",
   "IdentityProviderDetails": "IdentityProvider",
   "IdentityProviderType": "SERVICE_MANAGED",
   "LoggingRole": "CloudWatchLoggingRole",
   "Tags": [
      {
         "Key": "Name",
         "Value": "MyServer"
      }
   ]
}
```

Ejemplo

Este es un ejemplo de respuesta para esta llamada a la API.

Respuesta de ejemplo

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateUser

Crea un usuario y lo asocia con un servidor habilitado para Protocolo de transferencia de archivos existente. Solo puede crear y asociar los usuarios con servidores que tengan `IdentityProviderType` establecido en `SERVICE_MANAGED`. Con los parámetros para`CreateUser`, puede especificar el nombre de usuario, establecer el directorio principal, almacenar la clave pública del usuario y asignar la función del usuario AWS Identity and Access Management (IAM). También puede opcionalmente agregar una política de sesiones y asignar metadatos con etiquetas que se pueden utilizar para agrupar y buscar usuarios.

Sintaxis de la solicitud

```
{
   "HomeDirectory": "string",
   "HomeDirectoryMappings": [
      {
         "Entry": "string",
         "Target": "string",
         "Type": "string"
      }
   ],
   "HomeDirectoryType": "string",
   "Policy": "string",
   "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "Role": "string",
   "ServerId": "string",
   "SshPublicKeyBody": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "UserName": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HomeDirectory

Directorio de destino (carpeta) de un usuario cuando inicia sesión en el servidor a través del cliente.

Un ejemplo de `HomeDirectory` es `/bucket_name/home/mydirectory`.

> **Note**
>
> El parámetro `HomeDirectory` solo se utiliza si `HomeDirectoryType` está establecido en `PATH`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

HomeDirectoryMappings

Los mapeos de directorio lógico que especifican qué rutas de acceso y claves de Amazon S3 o Amazon EFS 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. Si solo especifica un destino, se muestra tal cual. También debe asegurarse de que su función AWS Identity and Access Management (de IAM) proporcione acceso a las rutas de entrada. `Target` Este valor solo se puede establecer si `HomeDirectoryType` está establecido en LOGICAL.

Lo siguiente es un ejemplo del par `Entry` y `Target`.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

En la mayoría de los casos, puede usar este valor en lugar de la política de sesión para limitar al usuario al directorio de inicio designado ("chroot"). Para ello, puede establecer Entry a / y establecer Target al valor que el usuario debería ver en su directorio de inicio al iniciar sesión.

A continuación, se muestra un ejemplo del par Entry y Target para chroot.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Tipo: Matriz de HomeDirectoryMapEntry objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50000 artículos.

Obligatorio: no

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 la ruta absoluta 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 HomeDirectoryMappings que correspondan con la forma en que quiere que las rutas de acceso de Amazon S3 o de Amazon EFS sean visibles para sus usuarios.

> **Note**
>
> Si HomeDirectoryType es LOGICAL, debe proporcionar las asignaciones mediante el parámetro HomeDirectoryMappings. Si, por el contrario, HomeDirectoryType es PATH, se proporciona una ruta absoluta mediante el parámetro HomeDirectory. No puede tener HomeDirectory y HomeDirectoryMappings en su plantilla.

Tipo: cadena

Valores válidos: PATH | LOGICAL

Obligatorio: no

Policy

Una política de sesión para su usuario, de modo que pueda usar el mismo rol AWS Identity and Access Management (IAM) en varios usuarios. Esta política reduce el ámbito de acceso de un usuario a partes de su bucket de Amazon S3. Entre las variables que puede utilizar dentro

de esta política se incluyen `${Transfer:UserName}`, `${Transfer:HomeDirectory}` y `${Transfer:HomeBucket}`.

> **Note**
>
> Esta política se aplica solo cuando el dominio de `ServerId` es Amazon S3. Amazon EFS no utiliza políticas de sesión.
> En el caso de las políticas de sesión, AWS Transfer Family almacena la política como un blob de JSON, en lugar del nombre de recurso de Amazon (ARN) de la política. Puede guardar la política como un blob JSON y pasarlo en el argumento `Policy`.
> Para ver un ejemplo de una política de sesión, consulte Example session policy (Ejemplo de política de sesión).
> Para obtener más información, consulte la AssumeRolereferencia de la API AWS de Security Token Service.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: no

PosixProfile

Especifica la identidad POSIX completa, incluido el ID de usuario (`Uid`), el ID de grupo (`Gid`) y cualquier ID de grupo secundario (`SecondaryGids`) 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 Amazon EFS determinan el nivel de acceso que obtienen los usuarios al transferir archivos dentro y fuera de los sistemas de archivos de Amazon EFS.

Tipo: objeto PosixProfile

Obligatorio: no

Role

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que controla el acceso de los usuarios al bucket de Amazon S3 o al sistema de archivos Amazon 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.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: sí

ServerId

Identificador único asignado por el sistema para una instancia del servidor. Este es el servidor específico al que ha agregado el usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

SshPublicKeyBody

La parte pública de la clave Secure Shell (SSH) utilizada para autenticar el usuario en el servidor.

Los tres elementos del formato de la clave pública SSH estándar son `<key type>`, `<body base64>` y uno opcional, `<comment>`, con espacios entre cada elemento.

AWS Transfer Family acepta claves RSA, ECDSA y ED25519.

- En el caso de las claves RSA, el tipo de clave es `ssh-rsa`.
- En el caso de las claves ED25519, el tipo de clave es `ssh-ed25519`.
- En el caso de las claves ECDSA, el tipo de clave es `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384` o `ecdsa-sha2-nistp521`, según el tamaño de la clave que se haya generado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: no

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar usuarios. Las etiquetas son metadatos asociados a usuarios para cualquier fin.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

UserName

Una cadena única que identifica a un usuario y está asociada a `ServerId`. Este nombre de usuario debe tener un mínimo de 3 caracteres y un máximo de 100. A continuación, se muestran caracteres válidos: a-z, A-Z, 0-9, guion bajo “_”, guion “-”, punto “.” y el signo “@”. El nombre de usuario no puede comenzar por un guion, un punto ni una arroba.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ServerId": "string",
   "UserName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ServerId

El ID del servidor al que se asocia el usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

UserName

Una cadena única que identifica a un usuario de Transfer Family.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el servicio. AWS Transfer Family

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

Para crear un usuario, primero puede guardar los parámetros en un archivo JSON, por ejemplo, `createUserParameters`, y luego ejecutar el comando de la API create-user.

```
{
    "HomeDirectory": "/DOC-EXAMPLE-BUCKET",
    "HomeDirectoryType": "PATH",
    "Role": "arn:aws:iam::111122223333:role/bob-role",
    "ServerId": "s-1111aaaa2222bbbb3",
    "SshPublicKeyBody": "ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA...
 bobusa@mycomputer.us-east-1.amazon.com",
    "UserName": "bobusa-API"
}
```

Solicitud de muestra

```
aws transfer create-user --cli-input-json file://createUserParameters
```

Respuesta de ejemplo

```
{
    "ServerId": ""s-1111aaaa2222bbbb3",
    "UserName": "bobusa-API"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS

- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateWorkflow

Permite crear un flujo de trabajo con pasos especificados y detalles de pasos que el flujo de trabajo invoca después de que se completa la transferencia de archivos. Después de crear un flujo de trabajo, puede asociarlo con cualquier servidor de transferencia especificando el campo `workflow-details` en las operaciones `CreateServer` y `UpdateServer`.

Sintaxis de la solicitud

```
{
   "Description": "string",
   "OnExceptionSteps": [
      {
         "CopyStepDetails": {
            "DestinationFileLocation": {
               "EfsFileLocation": {
                  "FileSystemId": "string",
                  "Path": "string"
               },
               "S3FileLocation": {
                  "Bucket": "string",
                  "Key": "string"
               }
            },
            "Name": "string",
            "OverwriteExisting": "string",
            "SourceFileLocation": "string"
         },
         "CustomStepDetails": {
            "Name": "string",
            "SourceFileLocation": "string",
            "Target": "string",
            "TimeoutSeconds": number
         },
         "DecryptStepDetails": {
            "DestinationFileLocation": {
               "EfsFileLocation": {
                  "FileSystemId": "string",
                  "Path": "string"
               },
               "S3FileLocation": {
                  "Bucket": "string",
                  "Key": "string"
```

```
            }
         },
         "Name": "string",
         "OverwriteExisting": "string",
         "SourceFileLocation": "string",
         "Type": "string"
      },
      "DeleteStepDetails": {
         "Name": "string",
         "SourceFileLocation": "string"
      },
      "TagStepDetails": {
         "Name": "string",
         "SourceFileLocation": "string",
         "Tags": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "Type": "string"
   }
],
"Steps": [
   {
      "CopyStepDetails": {
         "DestinationFileLocation": {
            "EfsFileLocation": {
               "FileSystemId": "string",
               "Path": "string"
            },
            "S3FileLocation": {
               "Bucket": "string",
               "Key": "string"
            }
         },
         "Name": "string",
         "OverwriteExisting": "string",
         "SourceFileLocation": "string"
      },
      "CustomStepDetails": {
         "Name": "string",
         "SourceFileLocation": "string",
```

```
            "Target": "string",
            "TimeoutSeconds": number
         },
         "DecryptStepDetails": {
            "DestinationFileLocation": {
               "EfsFileLocation": {
                  "FileSystemId": "string",
                  "Path": "string"
               },
               "S3FileLocation": {
                  "Bucket": "string",
                  "Key": "string"
               }
            },
            "Name": "string",
            "OverwriteExisting": "string",
            "SourceFileLocation": "string",
            "Type": "string"
         },
         "DeleteStepDetails": {
            "Name": "string",
            "SourceFileLocation": "string"
         },
         "TagStepDetails": {
            "Name": "string",
            "SourceFileLocation": "string",
            "Tags": [
               {
                  "Key": "string",
                  "Value": "string"
               }
            ]
         },
         "Type": "string"
      }
   ],
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Description

Descripción del texto del flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `[\w- ]*`

Obligatorio: no

OnExceptionSteps

Especifica los pasos (acciones) que se deben seguir si se encuentran errores durante la ejecución del flujo de trabajo.

> **Note**
>
> En el caso de los pasos personalizados, la función de Lambda debe enviar `FAILURE` a la API de devolución de llamadas para iniciar los pasos de excepción. Además, si la Lambda no se envía `SUCCESS` antes de que se agote el tiempo de espera, se ejecutan los pasos de excepción.

Tipo: matriz de objetos WorkflowStep

Miembros de la matriz: número mínimo de 0 artículos. La cantidad máxima es de 8 elementos.

Obligatorio: no

Steps

Especifica los detalles de los pasos que están en el flujo de trabajo especificado.

`TYPE` especifica cuáles de las siguientes acciones se van a realizar para este paso.

- **COPY** : copiar el archivo en otra ubicación.
- **CUSTOM**- Realice un paso personalizado con un objetivo de AWS Lambda función.
- **DECRYPT** : descifrar un archivo que se cifró antes de subir.
- **DELETE** : eliminar el archivo.
- **TAG** : agregar una etiqueta al archivo.

> **Note**
>
> Actualmente, la copia y el etiquetado solo se admiten en S3.

Para la ubicación del archivo, especifique el bucket y la clave de Amazon S3 o el ID y la ruta del sistema de archivos de Amazon EFS.

Tipo: matriz de objetos WorkflowStep

Miembros de la matriz: número mínimo de 0 artículos. La cantidad máxima es de 8 elementos.

Obligatorio: sí

Tags

Pares clave-valor que se pueden usar para agrupar y buscar flujos de trabajo. Las etiquetas son metadatos asociados a flujos de trabajo para cualquier fin.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "WorkflowId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

Puede guardar la información de los pasos del flujo de trabajo en un archivo de texto y, a continuación, usar ese archivo para crear un flujo de trabajo, como se describe en el siguiente ejemplo. En el siguiente ejemplo, se presupone que guardó los pasos del flujo de trabajo en *example-file.json* (en la misma carpeta desde la que ejecuta el comando) y que desea crear el flujo de trabajo en la región de Norte de Virginia (us-east-1).

```
aws transfer create-workflow --description "example workflow from a file" --steps
 file://example-file.json --region us-east-1
```

```
// Example file containing workflow steps
[
   {
     "Type": "TAG",
     "TagStepDetails": {
        "Name": "TagStep",
        "Tags": [
          {
            "Key": "name",
            "Value": "testTag"
          }
        ]
     }
   },
   {
     "Type": "COPY",
     "CopyStepDetails": {
        "Name": "CopyStep",
        "DestinationFileLocation": {
        "S3FileLocation": {
           "Bucket": "DOC-EXAMPLE-BUCKET",
           "Key": "DOC-EXAMPLE-KEY/"
```

```
                    }
            },
            "OverwriteExisting": "TRUE",
            "SourceFileLocation": "${original.file}"
        }
    },
    {
        "Type": "DELETE",
        "DeleteStepDetails":{
        "Name":"DeleteStep",
        "SourceFileLocation": "${original.file}"
        }
    }
]
```

Ejemplo

La llamada `CreateWorkflow` devuelve el identificador del flujo de trabajo nuevo.

Respuesta de ejemplo

```
{
    "WorkflowId": "w-1234abcd5678efghi"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteAccess

Permite eliminar el acceso especificado en los parámetros `ServerID` y `ExternalID`.

Sintaxis de la solicitud

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ExternalId

Un identificador único que se requiere para identificar grupos específicos dentro de su directorio. Los usuarios del grupo que asocie tienen acceso a sus recursos de Amazon S3 o Amazon EFS a través de los protocolos habilitados que utilizan AWS Transfer Family. Si conoce el nombre del grupo, puede ver los valores del SID ejecutando el siguiente comando en Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

En ese comando, YourGroupNamesustitúyalo por el nombre del grupo de Active Directory.

La expresión regular utilizada para validar este parámetro es una cadena de caracteres compuesta de caracteres alfanuméricos en mayúscula y minúscula, sin espacios. También puede incluir guiones bajos y cualquiera de los siguientes caracteres: =,.@:/-

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `S-1-[\d-]+`

Obligatorio: sí

ServerId

Identificador único asignado por el sistema para un servidor que tiene asignado este usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteAgreement

Eliminar el acuerdo que se especifica en el formulario proporcionado `AgreementId`

Sintaxis de la solicitud

```
{
   "AgreementId": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

AgreementId

Un identificador único para el acuerdo. Este identificador se devuelve al crear un acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `a-([0-9a-f]{17})`

Obligatorio: sí

ServerId

Identificador del servidor asociado al acuerdo que va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2

- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteCertificate

Elimina el certificado especificado en el parámetro `CertificateId`.

Sintaxis de la solicitud

```
{
   "CertificateId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

CertificateId

Identificador del objeto de certificado que se va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteConnector

Elimina el conector que se especifica en el `ConnectorId` proporcionado.

Sintaxis de la solicitud

```
{
   "ConnectorId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ConnectorId

Un identificador único para el conector.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteHostKey

Elimina la clave de host especificada en el parámetro `HostKeyId`.

Sintaxis de la solicitud

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HostKeyId

Identificador de la clave de host que está eliminando.

Tipo: cadena

Limitaciones de longitud: longitud fija de 25.

Patrón: `hostkey-[0-9a-f]{17}`

Obligatorio: sí

ServerId

El identificador del servidor que contiene la clave de host que se va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteProfile

Elimina el perfil especificado en el parámetro `ProfileId`.

Sintaxis de la solicitud

```
{
   "ProfileId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ProfileId

Identificador del perfil que se va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteServer

Elimina el servidor habilitado para el protocolo de transferencia de archivos que especifique.

No se obtiene ninguna respuesta de esta operación.

Sintaxis de la solicitud

```
{
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ServerId

Identificador único asignado por el sistema para una instancia del servidor.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

En el siguiente ejemplo se elimina un servidor.

Solicitud de muestra

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Ejemplo

Si se realiza correctamente, no se devuelve nada.

Respuesta de ejemplo

```
{
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteSshPublicKey

Elimina una Secure Shell (SSH) de una clave pública.

Sintaxis de la solicitud

```
{
   "ServerId": "string",
   "SshPublicKeyId": "string",
   "UserName": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ServerId

Un identificador único asignado por el sistema para una instancia de servidor habilitada para protocolo de transferencia de archivos al que le ha sido asignada el usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

SshPublicKeyId

Un identificador único que se utiliza para hacer referencia a la clave SSH específica del usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 21.

Patrón: `key-[0-9a-f]{17}`

Obligatorio: sí

UserName

Cadena única que identifica un usuario cuya clave pública está siendo eliminada.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

El siguiente ejemplo elimina una clave pública SSH de usuario.

Solicitud de muestra

```
{
   "ServerId": "s-01234567890abcdef",
   "SshPublicKeyId": "MyPublicKey",
   "UserName": "my_user"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteUser

Elimina el usuario que pertenece a un servidor habilitado para el protocolo de transferencia de archivos que especifique.

No se obtiene ninguna respuesta de esta operación.

> **Note**
>
> Al eliminar un usuario de un servidor, se pierde la información del usuario.

Sintaxis de la solicitud

```
{
   "ServerId": "string",
   "UserName": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ServerId

Identificador único asignado por el sistema para una instancia del servidor que tiene el usuario asignado.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

UserName

Una cadena única que identifica a un usuario que se está eliminando de un servidor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

En el siguiente ejemplo, se elimina un usuario de Transfer Family.

Solicitud de muestra

```
{
   "ServerId": "s-01234567890abcdef",
   "UserNames": "my_user"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteWorkflow

Actualiza el flujo de trabajo especificado.

Sintaxis de la solicitud

```
{
   "WorkflowId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeAccess

Describe el acceso que se asigna al servidor específico habilitado para el protocolo de transferencia de archivos, identificado por su propiedad `ServerId` y su `ExternalId`.

La respuesta de esta llamada devuelve las propiedades del acceso asociado al valor `ServerId` especificado.

Sintaxis de la solicitud

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ExternalId

Un identificador único que se requiere para identificar grupos específicos dentro de su directorio. Los usuarios del grupo que asocie tienen acceso a sus recursos de Amazon S3 o Amazon EFS a través de los protocolos habilitados que utilizan AWS Transfer Family. Si conoce el nombre del grupo, puede ver los valores del SID ejecutando el siguiente comando en Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

En ese comando, YourGroupNamesustitúyalo por el nombre del grupo de Active Directory.

La expresión regular utilizada para validar este parámetro es una cadena de caracteres compuesta de caracteres alfanuméricos en mayúscula y minúscula, sin espacios. También puede incluir guiones bajos y cualquiera de los siguientes caracteres: =,.@:/-

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `S-1-[\d-]+`

Obligatorio: sí

ServerId

Identificador único asignado por el sistema para un servidor que tiene asignado este acceso.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Access": {
      "ExternalId": "string",
      "HomeDirectory": "string",
      "HomeDirectoryMappings": [
         {
            "Entry": "string",
            "Target": "string",
            "Type": "string"
         }
      ],
      "HomeDirectoryType": "string",
      "Policy": "string",
      "PosixProfile": {
         "Gid": number,
         "SecondaryGids": [ number ],
         "Uid": number
      },
      "Role": "string"
   },
   "ServerId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Access

El identificador externo del servidor al que está conectado el acceso.

Tipo: objeto DescribedAccess

ServerId

Identificador único asignado por el sistema para un servidor que tiene asignado este acceso.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeAgreement

Describe el acuerdo que se identifica mediante `AgreementId`.

Sintaxis de la solicitud

```
{
   "AgreementId": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

AgreementId

Un identificador único para el acuerdo. Este identificador se devuelve al crear un acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `a-([0-9a-f]{17})`

Obligatorio: sí

ServerId

El identificador del servidor asociado al acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Agreement": {
      "AccessRole": "string",
      "AgreementId": "string",
      "Arn": "string",
      "BaseDirectory": "string",
      "Description": "string",
      "LocalProfileId": "string",
      "PartnerProfileId": "string",
      "ServerId": "string",
      "Status": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Agreement

Los detalles del acuerdo especificado, devueltos como un objeto `DescribedAgreement`.

Tipo: objeto DescribedAgreement

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeCertificate

Describe el certificado que se identifica con `CertificateId`.

Sintaxis de la solicitud

```
{
   "CertificateId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

CertificateId

Una matriz de identificadores de los certificados importados. Este identificador se utiliza para trabajar con perfiles y perfiles de socios.

Tipo: cadena

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Certificate": {
      "ActiveDate": number,
      "Arn": "string",
      "Certificate": "string",
      "CertificateChain": "string",
      "CertificateId": "string",
      "Description": "string",
      "InactiveDate": number,
```

```
      "NotAfterDate": number,
      "NotBeforeDate": number,
      "Serial": "string",
      "Status": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Type": "string",
      "Usage": "string"
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Certificate

Los detalles del certificado especificado, devuelto como un objeto.

Tipo: objeto DescribedCertificate

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeConnector

Describe el conector que se identifica mediante `ConnectorId`.

Sintaxis de la solicitud

```
{
   "ConnectorId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ConnectorId

Un identificador único para el conector.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Connector": {
      "AccessRole": "string",
      "Arn": "string",
      "As2Config": {
         "BasicAuthSecretId": "string",
         "Compression": "string",
         "EncryptionAlgorithm": "string",
         "LocalProfileId": "string",
         "MdnResponse": "string",
         "MdnSigningAlgorithm": "string",
```

```
         "MessageSubject": "string",
         "PartnerProfileId": "string",
         "SigningAlgorithm": "string"
      },
      "ConnectorId": "string",
      "LoggingRole": "string",
      "SecurityPolicyName": "string",
      "ServiceManagedEgressIpAddresses": [ "string" ],
      "SftpConfig": {
         "TrustedHostKeys": [ "string" ],
         "UserSecretId": "string"
      },
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Url": "string"
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Connector

Estructura que contiene los detalles del conector.

Tipo: objeto DescribedConnector

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeExecution

Puede utilizar `DescribeExecution` para comprobar los detalles de la ejecución del flujo de trabajo especificado.

> **Note**
>
> Esta llamada a la API solo devuelve detalles de los flujos de trabajo en curso.
> Si proporciona un identificador para una ejecución que no está en curso o si la ejecución no coincide con el identificador del flujo de trabajo especificado, recibirá una excepción `ResourceNotFound`.

Sintaxis de la solicitud

```
{
   "ExecutionId": "string",
   "WorkflowId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ExecutionId

Un identificador único para la ejecución del flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 36.

Patrón: `[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

Obligatorio: sí

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Execution": {
      "ExecutionId": "string",
      "ExecutionRole": "string",
      "InitialFileLocation": {
         "EfsFileLocation": {
            "FileSystemId": "string",
            "Path": "string"
         },
         "S3FileLocation": {
            "Bucket": "string",
            "Etag": "string",
            "Key": "string",
            "VersionId": "string"
         }
      },
      "LoggingConfiguration": {
         "LoggingRole": "string",
         "LogGroupName": "string"
      },
      "PosixProfile": {
         "Gid": number,
         "SecondaryGids": [ number ],
         "Uid": number
      },
      "Results": {
         "OnExceptionSteps": [
            {
               "Error": {
```

```
                  "Message": "string",
                  "Type": "string"
               },
               "Outputs": "string",
               "StepType": "string"
            }
         ],
         "Steps": [
            {
               "Error": {
                  "Message": "string",
                  "Type": "string"
               },
               "Outputs": "string",
               "StepType": "string"
            }
         ]
      },
      "ServiceMetadata": {
         "UserDetails": {
            "ServerId": "string",
            "SessionId": "string",
            "UserName": "string"
         }
      },
      "Status": "string"
   },
   "WorkflowId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Execution

La estructura que contiene los detalles de la ejecución del flujo de trabajo.

Tipo: objeto DescribedExecution

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++

- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeHostKey

Devuelve los detalles de la clave de host especificada por `HostKeyId` y `ServerId`.

Sintaxis de la solicitud

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HostKeyId

El identificador de la clave de host que desea describir.

Tipo: cadena

Limitaciones de longitud: longitud fija de 25.

Patrón: `hostkey-[0-9a-f]{17}`

Obligatorio: sí

ServerId

El identificador del servidor que contiene la clave de host que desea describir.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "HostKey": {
      "Arn": "string",
      "DateImported": number,
      "Description": "string",
      "HostKeyFingerprint": "string",
      "HostKeyId": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Type": "string"
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HostKey

Devuelve los detalles para la clave de host especificado.

Tipo: objeto DescribedHostKey

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeProfile

Devuelve los detalles del perfil especificado por el `ProfileId`.

Sintaxis de la solicitud

```
{
   "ProfileId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ProfileId

El identificador del perfil que desea describir.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Profile": {
      "Arn": "string",
      "As2Id": "string",
      "CertificateIds": [ "string" ],
      "ProfileId": "string",
      "ProfileType": "string",
      "Tags": [
         {
            "Key": "string",
```

```
            "Value": "string"
         }
      ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Profile

Los detalles del perfil especificado, devueltos como un objeto.

Tipo: objeto DescribedProfile

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeSecurityPolicy

Describe la política de seguridad que se adjunta al servidor o al conector SFTP. La respuesta contiene una descripción de las propiedades de la política de seguridad. Para obtener más información sobre las políticas de seguridad, consulte Uso de políticas de seguridad para servidores o Uso de políticas de seguridad para conectores SFTP.

Sintaxis de la solicitud

```
{
   "SecurityPolicyName": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

SecurityPolicyName

Especifique el nombre textual de la política de seguridad de la que desea obtener los detalles.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 100 caracteres.

Patrón: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "SecurityPolicy": {
      "Fips": boolean,
      "Protocols": [ "string" ],
      "SecurityPolicyName": "string",
      "SshCiphers": [ "string" ],
      "SshHostKeyAlgorithms": [ "string" ],
```

```
      "SshKexs": [ "string" ],
      "SshMacs": [ "string" ],
      "TlsCiphers": [ "string" ],
      "Type": "string"
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

SecurityPolicy

Matriz que contiene las propiedades de la política de seguridad.

Tipo: objeto DescribedSecurityPolicy

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

El siguiente comando de ejemplo toma el nombre de la política de seguridad como argumento y devuelve los algoritmos de la política de seguridad especificada.

Solicitud de muestra

```
aws transfer describe-security-policy --security-policy-name "TransferSecurityPolicy-
FIPS-2023-05"
```

Respuesta de ejemplo

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

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeServer

Describe un servidor habilitado para el protocolo de transferencia de archivos que se especifica pasando el parámetro `ServerId`.

La respuesta contiene una descripción de las propiedades de un servidor. Cuando se configura `EndpointType` en VPC, la respuesta contendrá `EndpointDetails`.

Sintaxis de la solicitud

```
{
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ServerId

Identificador único asignado por el sistema para un servidor.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Server": {
      "Arn": "string",
      "As2ServiceManagedEgressIpAddresses": [ "string" ],
      "Certificate": "string",
      "Domain": "string",
      "EndpointDetails": {
```

```
      "AddressAllocationIds": [ "string" ],
      "SecurityGroupIds": [ "string" ],
      "SubnetIds": [ "string" ],
      "VpcEndpointId": "string",
      "VpcId": "string"
   },
   "EndpointType": "string",
   "HostKeyFingerprint": "string",
   "IdentityProviderDetails": {
      "DirectoryId": "string",
      "Function": "string",
      "InvocationRole": "string",
      "SftpAuthenticationMethods": "string",
      "Url": "string"
   },
   "IdentityProviderType": "string",
   "LoggingRole": "string",
   "PostAuthenticationLoginBanner": "string",
   "PreAuthenticationLoginBanner": "string",
   "ProtocolDetails": {
      "As2Transports": [ "string" ],
      "PassiveIp": "string",
      "SetStatOption": "string",
      "TlsSessionResumptionMode": "string"
   },
   "Protocols": [ "string" ],
   "S3StorageOptions": {
      "DirectoryListingOptimization": "string"
   },
   "SecurityPolicyName": "string",
   "ServerId": "string",
   "State": "string",
   "StructuredLogDestinations": [ "string" ],
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "UserCount": number,
   "WorkflowDetails": {
      "OnPartialUpload": [
         {
            "ExecutionRole": "string",
```

```
                "WorkflowId": "string"
            }
         ],
         "OnUpload": [
            {
               "ExecutionRole": "string",
               "WorkflowId": "string"
            }
         ]
      }
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Server

Una matriz que contiene las propiedades de un servidor con las `ServerID` que especificó.

Tipo: objeto DescribedServer

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

En el siguiente ejemplo, se devuelven las propiedades asignadas a un servidor.

Solicitud de muestra

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Ejemplo

Este ejemplo ilustra un uso de DescribeServer.

Respuesta de ejemplo

```
{
    "Server": {
        "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
        "EndpointDetails": {
            "AddressAllocationIds": [
                "eipalloc-01a2eabe3c04d5678",
                "eipalloc-102345be"
            ],
            "SubnetIds": [
                "subnet-047eaa7f0187a7cde",
                "subnet-0a2d0f474daffde18"
            ],
            "VpcEndpointId": "vpce-03fe0080e7cb008b8",
            "VpcId": "vpc-09047a51f1c8e1634"
        },
```

```
        "EndpointType": "VPC",
        "HostKeyFingerprint": "your host key,
        "IdentityProviderType": "SERVICE_MANAGED",
        "ServerId": "s-01234567890abcdef",
        "State": "ONLINE",
        "Tags": [],
        "UserCount": 0
    }
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeUser

Describe el usuario asignado al servidor específico habilitado para el protocolo de transferencia de archivos, identificado por su propiedad `ServerId`.

La respuesta de esta llamada devuelve las propiedades del usuario asociadas al valor especificado `ServerId`.

Sintaxis de la solicitud

```
{
   "ServerId": "string",
   "UserName": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ServerId

Identificador único asignado por el sistema para un servidor que tiene asignado este usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

UserName

El nombre del usuario asignado a uno o más servidores. Los nombres de usuario forman parte de las credenciales de inicio de sesión para usar el AWS Transfer Family servicio y realizar tareas de transferencia de archivos.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ServerId": "string",
   "User": {
      "Arn": "string",
      "HomeDirectory": "string",
      "HomeDirectoryMappings": [
         {
            "Entry": "string",
            "Target": "string",
            "Type": "string"
         }
      ],
      "HomeDirectoryType": "string",
      "Policy": "string",
      "PosixProfile": {
         "Gid": number,
         "SecondaryGids": [ number ],
         "Uid": number
      },
      "Role": "string",
      "SshPublicKeys": [
         {
            "DateImported": number,
            "SshPublicKeyBody": "string",
            "SshPublicKeyId": "string"
         }
      ],
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "UserName": "string"
   }
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ServerId

Identificador único asignado por el sistema para un servidor que tiene asignado este usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

User

Matriz que contiene las propiedades del usuario Transfer Family para el valor `ServerID` que especificó.

Tipo: objeto DescribedUser

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

En el ejemplo siguiente se muestran los detalles de un usuario existente.

Solicitud de muestra

```
aws transfer describe-user --server-id s-1111aaaa2222bbbb3 --user-name bob-test
```

Respuesta de ejemplo

```
{
    "ServerId": "s-1111aaaa2222bbbb3",
    "User": {
        "Arn": "arn:aws:transfer:us-east-1:111122223333:user/s-1111aaaa2222bbbb3/bob-
test",
        "HomeDirectory": "/DOC-EXAMPLE-BUCKET",
        "HomeDirectoryType": "PATH",
        "Role": "arn:aws:iam::111122223333:role/bob-role",
        "SshPublicKeys": [
            {
                "DateImported": "2022-03-31T12:27:52.614000-04:00",
                "SshPublicKeyBody": "ssh-rsa AAAAB3NzaC1yc..... bobusa@mycomputer.us-
east-1.amaazon.com",
                "SshPublicKeyId": "key-abcde12345fghik67"
            }
        ],
        "Tags": [],
        "UserName": "bob-test"
    }
```

```
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeWorkflow

Describe el flujo de trabajo especificado.

Sintaxis de la solicitud

```
{
   "WorkflowId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Workflow": {
      "Arn": "string",
      "Description": "string",
      "OnExceptionSteps": [
         {
            "CopyStepDetails": {
               "DestinationFileLocation": {
                  "EfsFileLocation": {
                     "FileSystemId": "string",
                     "Path": "string"
                  },
```

```
            "S3FileLocation": {
               "Bucket": "string",
               "Key": "string"
            }
         },
         "Name": "string",
         "OverwriteExisting": "string",
         "SourceFileLocation": "string"
      },
      "CustomStepDetails": {
         "Name": "string",
         "SourceFileLocation": "string",
         "Target": "string",
         "TimeoutSeconds": number
      },
      "DecryptStepDetails": {
         "DestinationFileLocation": {
            "EfsFileLocation": {
               "FileSystemId": "string",
               "Path": "string"
            },
            "S3FileLocation": {
               "Bucket": "string",
               "Key": "string"
            }
         },
         "Name": "string",
         "OverwriteExisting": "string",
         "SourceFileLocation": "string",
         "Type": "string"
      },
      "DeleteStepDetails": {
         "Name": "string",
         "SourceFileLocation": "string"
      },
      "TagStepDetails": {
         "Name": "string",
         "SourceFileLocation": "string",
         "Tags": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
```

```
            },
            "Type": "string"
         }
      ],
      "Steps": [
         {
            "CopyStepDetails": {
               "DestinationFileLocation": {
                  "EfsFileLocation": {
                     "FileSystemId": "string",
                     "Path": "string"
                  },
                  "S3FileLocation": {
                     "Bucket": "string",
                     "Key": "string"
                  }
               },
               "Name": "string",
               "OverwriteExisting": "string",
               "SourceFileLocation": "string"
            },
            "CustomStepDetails": {
               "Name": "string",
               "SourceFileLocation": "string",
               "Target": "string",
               "TimeoutSeconds": number
            },
            "DecryptStepDetails": {
               "DestinationFileLocation": {
                  "EfsFileLocation": {
                     "FileSystemId": "string",
                     "Path": "string"
                  },
                  "S3FileLocation": {
                     "Bucket": "string",
                     "Key": "string"
                  }
               },
               "Name": "string",
               "OverwriteExisting": "string",
               "SourceFileLocation": "string",
               "Type": "string"
            },
            "DeleteStepDetails": {
```

```
                "Name": "string",
                "SourceFileLocation": "string"
            },
            "TagStepDetails": {
                "Name": "string",
                "SourceFileLocation": "string",
                "Tags": [
                    {
                        "Key": "string",
                        "Value": "string"
                    }
                ]
            },
            "Type": "string"
        }
    ],
    "Tags": [
        {
            "Key": "string",
            "Value": "string"
        }
    ],
    "WorkflowId": "string"
  }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Workflow

Estructura que contiene los detalles del flujo.

Tipo: objeto DescribedWorkflow

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ImportCertificate

Importa los certificados de firma y cifrado que necesita para crear perfiles locales (AS2) y perfiles de socios.

Sintaxis de la solicitud

```
{
   "ActiveDate": number,
   "Certificate": "string",
   "CertificateChain": "string",
   "Description": "string",
   "InactiveDate": number,
   "PrivateKey": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Usage": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ActiveDate

Una fecha opcional que especifica cuándo se activa el certificado.

Tipo: marca temporal

Obligatorio: no

Certificate

- Para la CLI, proporcione una ruta de archivo para un certificado en formato URI. Por ejemplo, `--certificate file://encryption-cert.pem`. Si lo desea, también puede proporcionar el contenido sin procesar.

- Para el SDK, especifique el contenido sin procesar de un archivo de certificado. Por ejemplo, `--certificate "`cat encryption-cert.pem`"`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 16384 caracteres.

Patrón: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Obligatorio: sí

CertificateChain

Una lista opcional de certificados que forman la cadena del certificado que se está importando.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 2097152.

Patrón: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Obligatorio: no

Description

Una breve descripción que ayuda a identificar el certificado.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Graph}]+`

Obligatorio: no

InactiveDate

Una fecha opcional que especifica cuándo el certificado pasa a estar inactivo.

Tipo: marca temporal

Obligatorio: no

PrivateKey

- Para la CLI, proporcione una ruta de archivo para una clave privada en formato URI. Por ejemplo, `--private-key file://encryption-key.pem`. Como alternativa, puede proporcionar el contenido sin procesar del archivo de clave privada.

- Para el SDK, especifique el contenido sin procesar de un archivo de clave privada. Por ejemplo, `--private-key "`cat encryption-key.pem`"`

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 16384 caracteres.

Patrón: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Obligatorio: no

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar certificados.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Usage

Especifica cómo se utiliza este certificado. Se puede utilizar de las siguientes maneras:

- `SIGNING`: Para firmar mensajes AS2
- `ENCRYPTION`: Para cifrar mensajes AS2
- `TLS`: Para proteger las comunicaciones AS2 enviadas a través de HTTPS

Tipo: cadena

Valores válidos: `SIGNING | ENCRYPTION`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "CertificateId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CertificateId

Una matriz de identificadores de los certificados importados. Este identificador se utiliza para trabajar con perfiles y perfiles de socios.

Tipo: cadena

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

En el siguiente ejemplo, se importa un certificado para usarlo en el cifrado. En el primer comando, proporcionamos el contenido del certificado y de los archivos de la cadena de certificados. Use este formato para los comandos del SDK.

```
aws transfer import-certificate --usage ENCRYPTION --certificate "`cat encryption-
cert.pem`" \
    --private-key "`cat encryption-key.pem`" --certificate-chain "`cat root-ca.pem`"
```

Ejemplo

El siguiente ejemplo es idéntico al comando anterior, excepto que proporcionamos las ubicaciones de los archivos de la clave privada, el certificado y la cadena de certificados. Esta versión del comando no funciona si utiliza un SDK.

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

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ImportHostKey

Agregue una clave de host al servidor especificada por el parámetro `ServerId`.

Sintaxis de la solicitud

```
{
   "Description": "string",
   "HostKeyBody": "string",
   "ServerId": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Description

La descripción textual que identifica esta clave de host.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Print}]*`

Obligatorio: no

HostKeyBody

La parte de clave privada de un par de claves SSH.

AWS Transfer Family acepta claves RSA, ECDSA y ED25519.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 4096 caracteres.

Obligatorio: sí

ServerId

El identificador del servidor que contiene la clave de host que se va a importar.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar claves de host.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HostKeyId

Devuelve el identificador de clave de host de la clave importada.

Tipo: cadena

Limitaciones de longitud: longitud fija de 25.

Patrón: `hostkey-[0-9a-f]{17}`

ServerId

Devuelve el identificador del servidor que contiene la clave importada.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el servicio. AWS Transfer Family

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ImportSshPublicKey

Añade una clave pública de Secure Shell (SSH) a un usuario de Transfer Family identificado por un valor `UserName` asignado al servidor habilitado para el protocolo de File Transfer específico, identificado por `ServerId`.

La respuesta devuelve el valor `UserName`, el valor `ServerId` y el nombre de `SshPublicKeyId`.

Sintaxis de la solicitud

```
{
   "ServerId": "string",
   "SshPublicKeyBody": "string",
   "UserName": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ServerId

Identificador único asignado por el sistema para un servidor.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

SshPublicKeyBody

La parte de clave pública de un par de claves SSH.

AWS Transfer Family acepta claves RSA, ECDSA y ED25519.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: sí

UserName

El nombre del usuario de Transfer Family que está asignado a uno o más servidores.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ServerId": "string",
   "SshPublicKeyId": "string",
   "UserName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ServerId

Identificador único asignado por el sistema para un servidor.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

SshPublicKeyId

Nombre otorgado a una clave pública por el sistema que se importó.

Tipo: cadena

Limitaciones de longitud: longitud fija de 21.

Patrón: `key-[0-9a-f]{17}`

UserName

Un nombre de usuario otorgado al `ServerID` valor que especificó.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el servicio. AWS Transfer Family

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

Este comando importa una clave ECDSA almacenada en el archivo `id_ecdsa.pub`.

```
aws transfer import-ssh-public-key --server-id s-021345abcdef6789 --ssh-public-key-body
 file://id_ecdsa.pub --user-name jane-doe
```

Ejemplo

Si ejecuta el comando anterior, el sistema devuelve la siguiente información.

```
{
    "ServerId": "s-021345abcdef6789",
   "SshPublicKeyId": "key-1234567890abcdef0",
   "UserName": "jane-doe"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2

- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListAccesses

Muestra los detalles de todos los accesos que tiene en su servidor.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

Especifica el número máximo de SID de acceso que se van a devolver.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Cuando pueda obtener resultados adicionales de la llamada `ListAccesses`, se devolverá un parámetro `NextToken` en la salida. A continuación, puede pasar un comando posterior al parámetro `NextToken` para seguir enumerando los accesos adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

ServerId

Identificador único asignado por el sistema para un servidor que tiene usuarios asignados.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Accesses": [
      {
         "ExternalId": "string",
         "HomeDirectory": "string",
         "HomeDirectoryType": "string",
         "Role": "string"
      }
   ],
   "NextToken": "string",
   "ServerId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Accesses

Devuelve los accesos y sus propiedades para el valor `ServerId` que especifique.

Tipo: matriz de objetos ListedAccess

NextToken

Cuando pueda obtener resultados adicionales de la llamada `ListAccesses`, se devolverá un parámetro `NextToken` en la salida. A continuación, puede pasar un comando posterior al parámetro `NextToken` para seguir enumerando los accesos adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

ServerId

Identificador único asignado por el sistema para un servidor que tiene usuarios asignados.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListAgreements

Devuelve una lista de los acuerdos del servidor que se identifica con el `ServerId` que usted proporciona. Si desea limitar los resultados a un número determinado, introduzca un valor para el parámetro `MaxResults`. Si ejecutó el comando anteriormente y recibió un valor para `NextToken`, puede proporcionarlo para seguir enumerando los acuerdos desde donde los dejó.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

El número máximo de acuerdos que devolver.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Cuando pueda obtener resultados adicionales de la llamada `ListAgreements`, se devolverá un parámetro `NextToken` en la salida. A continuación, puede pasar un comando posterior al parámetro `NextToken` para seguir enumerando los acuerdos adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

ServerId

El identificador del servidor para el que desea obtener una lista de acuerdos.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Agreements": [
      {
         "AgreementId": "string",
         "Arn": "string",
         "Description": "string",
         "LocalProfileId": "string",
         "PartnerProfileId": "string",
         "ServerId": "string",
         "Status": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Agreements

Devuelve una matriz en la que cada elemento contiene los detalles de un acuerdo.

Tipo: matriz de objetos ListedAgreement

NextToken

Devuelve un token que puede usar para volver a llamar a `ListAgreements` y recibir resultados adicionales, si los hay.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListCertificates

Devuelve una lista de los certificados actuales que se han importado AWS Transfer Family. Si desea limitar los resultados a un número determinado, introduzca un valor para el parámetro `MaxResults`. Si ejecutó el comando anteriormente y recibió un valor para el parámetro `NextToken`, puede proporcionarlo para seguir enumerando los certificados desde donde los dejó.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

El número máximo de certificados para devolver.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Cuando pueda obtener resultados adicionales de la llamada `ListCertificates`, se devolverá un parámetro `NextToken` en la salida. A continuación, puede pasar un comando posterior al parámetro `NextToken` para seguir enumerando los certificados adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "Certificates": [
      {
         "ActiveDate": number,
         "Arn": "string",
         "CertificateId": "string",
         "Description": "string",
         "InactiveDate": number,
         "Status": "string",
         "Type": "string",
         "Usage": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Certificates

Devuelve una matriz de los certificados que se especifican en la llamada `ListCertificates`.

Tipo: matriz de objetos ListedCertificate

NextToken

Devuelve el siguiente token, que puede usar para enumerar el siguiente certificado.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

ListConnectors

Muestra los conectores de la región especificada.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

El número máximo de conectores por devolver.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Cuando pueda obtener resultados adicionales de la llamada `ListConnectors`, se devolverá un parámetro `NextToken` en la salida. A continuación, puede pasar un comando posterior al parámetro `NextToken` para seguir enumerando conectores adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
{
```

```
   "Connectors": [
      {
         "Arn": "string",
         "ConnectorId": "string",
         "Url": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Connectors

Devuelve una matriz en la que cada elemento contiene los detalles de un conector.

Tipo: matriz de objetos ListedConnector

NextToken

Devuelve un token que puede usar para volver a llamar a `ListConnectors` y recibir resultados adicionales, si los hay.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListExecutions

Muestra todas las ejecuciones en curso del flujo de trabajo especificado.

> **Note**
>
> Si no se encuentra el identificador de flujo de trabajo especificado, `ListExecutions` devuelve una excepción `ResourceNotFound`.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string",
   "WorkflowId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

Especifica el número máximo de ejecuciones que se van a devolver.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

`ListExecutions` devuelve el parámetro `NextToken` en la salida. A continuación, puede pasar el parámetro `NextToken` en un comando posterior para seguir enumerando las ejecuciones adicionales.

Esto es útil para la paginación, por ejemplo. Si tiene 100 ejecuciones para un flujo de trabajo, es posible que solo desee enumerar las 10 primeras. Si es así, llame a la API al especificar el `max-results`:

```
aws transfer list-executions --max-results 10
```

Esto devuelve los detalles de las 10 primeras ejecuciones, así como el puntero (`NextToken`) de la undécima ejecución. Ahora puede volver a llamar a la API proporcionando el valor `NextToken` que recibió:

```
aws transfer list-executions --max-results 10 --next-token
$somePointerReturnedFromPreviousListResult
```

Esta llamada devuelve las siguientes 10 ejecuciones, de la undécima a la vigésima. A continuación, puede repetir la llamada hasta obtener los detalles de las 100 ejecuciones.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Executions": [
      {
         "ExecutionId": "string",
         "InitialFileLocation": {
            "EfsFileLocation": {
               "FileSystemId": "string",
```

```
                "Path": "string"
            },
            "S3FileLocation": {
                "Bucket": "string",
                "Etag": "string",
                "Key": "string",
                "VersionId": "string"
            }
        },
        "ServiceMetadata": {
            "UserDetails": {
                "ServerId": "string",
                "SessionId": "string",
                "UserName": "string"
            }
        },
        "Status": "string"
      }
   ],
   "NextToken": "string",
   "WorkflowId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Executions

Devuelve los detalles de cada ejecución, en una matriz `ListedExecution`.

Tipo: matriz de objetos ListedExecution

NextToken

`ListExecutions` devuelve el parámetro `NextToken` en la salida. A continuación, puede pasar el parámetro `NextToken` en un comando posterior para seguir enumerando las ejecuciones adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListHostKeys

Agregue una lista de claves de host al servidor especificada por el `ServerId` parámetro.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

Número máximo de claves de host que se devolverán.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Cuando hay resultados adicionales que no se devolvieron, se devuelve un parámetro `NextToken`. Puede usar ese valor en una llamada posterior a `ListHostKeys` para seguir publicando los resultados.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

ServerId

El identificador del servidor que contiene las claves del host que desea visualizar.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "HostKeys": [
      {
         "Arn": "string",
         "DateImported": number,
         "Description": "string",
         "Fingerprint": "string",
         "HostKeyId": "string",
         "Type": "string"
      }
   ],
   "NextToken": "string",
   "ServerId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HostKeys

Devuelve una matriz en la que cada elemento contiene los detalles de una clave del host.

Tipo: matriz de objetos ListedHostKey

NextToken

Devuelve un token que puede usar para volver a llamar a `ListHostKeys` y recibir resultados adicionales, si los hay.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

ServerId

Devuelve el identificador del servidor que contiene las claves del host enumeradas.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListProfiles

Devuelve una lista de los perfiles del sistema. Si desea limitar los resultados a un número determinado, introduzca un valor para el parámetro `MaxResults`. Si ejecutó el comando anteriormente y recibió un valor para `NextToken`, puede proporcionarlo para seguir enumerando los perfiles desde donde los dejó.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ProfileType": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

Número máximo de perfiles que se devolverán.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Cuando hay resultados adicionales que no se devolvieron, se devuelve un parámetro `NextToken`. Puede usar ese valor en una llamada posterior a `ListProfiles` para seguir publicando los resultados.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

ProfileType

Indica si se deben enumerar solo los perfiles de tipo `LOCAL` o solo los perfiles de tipo `PARTNER`. Si no se proporciona en la solicitud, el comando muestra todos los tipos de perfiles.

Tipo: cadena

Valores válidos: `LOCAL | PARTNER`

Obligatorio: no

Sintaxis de la respuesta

```
{
   "NextToken": "string",
   "Profiles": [
      {
         "Arn": "string",
         "As2Id": "string",
         "ProfileId": "string",
         "ProfileType": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Devuelve un token que puede usar para volver a llamar a `ListProfiles` y recibir resultados adicionales, si los hay.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Profiles

Devuelve una matriz en la que cada elemento contiene los detalles de un perfil.

Tipo: matriz de objetos ListedProfile

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListSecurityPolicies

Enumera las políticas de seguridad que están conectadas a los servidores y a los conectores SFTP. Para obtener más información sobre las políticas de seguridad, consulte Uso de políticas de seguridad para servidores o Uso de políticas de seguridad para conectores SFTP.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

Especifica el número de políticas de seguridad que se devolverán como respuesta a la consulta `ListSecurityPolicies`.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Cuando se obtienen resultados adicionales del comando `ListSecurityPolicies`, se devuelve un parámetro `NextToken` en la salida. A continuación, puede pasar un comando posterior al parámetro `NextToken` para seguir enumerando las políticas de seguridad adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "NextToken": "string",
   "SecurityPolicyNames": [ "string" ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Cuando pueda obtener resultados adicionales de la operación `ListSecurityPolicies`, se devolverá un parámetro `NextToken` en la salida. En el siguiente comando, puede pasar el parámetro `NextToken` para seguir enumerando las políticas de seguridad.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

SecurityPolicyNames

Matriz de políticas de seguridad que se enumeraron.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 100 caracteres.

Patrón: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

En el siguiente ejemplo, se muestran los nombres de todas las políticas de seguridad disponibles.

Solicitud de muestra

```
aws transfer list-security-policies
```

Respuesta de ejemplo

```
{
    "SecurityPolicyNames": [
        "TransferSecurityPolicy-2023-05",
        "TransferSecurityPolicy-2022-03",
        "TransferSecurityPolicy-FIPS-2024-01",
        "TransferSecurityPolicy-2024-01",
        "TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04",
        "TransferSecurityPolicy-PQ-SSH-Experimental-2023-04",
        "TransferSecurityPolicy-FIPS-2020-06",
        "TransferSecurityPolicy-2020-06",
        "TransferSecurityPolicy-2018-11",
        "TransferSecurityPolicy-FIPS-2023-05"
```

```
    ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListServers

Muestra los servidores habilitados para el protocolo de transferencia de archivos que están asociados a su cuenta de AWS .

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

Especifica el número de servidores que se devolverán como respuesta a la consulta `ListServers`.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Cuando se obtienen resultados adicionales del comando `ListServers`, se devuelve un parámetro `NextToken` en la salida. A continuación, puede pasar el parámetro `NextToken` en un comando posterior para seguir enumerando servidores adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "NextToken": "string",
   "Servers": [
      {
         "Arn": "string",
         "Domain": "string",
         "EndpointType": "string",
         "IdentityProviderType": "string",
         "LoggingRole": "string",
         "ServerId": "string",
         "State": "string",
         "UserCount": number
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Cuando pueda obtener resultados adicionales de la operación `ListServers`, se devolverá un parámetro `NextToken` en la salida. En el siguiente comando, puede pasar el parámetro `NextToken` para seguir enumerando servidores adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Servers

Conjunto de servidores que estaban en la lista.

Tipo: matriz de objetos ListedServer

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

El siguiente ejemplo muestra los servidores que existen en su Cuenta de AWS.

Tenga en cuenta que los valores `NextToken` del ejemplo no son reales: están pensados para indicar cómo utilizar el parámetro.

Solicitud de muestra

```
{
   "MaxResults": 1,
   "NextToken": "token-from-previous-API-call"
}
```

Respuesta de ejemplo

```
{
   "NextToken": "another-token-to-continue-listing",
   "Servers": [
      {
         "Arn": "arn:aws:transfer:us-east-1:111112222222:server/s-01234567890abcdef",
         "Domain": "S3",
         "IdentityProviderType": "SERVICE_MANAGED",
         "EndpointType": "PUBLIC",
         "LoggingRole": "arn:aws:iam::111112222222:role/my-role",
         "ServerId": "s-01234567890abcdef",
         "State": "ONLINE",
         "UserCount": 3
      }
   ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListTagsForResource

Enumera todas las etiquetas asociadas con el nombre de recurso de Amazon (ARN) que especifique. El recurso puede ser un usuario, un servidor o un rol.

Sintaxis de la solicitud

```
{
   "Arn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Arn

Solicita las etiquetas asociadas con un nombre de recurso de Amazon (ARN) concreto. Un ARN es un identificador de un AWS recurso específico, como un servidor, un usuario o un rol.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

MaxResults

Especifica el número de etiquetas que se devolverán como respuesta a la solicitud `ListTagsForResource`.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Al solicitar resultados adicionales de la operación `ListTagsForResource`, se devuelve un parámetro `NextToken` en la entrada. A continuación, puede pasar un comando posterior al parámetro `NextToken` para seguir enumerando etiquetas adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "Arn": "string",
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Arn

El ARN que especificó para enumerar las etiquetas.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

NextToken

Cuando pueda obtener resultados adicionales de la llamada `ListTagsForResource`, se devolverá un parámetro `NextToken` en la salida. A continuación, puede pasar un comando posterior al parámetro `NextToken` para seguir enumerando etiquetas adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Tags

Pares clave-valor que se asignan a un recurso, normalmente con el fin de agrupar y buscar elementos. Las etiquetas son metadatos que usted puede definir.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

En el ejemplo siguiente, se enumeran las etiquetas del recurso con el ARN que especificó.

Solicitud de muestra

```
{
   "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef"
}
```

Ejemplo

Este ejemplo ilustra un uso de ListTagsForResource.

Respuesta de ejemplo

```
{
   "Tags": [
      {
         "Key": "Name",
         "Value": "MyServer"
      }
   ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2

- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListUsers

Muestra los usuarios de un servidor habilitado para el protocolo de File Transfer que especifique pasando el parámetro `ServerId`.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

Especifica el número de usuarios que se devolverán como respuesta a la solicitud `ListUsers`.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

Si hay resultados adicionales de la llamada `ListUsers`, se devuelve un parámetro `NextToken` en la salida. A continuación, puede pasar el `NextToken` a un comando `ListUsers` posterior para continuar con la lista de usuarios adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

ServerId

Identificador único asignado por el sistema para un servidor que tiene usuarios asignados.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "NextToken": "string",
   "ServerId": "string",
   "Users": [
      {
         "Arn": "string",
         "HomeDirectory": "string",
         "HomeDirectoryType": "string",
         "Role": "string",
         "SshPublicKeyCount": number,
         "UserName": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Cuando pueda obtener resultados adicionales de la llamada `ListUsers`, se devolverá un parámetro `NextToken` en la salida. A continuación, puede pasar un comando posterior al parámetro `NextToken` para seguir enumerando los usuarios adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

ServerId

Identificador único asignado por el sistema para un servidor al que están asignados los usuarios.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Users

Devuelve los usuarios de Transfer Family y sus propiedades para el valor `ServerId` que especifique.

Tipo: matriz de objetos ListedUser

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

La llamada a la API `ListUsers` devuelve una lista de usuarios asociados al servidor que especifique.

Solicitud de muestra

```
        {
         "MaxResults": 100,
         "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b1X0cnVuU2F0ZV9hbW91bnQiOiAyfQ==",
         "ServerId": "s-01234567890abcdef"
         }
```

Ejemplo

Este es un ejemplo de respuesta para esta llamada a la API.

Respuesta de ejemplo

```
{
   "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b1X0cnVuU2F0ZV9hbW91bnQiOiAyfQ==",
   "ServerId": "s-01234567890abcdef",
   "Users": [
      {
         "Arn": "arn:aws:transfer:us-east-1:176354371281:user/s-01234567890abcdef/
charlie",
         "HomeDirectory": "/tests/home/charlie",
         "SshPublicKeyCount": 1,
         "Role": "arn:aws:iam::176354371281:role/transfer-role1",
         "Tags": [
            {
```

```
                "Key": "Name",
                "Value": "user1"
            }
         ],
         "UserName": "my_user"
      }
   ]
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListWorkflows

Muestra todos los flujos de trabajo asociados Cuenta de AWS a su región actual.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

Especifica el número máximo de registros que se van a devolver.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1000.

Obligatorio: no

NextToken

`ListWorkflows` devuelve el parámetro `NextToken` en la salida. A continuación, puede pasar el parámetro `NextToken` en un comando posterior para seguir enumerando los flujos de trabajo adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
{
```

```
   "NextToken": "string",
   "Workflows": [
      {
         "Arn": "string",
         "Description": "string",
         "WorkflowId": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

`ListWorkflows` devuelve el parámetro `NextToken` en la salida. A continuación, puede pasar el parámetro `NextToken` en un comando posterior para seguir enumerando los flujos de trabajo adicionales.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 6144 caracteres.

Workflows

Devuelve `Arn`, `WorkflowId` y `Description` para cada flujo de trabajo.

Tipo: matriz de objetos ListedWorkflow

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidNextTokenException

El parámetro `NextToken` que se pasó no es válido.

Código de estado HTTP: 400

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

SendWorkflowStepState

Envía una devolución de llamada para pasos personalizados asíncronos.

`ExecutionId`, `WorkflowId` y `Token` se transfieren al recurso de destino durante la ejecución de un paso personalizado de un flujo de trabajo. Debe incluirlos en la devolución de llamada, así como proporcionar un estado.

Sintaxis de la solicitud

```
{
   "ExecutionId": "string",
   "Status": "string",
   "Token": "string",
   "WorkflowId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ExecutionId

Un identificador único para la ejecución del flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 36.

Patrón: `[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

Obligatorio: sí

Status

Indica si el paso especificado se realizó o no correctamente.

Tipo: cadena

Valores válidos: `SUCCESS | FAILURE`

Obligatorio: sí

Token

Se utiliza para distinguir entre diferentes devoluciones de llamada para varios pasos de Lambda dentro de la misma ejecución.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 64.

Patrón: `\w+`

Obligatorio: sí

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

StartDirectoryListing

Recupera una lista del contenido de un directorio de un servidor SFTP remoto. Debe especificar el ID del conector, la ruta de salida y la ruta del directorio remoto. También puede especificar el `MaxItems` valor opcional para controlar el número máximo de elementos que se enumeran en el directorio remoto. Esta API devuelve una lista de todos los archivos y directorios del directorio remoto (hasta el valor máximo), pero no devuelve los archivos o carpetas de los subdirectorios. Es decir, solo devuelve una lista de archivos y directorios de un nivel de profundidad.

Tras recibir el archivo del listado, puede proporcionar los archivos que desee transferir al `RetrieveFilePaths` parámetro de la llamada a la `StartFileTransfer` API.

La convención de nomenclatura del archivo de salida es *`connector-ID-listing-ID`*`.json`. El archivo de salida 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 formato de hora 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 10 000 elementos).

Sintaxis de la solicitud

```
{
   "ConnectorId": "string",
   "MaxItems": number,
   "OutputDirectoryPath": "string",
   "RemoteDirectoryPath": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ConnectorId

Un identificador único para el conector.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Obligatorio: sí

MaxItems

Un parámetro opcional en el que puede especificar el número máximo de nombres de archivos/directorios que se van a recuperar. El valor predeterminado es 1,000.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 10000.

Obligatorio: no

OutputDirectoryPath

Especifica la ruta (bucket y prefijo) en el almacenamiento de Amazon S3 para almacenar los resultados de la lista de directorios.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1024 caracteres.

Patrón: `(.)+`

Obligatorio: sí

RemoteDirectoryPath

Especifica el directorio del servidor SFTP remoto cuyo contenido desea enumerar.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1024 caracteres.

Patrón: `(.)+`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ListingId": "string",
   "OutputFileName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ListingId

Devuelve un identificador único para la llamada a la lista de directorios.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es 512.

Patrón: `[0-9a-zA-Z./-]+`

OutputFileName

Devuelve el nombre del archivo en el que se almacenan los resultados. Esta es una combinación del ID del conector y el ID del listado:`<connector-id>-<listing-id>.json`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 26. Longitud máxima de 537.

Patrón: `c-([0-9a-f]{17})-[0-9a-zA-Z./-]+.json`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo, se muestra el contenido de la `home` carpeta del servidor SFTP remoto, que se identifica mediante el conector especificado. Los resultados se colocan en la ubicación `/DOC-EXAMPLE-BUCKET/connector-files` de Amazon S3 y en un archivo denominado`doc-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json`.

Solicitud de muestra

```
{
    "ConnectorId": "c-AAAA1111BBBB2222C",
    "MaxItems": "10",
    "OutputDirectoryPath": "/DOC-EXAMPLE-BUCKET/connector-files",
    "RemoteDirectoryPath": "/home"
}
```

Respuesta de ejemplo

```
{
    "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",
    "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"
}
```

```
// under bucket "DOC-EXAMPLE-BUCKET"
connector-files/c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json
{
    "files": [
        {
            "filePath": "/home/what.txt",
            "modifiedTimestamp": "2024-01-30T20:34:54Z",
            "size" : 2323
        },
        {
            "filePath": "/home/how.pgp",
            "modifiedTimestamp": "2024-01-30T20:34:54Z",
            "size" : 51238
        }
    ],
    "paths": [
        {
            "path": "/home/magic"
        },
        {
            "path": "/home/aws"
        },
    ],
    "truncated": false
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

StartFileTransfer

Inicia una transferencia de archivos entre el AWS almacenamiento local y un servidor AS2 o SFTP remoto.

- En el caso de un conector AS2, debe especificar el `ConnectorId` y uno o varios `SendFilePaths` para identificar los archivos que desea transferir.
- En el caso de conector SFTP, la transferencia de archivos puede ser entrante o saliente. En ambos casos, debe especificar el `ConnectorId`. Según la dirección de la transferencia, también se especifican los elementos siguientes:
  - Si va a transferir un archivo desde el servidor SFTP de un socio al almacenamiento de Amazon Web Services, debe especificar un `RetrieveFilePaths` o más para identificar los archivos que desea transferir y un `LocalDirectoryPath` para especificar la carpeta de destino.
  - Si va a transferir un archivo desde el almacenamiento AWS al servidor SFTP de un socio, debe especificar un `SendFilePaths` o más para identificar los archivos que desea transferir y un `RemoteDirectoryPath` para especificar la carpeta de destino.

Sintaxis de la solicitud

```
{
   "ConnectorId": "string",
   "LocalDirectoryPath": "string",
   "RemoteDirectoryPath": "string",
   "RetrieveFilePaths": [ "string" ],
   "SendFilePaths": [ "string" ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ConnectorId

Un identificador único para el conector.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Obligatorio: sí

LocalDirectoryPath

En el caso de una transferencia entrante, `LocaDirectoryPath` especifica el destino de uno o más archivos que se transfieren desde el servidor SFTP del socio.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1024 caracteres.

Patrón: `(.)+`

Obligatorio: no

RemoteDirectoryPath

En el caso de una transferencia saliente, `RemoteDirectoryPath` especifica el destino de un archivo o más que se transfieren al servidor SFTP del asociado. Si no especifica un `RemoteDirectoryPath`, el destino de los archivos transferidos es el directorio de inicio del usuario de SFTP.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1024 caracteres.

Patrón: `(.)+`

Obligatorio: no

RetrieveFilePaths

Una o más rutas de origen para el servidor SFTP del asociado. Cada cadena representa la ruta del archivo de origen para una transferencia de archivos entrante.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1024 caracteres.

Patrón: `(.)+`

Obligatorio: no

SendFilePaths

Una o más rutas de origen para el almacenamiento de Amazon S3. Cada cadena representa la ruta del archivo de origen para una transferencia de archivos saliente. Por ejemplo, *DOC-EXAMPLE-BUCKET/myfile.txt* .

> **Note**
>
> Sustituya *DOC-EXAMPLE-BUCKET* por uno de sus depósitos reales.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1024 caracteres.

Patrón: `(.)+`

Obligatorio: no

Sintaxis de la respuesta

```
{
   "TransferId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

TransferId

Devuelve el identificador único de una transferencia de archivos.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es 512.

Patrón: `[0-9a-zA-Z./-]+`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

El ejemplo siguiente inicia un AS2 file transfer desde un servidor de Transfer Family al punto de conexión de un socio comercial remoto. Sustituya *`DOC-EXAMPLE-BUCKET`* por uno de sus depósitos reales.

Solicitud de muestra

```
{
    "ConnectorId": "c-AAAA1111BBBB2222C",
    "SendFilePaths": [
        "/DOC-EXAMPLE-BUCKET/myfile-1.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-2.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-3.txt"
    ]
}
```

Respuesta de ejemplo

```
{
   "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Ejemplo

El siguiente ejemplo inicia una transferencia de archivos desde el AWS almacenamiento local a un servidor SFTP remoto.

Solicitud de muestra

```
{
    "ConnectorId": "c-01234567890abcdef",
    "SendFilePaths": [
        "/DOC-EXAMPLE-BUCKET/myfile-1.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-2.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-3.txt"
    ],
    "RemoteDirectoryPath": "/MySFTPRootFolder/fromTranferFamilyServer"
}
```

Respuesta de ejemplo

```
{
   "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
}
```

Ejemplo

El ejemplo siguiente inicia una transferencia de archivos desde un servidor SFTP remoto al almacenamiento AWS local.

Solicitud de muestra

```
{
    "ConnectorId": "c-111122223333AAAAA",
    "RetrieveFilePaths": [
        "/MySFTPFolder/toTranferFamily/myfile-1.txt",
        "/MySFTPFolder/toTranferFamily/myfile-2.txt",
        "/MySFTPFolder/toTranferFamily/myfile-3.txt"
    ],
    "LocalDirectoryPath": "/DOC-EXAMPLE-BUCKET/mySourceFiles"
}
```

Respuesta de ejemplo

```
{
   "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

StartServer

Cambia el estado de un servidor habilitado para el protocolo de File Transfer de `OFFLINE` a `ONLINE`. No afecta a un servidor que ya esté `ONLINE`. Un servidor `ONLINE` puede aceptar y procesar trabajos de File Transfer.

El estado `STARTING` indica que el servidor se encuentra en un estado intermedio, es decir, que no puede responder completamente o que no está completamente conectado. Los valores de `START_FAILED` pueden indicar una condición de error.

No se devuelve ninguna respuesta de esta llamada.

Sintaxis de la solicitud

```
{
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ServerId

Identificador único asignado por parte del sistema para una instancia del servidor.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

El ejemplo siguiente crea un servidor.

Solicitud de muestra

```
{
   "ServerId": "s-01234567890abcdef"
```

```
}
```

Ejemplo

Este es un ejemplo de respuesta para esta llamada a la API.

Respuesta de ejemplo

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

StopServer

Cambia el estado de un servidor habilitado para el protocolo de File Transfer de `ONLINE` a `OFFLINE`. Un servidor `OFFLINE` no puede aceptar ni procesar trabajos de File Transfer. La información vinculada a su servidor, así como las propiedades del servidor y del usuario, no se ven afectadas por la detención del servidor.

> **Note**
>
> Detener el servidor no reduce ni afecta a la facturación de los puntos de conexión del protocolo de File Transfer: debe eliminar el servidor para dejar de facturarse.

El estado de `STOPPING` indica que el servidor se encuentra en un estado intermedio; es decir, que no puede responder por completo o que no está completamente desconectado. Los valores de `STOP_FAILED` pueden indicar una condición de error.

No se devuelve ninguna respuesta de esta llamada.

Sintaxis de la solicitud

```
{
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ServerId

Identificador único asignado por el sistema para un servidor que haya detenido.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

El siguiente detiene el servicio.

Solicitud de muestra

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Ejemplo

Este es un ejemplo de respuesta para esta llamada a la API.

Respuesta de ejemplo

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

TagResource

Adjunta un par clave-valor a un recurso, identificado por su nombre de recurso de Amazon (ARN). Los recursos son usuarios, servidores, roles y otras entidades.

No se ha obtenido ninguna respuesta de esta llamada.

Sintaxis de la solicitud

```
{
   "Arn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Arn

Un nombre de recurso de Amazon (ARN) para un AWS recurso específico, como un servidor, un usuario o un rol.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

Tags

Pares clave-valor asignados a ARN que se pueden utilizar para agrupar y buscar recursos por tipo. Puede adjuntar estos metadatos a los recursos (servidores, usuarios, flujos de trabajo, etc.) para cualquier propósito.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

En el siguiente ejemplo, se agrega una etiqueta a un servidor con el protocolo de transferencia de archivos habilitado.

Solicitud de muestra

```
{
   "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
   "Tags": [
      {
         "Key": "Group",
         "Value": "Europe"
      }
   ]
}
```

Ejemplo

Este ejemplo ilustra un uso de TagResource.

Respuesta de ejemplo

```
         HTTP 200 response with an empty HTTP body.
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2

- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

TestConnection

Comprueba si el conector SFTP está configurado correctamente. Le recomendamos encarecidamente que realice esta operación para probar su capacidad de transferir archivos entre el AWS almacenamiento local y el servidor SFTP de un socio comercial.

Sintaxis de la solicitud

```
{
   "ConnectorId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ConnectorId

Un identificador único para el conector.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ConnectorId": "string",
   "Status": "string",
   "StatusMessage": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ConnectorId

Devuelve el identificador del objeto conector que está probando.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Status

Devuelve `OK` la prueba se ha realizado correctamente o `ERROR` si la prueba no ha sido satisfactoria.

Tipo: cadena

StatusMessage

Devuelve `Connection succeeded` si la actualización se realiza correctamente. O bien, devuelve un mensaje de error descriptivo si la prueba no es satisfactoria. En la siguiente lista se proporcionan detalles sobre la solución de problemas, en función del mensaje de error que reciba.

- Compruebe que su nombre secreto coincide con el de los permisos de Transfer Role.
- Compruebe la URL del servidor en la configuración del conector y compruebe que las credenciales de inicio de sesión funcionan correctamente fuera del conector.
- Compruebe que el secreto existe y que tiene el formato correcto.
- Compruebe que la clave de host de confianza de la configuración del conector coincide con la salida de `ssh-keyscan`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

El siguiente ejemplo prueba la conexión a un servidor remoto.

```
aws transfer test-connection --connector-id c-abcd1234567890fff
```

Respuesta de ejemplo

Si se realiza correctamente, la llamada a la API devuelve los siguientes detalles.

```
{

    "Status": "OK",

    "StatusMessage": "Connection succeeded"

}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

TestIdentityProvider

Si el `IdentityProviderType` de un servidor con protocolo de transferencia de archivos habilitado es `AWS_DIRECTORY_SERVICE` o `API_Gateway`, comprueba si su proveedor de identidad está configurado correctamente. Le recomendamos que inicie esta operación para comprobar su método de autenticación tan pronto como cree el servidor. De este modo, puede solucionar problemas relacionados con la integración del proveedor de identidades para garantizar que sus usuarios puedan utilizar el servicio correctamente.

Los parámetros `ServerId` y `UserName` son obligatorios. Los `ServerProtocol`, `SourceIp` y `UserPassword` son todos opcionales.

Tenga en cuenta lo siguiente:

- No puede usar `TestIdentityProvider` si el `IdentityProviderType` de su servidor es `SERVICE_MANAGED`.
- `TestIdentityProvider` no funciona con claves: solo acepta contraseñas.
- `TestIdentityProvider` puede probar el funcionamiento de la contraseña para un proveedor de identidad personalizado que gestione las claves y las contraseñas.
- Si proporciona valores incorrectos para algún parámetro, el campo `Response` estará vacío.
- Si proporciona un identificador de servidor para un servidor que utiliza usuarios administrados por el servicio, aparecerá un error:

  `An error occurred (InvalidRequestException) when calling the TestIdentityProvider operation: s-`*`server-ID`*` not configured for external auth`
- Si introduce una ID de servidor para el parámetro `--server-id` que no identifica a un servidor de transferencia real, recibirá el siguiente error:

  `An error occurred (ResourceNotFoundException) when calling the TestIdentityProvider operation: Unknown server`.

  Es posible que su servidor se encuentre en una región diferente. Puede especificar una región añadiendo lo siguiente: `--region region-code`, por ejemplo, `--region us-east-2` para especificar un servidor en Este de EE. UU. (Ohio).

Sintaxis de la solicitud

```
{
   "ServerId": "string",
   "ServerProtocol": "string",
   "SourceIp": "string",
   "UserName": "string",
   "UserPassword": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ServerId

Identificador asignado por el sistema para un servidor específico. El método de autenticación de usuarios de ese servidor se prueba con un nombre de usuario y contraseña.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

ServerProtocol

El tipo de protocolo de transferencia de archivos que se probará.

Los protocolos disponibles son:

- Protocolo de File Transfer (SFTP) Secure Shell (SSH)
- Protocolo seguro de File Transfer (FTPS)
- Protocolo de File Transfer (FTP)
- Declaración de aplicabilidad 2 (AS2)

Tipo: cadena

Valores válidos: `SFTP | FTP | FTPS | AS2`

Obligatorio: no

SourceIp

La dirección IP de origen de la cuenta que será comprobada.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 32 caracteres.

Patrón: `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`

Obligatorio: no

UserName

El nombre de la cuenta que será comprobada.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: sí

UserPassword

La contraseña de la cuenta que se probará.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es 1024.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "Message": "string",
   "Response": "string",
```

```
    "StatusCode": number,
    "Url": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Message

Un mensaje que indica si la prueba se ha realizado correctamente o no.

> **Note**
>
> Si se devuelve una cadena vacía, lo más probable es que la autenticación haya fallado debido a un nombre de usuario o contraseña incorrectos.

Tipo: cadena

Response

La respuesta que devuelve su puerta de enlace API o su función de Lambda.

Tipo: cadena

StatusCode

El código de estado HTTP que es la respuesta de su puerta de enlace API o de su función de Lambda.

Tipo: entero

Url

El punto de conexión del servicio utilizado para autenticar a un usuario.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 255 caracteres.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

La siguiente solicitud devuelve un mensaje de un proveedor de identidad en el que se indica que una combinación de nombre de usuario y contraseña es una identidad válida para utilizarla AWS Transfer Family.

Solicitud de muestra

```
{
   "ServerID": "s-01234567890abcdef",
   "UserName": "my_user",
   "UserPassword": "MyPassword-1"
}
```

Ejemplo

La siguiente respuesta muestra un ejemplo de respuesta para una prueba satisfactoria.

Respuesta de ejemplo

```
      "Response":"
      {\"homeDirectory\":\"/mybucket001\",\"homeDirectoryDetails\":null,
\"homeDirectoryType\":\"PATH\",\"posixProfile\":null,
      \"publicKeys\":\"[ssh-rsa-key]\",\"role\":\"arn:aws:iam::123456789012:role/
my_role\",\"policy\":null,\"username\":\"transferuser002\",
      \"identityProviderType\":null,\"userConfigMessage\":null)"}
      "StatusCode": "200",
      "Message": ""
```

Ejemplo

La siguiente respuesta indica que el usuario especificado pertenece a más de un grupo al que tiene acceso.

```
         "Response":"",
         "StatusCode":200,
         "Message":"More than one associated access found for user's groups."
```

Ejemplo

Si ha creado y configurado un proveedor de identidad personalizado mediante una puerta de enlace API, puede introducir el siguiente comando para probar su usuario:

`aws transfer test-identity-provider --server-id` *`s-0123456789abcdefg`* `--user-name` *`myuser`*

donde s-0123456789abcdefg sea su servidor de transferencias y myuser, el nombre de usuario de su usuario personalizado.

Si el comando se ejecuta correctamente, la respuesta será similar a la siguiente, donde:

- Cuenta de AWS El ID es 012345678901

- El rol de usuario es user-role-api-gateway
- El directorio de inicio es myuser-bucket
- La clave pública es public-key
- La URL de invocación es invocation-URL

```
{
    "Response": "{\"Role\": \"arn:aws:iam::012345678901:role/user-role-api-gateway\",
\"HomeDirectory\": \"/myuser-bucket\",\"PublicKeys\": \"[public-key]\"}",
    "StatusCode": 200,
    "Message": "",
    "Url": "https://invocation-URL/servers/s-0123456789abcdefg/users/myuser/config"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los SDK específicos del idioma AWS , consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UntagResource

Separa un par clave-valor de un recurso, identificado por su nombre de recurso de Amazon (ARN). Los recursos son usuarios, servidores, roles y otras entidades.

No se devuelve ninguna respuesta de esta llamada.

Sintaxis de la solicitud

```
{
   "Arn": "string",
   "TagKeys": [ "string" ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Arn

El valor del recurso al que se le eliminará la etiqueta. Un nombre de recurso de Amazon (ARN) es un identificador de un AWS recurso específico, como un servidor, un usuario o un rol.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

TagKeys

TagKeys son pares clave-valor asignados a los ARN que se pueden usar para agrupar y buscar recursos por tipo. Estos metadatos se pueden adjuntar a los recursos para cualquier propósito.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 128 caracteres.

Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el servicio. AWS Transfer Family

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

Ejemplos

Ejemplo

En el siguiente ejemplo, se elimina una etiqueta de un servidor con el protocolo de transferencia de archivos habilitado.

Solicitud de muestra

```
{
   "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
   "TagKeys": "Europe" ]
}
```

Ejemplo

Este ejemplo ilustra un uso de UntagResource.

Respuesta de ejemplo

```
        HTTP 200 response with an empty HTTP body.
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateAccess

Permite actualizar los parámetros del acceso especificado en los parámetros `ServerID` y `ExternalID`.

Sintaxis de la solicitud

```
{
   "ExternalId": "string",
   "HomeDirectory": "string",
   "HomeDirectoryMappings": [
      {
         "Entry": "string",
         "Target": "string",
         "Type": "string"
      }
   ],
   "HomeDirectoryType": "string",
   "Policy": "string",
   "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "Role": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ExternalId

Un identificador único que se requiere para identificar grupos específicos dentro de su directorio. Los usuarios del grupo que asocie tienen acceso a sus recursos de Amazon S3 o Amazon EFS a través de los protocolos habilitados que utilizan AWS Transfer Family. Si conoce el nombre del grupo, puede ver los valores del SID ejecutando el siguiente comando en Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

En ese comando, YourGroupNamesustitúyalo por el nombre del grupo de Active Directory.

La expresión regular utilizada para validar este parámetro es una cadena de caracteres compuesta de caracteres alfanuméricos en mayúscula y minúscula, sin espacios. También puede incluir guiones bajos y cualquiera de los siguientes caracteres: =,.@:/-

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `S-1-[\d-]+`

Obligatorio: sí

HomeDirectory

Directorio de destino (carpeta) de un usuario cuando inicia sesión en el servidor a través del cliente.

Un ejemplo de `HomeDirectory` es `/bucket_name/home/mydirectory`.

> **Note**
>
> El parámetro `HomeDirectory` solo se utiliza si `HomeDirectoryType` está establecido en `PATH`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

HomeDirectoryMappings

Los mapeos de directorio lógico que especifican qué rutas de acceso y claves de Amazon S3 o Amazon EFS 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. Si solo especifica un destino, se muestra tal cual. También debe asegurarse de que su función AWS Identity and Access Management (de IAM) proporcione acceso a las rutas de entrada. `Target` Este valor solo se puede establecer si `HomeDirectoryType` está establecido en LOGICAL.

Lo siguiente es un ejemplo del par `Entry` y `Target`.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

En la mayoría de los casos, puede utilizar este valor en lugar de la política de sesión para limitar al usuario al directorio de inicio designado ("`chroot`"). Para ello, puede establecer `Entry` en `/`, y `Target` al valor del parámetro `HomeDirectory`.

A continuación, se muestra un ejemplo del par `Entry` y `Target` para `chroot`.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Tipo: Matriz de HomeDirectoryMapEntry objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50000 artículos.

Obligatorio: no

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 la ruta absoluta 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 `HomeDirectoryMappings` que correspondan con la forma en que quiere que las rutas de acceso de Amazon S3 o de Amazon EFS sean visibles para sus usuarios.

> **Note**
>
> Si `HomeDirectoryType` es `LOGICAL`, debe proporcionar las asignaciones mediante el parámetro `HomeDirectoryMappings`. Si, por el contrario, `HomeDirectoryType` es `PATH`, se proporciona una ruta absoluta mediante el parámetro `HomeDirectory`. No puede tener `HomeDirectory` y `HomeDirectoryMappings` en su plantilla.

Tipo: cadena

Valores válidos: `PATH | LOGICAL`

Obligatorio: no

Policy

Una política de sesión para su usuario, de modo que pueda usar el mismo rol AWS Identity and Access Management (IAM) en varios usuarios. Esta política reduce el ámbito de acceso de un usuario a partes de su bucket de Amazon S3. Entre las variables que puede utilizar dentro de esta política se incluyen `${Transfer:UserName}`, `${Transfer:HomeDirectory}` y `${Transfer:HomeBucket}`.

> **Note**
>
> Esta política se aplica solo cuando el dominio de `ServerId` es Amazon S3. Amazon EFS no utiliza políticas de sesión.
>
> En el caso de las políticas de sesión, AWS Transfer Family almacena la política como un blob de JSON, en lugar del nombre de recurso de Amazon (ARN) de la política. Puede guardar la política como un blob JSON y pasarlo en el argumento `Policy`.
>
> Para ver un ejemplo de una política de sesión, consulte Example session policy (Ejemplo de política de sesión).
>
> Para obtener más información, consulte la AssumeRolereferencia de la API AWS de Security Token Service.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: no

PosixProfile

La identidad POSIX completa, incluido el ID de usuario (`Uid`), el ID de grupo (`Gid`) y cualquier ID de grupo secundario (`SecondaryGids`) 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.

Tipo: objeto PosixProfile

Obligatorio: no

Role

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que controla el acceso de los usuarios al bucket de Amazon S3 o al sistema de archivos Amazon 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.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

ServerId

Identificador único asignado por el sistema para una instancia del servidor. Este es el servidor específico al que ha agregado el usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ExternalId

El identificador externo del grupo cuyos usuarios tienen acceso a sus recursos de Amazon S3 o Amazon EFS a través de los protocolos habilitados mediante AWS Transfer Family.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `S-1-[\d-]+`

ServerId

El ID del servidor al que se asocia el usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateAgreement

Actualiza algunos de los parámetros de un acuerdo existente. Proporcione los valores `AgreementId` y `ServerId` del acuerdo que desee actualizar, junto con los nuevos valores de los parámetros que desee actualizar.

Sintaxis de la solicitud

```
{
   "AccessRole": "string",
   "AgreementId": "string",
   "BaseDirectory": "string",
   "Description": "string",
   "LocalProfileId": "string",
   "PartnerProfileId": "string",
   "ServerId": "string",
   "Status": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

AccessRole

Los conectores se utilizan para enviar archivos mediante el protocolo AS2 o SFTP. Para la función de acceso, proporcione el nombre de recurso de Amazon (ARN) de la AWS Identity and Access Management función que se va a utilizar.

Para conectores AS2

Con AS2, puede enviar archivos llamando a `StartFileTransfer` y especificando las rutas de los archivos en el parámetro de solicitud, `SendFilePaths`. Utilizamos el directorio principal del archivo (por ejemplo, para `--send-file-paths /bucket/dir/file.txt`, el directorio principal es `/bucket/dir/`) para almacenar temporalmente un archivo de mensajes AS2 procesado, almacenar el MDN cuando lo recibimos del socio y escribir un archivo JSON final que contenga los metadatos relevantes de la transmisión. Por lo tanto, `AccessRole` debe

proporcionar acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`. Además, debe proporcionar acceso de lectura y escritura al directorio principal de los archivos que desea enviar con `StartFileTransfer`.

Si utiliza la autenticación básica para el conector AS2, el rol de acceso requiere el permiso `secretsmanager:GetSecretValue` para el secreto. Si el secreto se cifra con una clave gestionada por el cliente en lugar de la clave AWS gestionada en Secrets Manager, el rol también necesitará el `kms:Decrypt` permiso para esa clave.

Para conectores SFTP

Asegúrese de que el acceso al 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 otorgue `secretsmanager:GetSecretValue` permiso a. AWS Secrets Manager

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

AgreementId

Un identificador único para el acuerdo. Este identificador se devuelve al crear un acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `a-([0-9a-f]{17})`

Obligatorio: sí

BaseDirectory

Para cambiar el directorio de destino (carpeta) de los archivos que se transfieren, proporcione la carpeta de bucket que desee usar, por ejemplo, */DOC-EXAMPLE-BUCKET/home/mydirectory* .

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

Description

Para reemplazar la descripción existente, proporcione una descripción breve del acuerdo.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Graph}]+`

Obligatorio: no

LocalProfileId

Un identificador único para el perfil local de AS2.

Para cambiar el identificador del perfil local, introduzca aquí un nuevo valor.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

PartnerProfileId

Un identificador único para el perfil de socio. Para cambiar el identificador del perfil del socio, introduzca aquí un nuevo valor.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

ServerId

Identificador único asignado por el sistema para una instancia del servidor. Este identificador indica el servidor específico que utiliza el acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Status

Puede actualizar el estado del acuerdo, ya sea activando un acuerdo inactivo o al revés.

Tipo: cadena

Valores válidos: `ACTIVE | INACTIVE`

Obligatorio: no

Sintaxis de la respuesta

```
{
   "AgreementId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AgreementId

Un identificador único para el acuerdo. Este identificador se devuelve al crear un acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `a-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateCertificate

Actualiza las fechas activas e inactivas de un certificado.

Sintaxis de la solicitud

```
{
   "ActiveDate": number,
   "CertificateId": "string",
   "Description": "string",
   "InactiveDate": number
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ActiveDate

Una fecha opcional que especifica cuándo se activa el certificado.

Tipo: marca temporal

Obligatorio: no

CertificateId

El identificador del objeto de certificado que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Obligatorio: sí

Description

Una descripción breve para ayudar a identificar el certificado.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Graph}]+`

Obligatorio: no

InactiveDate

Una fecha opcional que especifica cuándo el certificado pasa a estar inactivo.

Tipo: marca temporal

Obligatorio: no

Sintaxis de la respuesta

```
{
   "CertificateId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CertificateId

Devuelve el identificador del objeto de certificado que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo, se actualiza la fecha de activación de un certificado y se establece en el 16 de enero de 2022 a las 16:12:07 UTC -5 horas.

Solicitud de muestra

```
aws transfer update-certificate --certificate-id c-abcdefg123456hijk --active-date
 2022-01-16T16:12:07-05:00
```

Ejemplo

A continuación se muestra un ejemplo de respuesta para esta llamada a la API .

Respuesta de ejemplo

```
"CertificateId": "c-abcdefg123456hijk"
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateConnector

Actualiza algunos de los parámetros de un conector existente. Proporcione el valor `ConnectorId` del conector que desee actualizar, junto con los nuevos valores de los parámetros que desee actualizar.

Sintaxis de la solicitud

```
{
   "AccessRole": "string",
   "As2Config": {
      "BasicAuthSecretId": "string",
      "Compression": "string",
      "EncryptionAlgorithm": "string",
      "LocalProfileId": "string",
      "MdnResponse": "string",
      "MdnSigningAlgorithm": "string",
      "MessageSubject": "string",
      "PartnerProfileId": "string",
      "SigningAlgorithm": "string"
   },
   "ConnectorId": "string",
   "LoggingRole": "string",
   "SecurityPolicyName": "string",
   "SftpConfig": {
      "TrustedHostKeys": [ "string" ],
      "UserSecretId": "string"
   },
   "Url": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

AccessRole

Los conectores se utilizan para enviar archivos mediante el protocolo AS2 o SFTP. Para la función de acceso, proporcione el nombre de recurso de Amazon (ARN) de la AWS Identity and Access Management función que se va a utilizar.

Para conectores AS2

Con AS2, puede enviar archivos llamando a `StartFileTransfer` y especificando las rutas de los archivos en el parámetro de solicitud, `SendFilePaths`. Utilizamos el directorio principal del archivo (por ejemplo, para `--send-file-paths /bucket/dir/file.txt`, el directorio principal es `/bucket/dir/`) para almacenar temporalmente un archivo de mensajes AS2 procesado, almacenar el MDN cuando lo recibimos del socio y escribir un archivo JSON final que contenga los metadatos relevantes de la transmisión. Por lo tanto, `AccessRole` debe proporcionar acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`. Además, debe proporcionar acceso de lectura y escritura al directorio principal de los archivos que desea enviar con `StartFileTransfer`.

Si utiliza la autenticación básica para el conector AS2, el rol de acceso requiere el permiso `secretsmanager:GetSecretValue` para el secreto. Si el secreto se cifra con una clave gestionada por el cliente en lugar de la clave AWS gestionada en Secrets Manager, el rol también necesitará el `kms:Decrypt` permiso para esa clave.

Para conectores SFTP

Asegúrese de que el acceso al 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 otorgue `secretsmanager:GetSecretValue` permiso a. AWS Secrets Manager

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

As2Config

Una estructura que contiene los parámetros de un objeto de conexión AS2.

Tipo: objeto As2ConnectorConfig

Obligatorio: no

ConnectorId

Un identificador único para el conector.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Obligatorio: sí

LoggingRole

El nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que permite a un conector activar el CloudWatch registro de los eventos de Amazon S3. Cuando esté configurado, podrá ver la actividad del conector en sus CloudWatch registros.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

SecurityPolicyName

Especifica el nombre de la política de seguridad del conector.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 100 caracteres.

Patrón: `TransferSFTPConnectorSecurityPolicy-[A-Za-z0-9-]+`

Obligatorio: no

SftpConfig

Una estructura que contiene los parámetros de un objeto de conexión SFTP.

Tipo: objeto SftpConnectorConfig

Obligatorio: no

Url

La URL del punto de conexión de AS2 o SFTP del socio.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 255 caracteres.

Obligatorio: no

Sintaxis de la respuesta

```
{
   "ConnectorId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ConnectorId

Devuelve el identificador del objeto conector que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateHostKey

Actualiza la descripción de la clave de host especificada en los parámetros `ServerId` y `HostKeyId`.

Sintaxis de la solicitud

```
{
   "Description": "string",
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Description

Descripción actualizada de la clave de host.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Print}]*`

Obligatorio: sí

HostKeyId

El identificador de la clave de host que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud fija de 25.

Patrón: `hostkey-[0-9a-f]{17}`

Obligatorio: sí

ServerId

El identificador del servidor que contiene la clave de host que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HostKeyId

Devuelve el identificador de clave de host de la clave de host actualizada.

Tipo: cadena

Limitaciones de longitud: longitud fija de 25.

Patrón: `hostkey-[0-9a-f]{17}`

ServerId

Devuelve el identificador del servidor que contiene la clave de host actualizada.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateProfile

Actualiza algunos de los parámetros de un perfil existente. Proporcione el valor `ProfileId` del perfil que desee actualizar, junto con los nuevos valores de los parámetros que desee actualizar.

Sintaxis de la solicitud

```
{
   "CertificateIds": [ "string" ],
   "ProfileId": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

CertificateIds

Una matriz de identificadores de los certificados importados. Este identificador se utiliza para trabajar con perfiles y perfiles de socios.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Obligatorio: no

ProfileId

El identificador del objeto de perfil que está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ProfileId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ProfileId

Devuelve el identificador del perfil que se está actualizando.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateServer

Actualiza las propiedades del servidor habilitado para el protocolo de transferencia de archivos una vez creado el servidor.

La llamada `UpdateServer` devuelve las `ServerId` del servidor que ha actualizado.

Sintaxis de la solicitud

```
{
   "Certificate": "string",
   "EndpointDetails": {
      "AddressAllocationIds": [ "string" ],
      "SecurityGroupIds": [ "string" ],
      "SubnetIds": [ "string" ],
      "VpcEndpointId": "string",
      "VpcId": "string"
   },
   "EndpointType": "string",
   "HostKey": "string",
   "IdentityProviderDetails": {
      "DirectoryId": "string",
      "Function": "string",
      "InvocationRole": "string",
      "SftpAuthenticationMethods": "string",
      "Url": "string"
   },
   "LoggingRole": "string",
   "PostAuthenticationLoginBanner": "string",
   "PreAuthenticationLoginBanner": "string",
   "ProtocolDetails": {
      "As2Transports": [ "string" ],
      "PassiveIp": "string",
      "SetStatOption": "string",
      "TlsSessionResumptionMode": "string"
   },
   "Protocols": [ "string" ],
   "S3StorageOptions": {
      "DirectoryListingOptimization": "string"
   },
   "SecurityPolicyName": "string",
   "ServerId": "string",
   "StructuredLogDestinations": [ "string" ],
```

```
   "WorkflowDetails": {
      "OnPartialUpload": [
         {
            "ExecutionRole": "string",
            "WorkflowId": "string"
         }
      ],
      "OnUpload": [
         {
            "ExecutionRole": "string",
            "WorkflowId": "string"
         }
      ]
   }
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Certificate

El nombre de recurso de Amazon (ARN) del AWS certificado Certificate Manager (ACM). Necesario cuando `Protocols` se establece en `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 SSL/TLS X.509 versión 3 válido con FQDN o dirección IP especificada e información sobre el emisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1600 caracteres.

Obligatorio: no

EndpointDetails

Los ajustes del punto de conexión de la nube privada virtual (VPC) que está configurado para su servidor. Cuando aloja el punto de conexión dentro de la VPC, puede hacer que sea accesible solo para los recursos de la VPC, o puede adjuntar direcciones IP elásticas y hacer que sea accesible para los clientes a través de Internet. Los grupos de seguridad predeterminados de su VPC se asignan automáticamente a su punto de conexión.

Tipo: objeto EndpointDetails

Obligatorio: no

EndpointType

El tipo de punto de conexión que desea que use el servidor. Puede optar por hacer que el punto de conexión de su servidor sea de acceso público (PUBLIC) o alojarlo dentro de su VPC. Con un punto de conexión alojado en una VPC, puede restringir el acceso al servidor y a los recursos solo dentro de su VPC o elegir que esté orientado a Internet al adjuntarle direcciones IP elásticas directamente.

> **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 19 de mayo de 2021 o antes, no se verá afectado. Después de esta fecha, use `EndpointType=VPC`.
> Para obtener más información, consulte Suspender el uso de VPC_ENDPOINT.

Se recomienda que utilice `VPC` como `EndpointType`. Con este tipo de punto de conexión, tiene la opción de asociar directamente hasta tres direcciones IPv4 Elastic (IP BYO incluida) con el punto de conexión del servidor y utilizar grupos de seguridad de VPC para restringir el tráfico de la dirección IP pública del cliente. Esto no es posible si se establece `EndpointType` en `VPC_ENDPOINT`.

Tipo: cadena

Valores válidos: `PUBLIC | VPC | VPC_ENDPOINT`

Obligatorio: no

HostKey

La clave privada RSA, ECDSA o ED25519 que se utilizará en el servidor habilitado para SFTP. Puede agregar varias claves de host, en caso de que desee rotar las claves, o tener un conjunto de claves activas que utilicen algoritmos diferentes.

Use el siguiente comando para generar una clave RSA de 2048 bits sin contraseña:

`ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key`.

Utilice un valor mínimo de 2048 para la opción `-b`. Puede crear una clave más fuerte utilizando 3072 o 4096.

Utilice el siguiente comando para generar una clave ECDSA de 256 bits sin contraseña:

`ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key`.

Los valores válidos para la opción `-b` de ECDSA son 256, 384 y 521.

Utilice el siguiente comando para generar una clave ED25519 sin contraseña:

`ssh-keygen -t ed25519 -N "" -f my-new-server-key`.

Puedes reemplazar todos estos comandos por my-new-server-keyla cadena que prefieras.

Important

Si no planea migrar los usuarios existentes de un servidor compatible con SFTP a un servidor nuevo, no actualice la clave de host. El cambio accidental de la clave de host de un servidor puede ser disruptivo.

Para obtener más información, consulte Actualizar las claves de host de un servidor con SFTP en la AWS Transfer Family Guía del usuario.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 4096 caracteres.

Obligatorio: no

IdentityProviderDetails

Matriz que contiene toda la información necesaria para llamar al método de API de autenticación del cliente.

Tipo: objeto IdentityProviderDetails

Obligatorio: no

LoggingRole

El nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que permite a un servidor activar el CloudWatch registro de Amazon para Amazon S3 o Amazon EFSEvents. Cuando esté configurado, podrá ver la actividad de los usuarios en sus registros. CloudWatch

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Patrón: `(|arn:.*role/\S+)`

Obligatorio: no

PostAuthenticationLoginBanner

Especifica una cadena para que se muestre cuando los usuarios se conecten a un servidor. Esta cadena se muestra después de que el usuario se autentique.

> **Note**
>
> El protocolo SFTP no admite banners de visualización posteriores a la autenticación.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 4 096 caracteres.

Patrón: `[\x09-\x0D\x20-\x7E]*`

Obligatorio: no

PreAuthenticationLoginBanner

Especifica una cadena para que se muestre cuando los usuarios se conecten a un servidor. Esta cadena se muestra antes de que el usuario se autentique. Por ejemplo, el siguiente banner muestra detalles sobre el uso del sistema:

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 4 096 caracteres.

Patrón: `[\x09-\x0D\x20-\x7E]*`

Obligatorio: no

ProtocolDetails

La configuración de protocolo configurados para su servidor.

- Use el parámetro `PassiveIp` para indicar el modo pasivo (para los protocolos FTP y FTPS). Ingrese una sola dirección IPv4 de cuatro puntos, como la dirección IP externa de un firewall, un enrutador o un equilibrador de carga.
- Utilice el parámetro `SetStatOption` para ignorar el error que se genera cuando el cliente intenta usar el comando `SETSTAT` en un archivo que esté cargando en un bucket de Amazon S3. Para que el AWS Transfer Family servidor ignore el `SETSTAT` comando y cargue archivos sin necesidad de realizar ningún cambio en el cliente SFTP, defina `ENABLE_NO_OP` el valor en. Si estableces el `SetStatOption` parámetro en`ENABLE_NO_OP`, Transfer Family generará una entrada de registro en Amazon CloudWatch Logs para que puedas determinar cuándo el cliente está realizando una `SETSTAT` llamada.
- Para determinar si su AWS Transfer Family servidor reanuda las sesiones negociadas recientes mediante un identificador de sesión único, utilice el `TlsSessionResumptionMode` parámetro.

- `As2Transports` indica el método de transporte de los mensajes de AS2. Actualmente, solo se admite HTTP.

Tipo: objeto ProtocolDetails

Obligatorio: no

Protocols

Especifica el protocolo o los protocolos de File Transfer a través de los cuales el cliente de protocolo de File Transfer puede conectarse al punto de enlace del servidor. Los protocolos disponibles son:

- `SFTP` (Protocolo de File Transfer Secure Shell (SSH)): transferencia de archivos a través de SSH
- `FTPS` (Protocolo de File Transfer seguro): transferencia de archivos con cifrado TLS
- `FTP` (Protocolo de File Transfer): transferencia de archivos sin cifrar
- `AS2`(Declaración de aplicabilidad 2): se utiliza para transportar datos estructurados business-to-business

> **Note**
>
> - Si lo seleccionaFTPS, debe elegir un certificado almacenado en AWS Certificate Manager (ACM) que se utilice para identificar el servidor cuando los clientes se conecten a él a través de FTPS.
> - Si el `Protocol` incluye `FTP` o `FTPS`, el `EndpointType` debe ser `VPC` y el `IdentityProviderType` debe ser `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
> - Si `Protocol` incluye `FTP`, entonces `AddressAllocationIds` no se puede asociar.
> - Si el `Protocol` se establece solo en `SFTP`, se puede establecer el `EndpointType` como `PUBLIC` y el `IdentityProviderType` se puede configurar como cualquiera de los tipos de identidad admitidos: `SERVICE_MANAGED`, `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
> - Si `Protocol` incluye `AS2`, `EndpointType` debe ser `VPC` y el dominio debe ser Amazon S3.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Valores válidos: `SFTP | FTP | FTPS | AS2`

Obligatorio: no

S3StorageOptions

Especifica si el rendimiento de los directorios de Amazon S3 está optimizado o no. Esta opción está deshabilitada de forma predeterminada.

De forma predeterminada, las asignaciones de los directorios principales tienen un `TYPE` valor de. `DIRECTORY` Si habilita esta opción, tendrá que establecerla de forma explícita `FILE` si `HomeDirectoryMapEntry` `Type` desea que la asignación tenga un destino de archivo.

Tipo: objeto S3StorageOptions

Obligatorio: no

SecurityPolicyName

Especifica el nombre de la política de seguridad del servidor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 100 caracteres.

Patrón: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Obligatorio: no

ServerId

Identificador único asignado por el sistema para una instancia del servidor a la que está asignado el usuario de Transfer Family.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

StructuredLogDestinations

Especifica los grupos de registro a los que se envían los registros de su servidor.

Para especificar un grupo de registros, debe proporcionar el ARN de un grupo de registros existente. En este caso, el formato del grupo de registros es el siguiente:

`arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*`

Por ejemplo, `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

Si ha especificado previamente un grupo de registros para un servidor, puede borrarlo y desactivar el registro estructurado proporcionando un valor vacío para este parámetro en una llamada `update-server`. Por ejemplo:

```
update-server --server-id s-1234567890abcdef0 --structured-log-
destinations
```

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: no

WorkflowDetails

Especifica el ID del flujo de trabajo que se va a asignar y el rol de ejecución que se utiliza para ejecutar el flujo de trabajo.

Además de un flujo de trabajo que se ejecuta cuando un archivo se carga por completo, `WorkflowDetails` también puede contener un ID de flujo de trabajo (y un rol de ejecución) para que un flujo de trabajo se ejecute en una carga parcial. Se produce una carga parcial si la sesión de servidor se desconecta mientras se está cargando el archivo.

Para eliminar un flujo de trabajo asociado de un servidor, puede proporcionar un objeto `OnUpload` vacío, tal y como se muestra en el siguiente ejemplo.

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-
details '{"OnUpload":[]}'
```

Tipo: objeto WorkflowDetails

Obligatorio: no

Sintaxis de la respuesta

```
{
   "ServerId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ServerId

Identificador único asignado por el sistema para un servidor al que está asignado el usuario de Transfer Family.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

ConflictException

Esta excepción se produce cuando `UpdateServer` se llama a un servidor habilitado para el protocolo de transferencia de archivos que tiene VPC como tipo de punto de conexión y el `VpcEndpointID` del servidor no está en el estado disponible.

Código de estado HTTP: 400

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceExistsException

El recurso solicitado no existe o existe en una región distinta de la especificada para el comando.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo actualiza el rol de un servidor.

Solicitud de muestra

```
{
```

```
   "EndpointDetails": {
   "VpcEndpointId": "vpce-01234f056f3g13",
   "LoggingRole": "CloudWatchS3Events",
   "ServerId": "s-01234567890abcdef"
   }
}
```

Ejemplo

En el siguiente ejemplo, se eliminan del servidor todos los flujos de trabajo asociados.

Solicitud de muestra

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
 '{"OnUpload":[]}'
```

Ejemplo

Este es un ejemplo de respuesta para esta llamada a la API.

Respuesta de ejemplo

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python

- AWS SDK para Ruby V3

UpdateUser

Asigna nuevas propiedades a un usuario. Los parámetros que se transfieren modifican algunos o todos los elementos siguientes: el directorio de inicio, el rol y la política de la `UserName` y `ServerId` que especifique.

La respuesta devuelve el `ServerId` y el `UserName` para el usuario actualizado.

En la consola, puede seleccionar Restringido al crear o actualizar un usuario. Esto garantiza que el usuario no pueda acceder a nada que esté fuera de su directorio principal. La forma programática de configurar este comportamiento es actualizar al usuario. `HomeDirectoryType`Configúrelos `LOGICAL` como directorio raíz () y `HomeDirectoryMappings` especifíquelos `Entry` como directorio raíz (`/`) y `Target` como directorio principal.

Por ejemplo, si el directorio principal del usuario es`/test/admin-user`, el siguiente comando actualiza al usuario para que su configuración en la consola muestre el indicador Restringido como seleccionado.

```
aws transfer update-user --server-id <server-id> --user-name admin-user --
home-directory-type LOGICAL --home-directory-mappings "[{\"Entry\":\"/\",
\"Target\":\"/test/admin-user\"}]"
```

Sintaxis de la solicitud

```
{
   "HomeDirectory": "string",
   "HomeDirectoryMappings": [
      {
         "Entry": "string",
         "Target": "string",
         "Type": "string"
      }
   ],
   "HomeDirectoryType": "string",
   "Policy": "string",
   "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
   },
   "Role": "string",
```

```
    "ServerId": "string",
    "UserName": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HomeDirectory

Directorio de destino (carpeta) de un usuario cuando inicia sesión en el servidor a través del cliente.

Un ejemplo de `HomeDirectory` es `/bucket_name/home/mydirectory`.

> **Note**
>
> El parámetro `HomeDirectory` solo se utiliza si `HomeDirectoryType` está establecido en `PATH`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

HomeDirectoryMappings

Los mapeos de directorio lógico que especifican qué rutas de acceso y claves de Amazon S3 o Amazon EFS 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. Si solo especifica un destino, se muestra tal cual. También debe asegurarse de que su función AWS Identity and Access Management (de IAM) proporcione acceso a las rutas de entrada. `Target` Este valor solo se puede establecer si `HomeDirectoryType` está establecido en LOGICAL.

Lo siguiente es un ejemplo del par `Entry` y `Target`.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

En la mayoría de los casos, puede utilizar este valor en lugar de la política de sesión para limitar al usuario al directorio de inicio designado (“`chroot`”). Para ello, puede `Entry` establecer el valor «/» y el valor del HomeDirectory parámetro. `Target`

A continuación, se muestra un ejemplo del par `Entry` y `Target` para `chroot`.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Tipo: Matriz de HomeDirectoryMapEntry objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50000 artículos.

Obligatorio: no

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 la ruta absoluta 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 `HomeDirectoryMappings` que correspondan con la forma en que quiere que las rutas de acceso de Amazon S3 o de Amazon EFS sean visibles para sus usuarios.

> **Note**
>
> Si `HomeDirectoryType` es `LOGICAL`, debe proporcionar las asignaciones mediante el parámetro `HomeDirectoryMappings`. Si, por el contrario, `HomeDirectoryType` es `PATH`, se proporciona una ruta absoluta mediante el parámetro `HomeDirectory`. No puede tener `HomeDirectory` y `HomeDirectoryMappings` en su plantilla.

Tipo: cadena

Valores válidos: `PATH | LOGICAL`

Obligatorio: no

Policy

Una política de sesión para su usuario, de modo que pueda usar el mismo rol AWS Identity and Access Management (IAM) en varios usuarios. Esta política reduce el ámbito de acceso de un usuario a partes de su bucket de Amazon S3. Entre las variables que puede utilizar dentro de esta política se incluyen `${Transfer:UserName}`, `${Transfer:HomeDirectory}` y `${Transfer:HomeBucket}`.

> **Note**
>
> Esta política se aplica solo cuando el dominio de `ServerId` es Amazon S3. Amazon EFS no utiliza políticas de sesión.
>
> En el caso de las políticas de sesión, AWS Transfer Family almacena la política como un blob de JSON, en lugar del nombre de recurso de Amazon (ARN) de la política. Puede guardar la política como un blob JSON y pasarlo en el argumento `Policy`.
>
> Para ver un ejemplo de una política de sesión, consulte Example session policy (Ejemplo de política de sesión).
>
> Para obtener más información, consulte la AssumeRolereferencia de la API AWS de Security Token Service.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: no

PosixProfile

Especifica la identidad POSIX completa, incluido el ID de usuario (`Uid`), el ID de grupo (`Gid`) y cualquier ID de grupo secundario (`SecondaryGids`), que controla el acceso de los usuarios a los sistemas de archivos de Amazon Elastic File System (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.

Tipo: objeto PosixProfile

Obligatorio: no

Role

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que controla el acceso de los usuarios al bucket de Amazon S3 o al sistema de archivos Amazon 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.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

ServerId

Identificador único asignado por el sistema para una instancia del servidor de Transfer Family a la que está asignado el usuario.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

UserName

Una cadena única que identifica un usuario y se asocia a un servidor según se especifique en `ServerId`. Este nombre de usuario debe tener un mínimo de 3 caracteres y un máximo de 100. A continuación, se muestran caracteres válidos: a-z, A-Z, 0-9, guion bajo “_”, guion “-”, punto “.” y el signo “@”. El nombre de usuario no puede comenzar por un guion, un punto ni una arroba.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ServerId": "string",
   "UserName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ServerId

Identificador único asignado por el sistema para una instancia del servidor de Transfer Family a la que está asignada la cuenta.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

UserName

El identificador único de un usuario que está asignado a una instancia de servidor que se especificó en la solicitud.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServiceError

Esta excepción se produce cuando se produce un error en el AWS Transfer Family servicio.

Código de estado HTTP: 500

InvalidRequestException

Esta excepción se produce cuando el cliente envía una solicitud con un formato incorrecto.

Código de estado HTTP: 400

ResourceNotFoundException

Esta excepción se produce cuando el servicio AWS Transfer Family no encuentra un recurso.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud ha fallado porque el servicio AWS Transfer Family no está disponible.

Código de estado HTTP: 500

ThrottlingException

La solicitud fue denegada debido a una limitación de la solicitud.

Código de estado HTTP: 400

Ejemplos

Ejemplo

En el siguiente ejemplo se actualizan los usuarios de Transfer Family.

Solicitud de muestra

```
{
   "HomeDirectory": "/bucket2/documentation",
   "HomeDirectoryMappings": [
      {
         "Entry": "/directory1",
         "Target": "/bucket_name/home/mydirectory"
      }
```

```
    ],
    "HomeDirectoryType:" "PATH",
    "Role": "AssumeRole",
    "ServerId": "s-01234567890abcdef",
    "UserName": "my_user"
}
```

Ejemplo

Este es un ejemplo de respuesta para esta llamada a la API.

Respuesta de ejemplo

```
{
    "ServerId": "s-01234567890abcdef",
    "UserName": "my_user"
}
```

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

Data Types

Los siguientes tipos de datos son compatibles:

- As2ConnectorConfig

- CopyStepDetails
- CustomStepDetails
- DecryptStepDetails
- DeleteStepDetails
- DescribedAccess
- DescribedAgreement
- DescribedCertificate
- DescribedConnector
- DescribedExecution
- DescribedHostKey
- DescribedProfile
- DescribedSecurityPolicy
- DescribedServer
- DescribedUser
- DescribedWorkflow
- EfsFileLocation
- EndpointDetails
- ExecutionError
- ExecutionResults
- ExecutionStepResult
- FileLocation
- HomeDirectoryMapEntry
- IdentityProviderDetails
- InputFileLocation
- ListedAccess
- ListedAgreement
- ListedCertificate
- ListedConnector
- ListedExecution
- ListedHostKey

- ListedProfile
- ListedServer
- ListedUser
- ListedWorkflow
- LoggingConfiguration
- PosixProfile
- ProtocolDetails
- S3FileLocation
- S3InputFileLocation
- S3StorageOptions
- S3Tag
- ServiceMetadata
- SftpConnectorConfig
- SshPublicKey
- Tag
- TagStepDetails
- UserDetails
- WorkflowDetail
- WorkflowDetails
- WorkflowStep

As2ConnectorConfig

Contiene los detalles de un objeto conector AS2. El objeto conector se utiliza para los procesos salientes de AS2, para conectar al AWS Transfer Family cliente con el socio comercial.

Contenido

BasicAuthSecretId

Proporciona soporte de autenticación básica a la API de conectores AS2. Para utilizar la autenticación básica, debe proporcionar el nombre o el nombre de recurso de Amazon (ARN) de un secreto en AWS Secrets Manager.

El valor predeterminado para este parámetro es `null`, que indica que la autenticación básica no está habilitada para el conector.

Si el conector debe usar la autenticación básica, el secreto debe tener el siguiente formato:

```
{ "Username": "user-name", "Password": "user-password" }
```

Sustituya `user-name` y `user-password` por las credenciales del usuario real que se está autenticando.

Tenga en cuenta lo siguiente:

- Está almacenando estas credenciales en Secrets Manager, no pasándolas directamente a esta API.
- Si utiliza la API, los SDK o CloudFormation para configurar el conector, debe crear el secreto antes de poder habilitar la autenticación básica. Sin embargo, si utiliza la consola AWS de administración, puede hacer que el sistema cree el secreto por usted.

Si anteriormente habilitó la autenticación básica para un conector, puede deshabilitarla mediante la llamada a la API `UpdateConnector`. Por ejemplo, si utiliza la CLI, puede ejecutar el siguiente comando para eliminar la autenticación básica:

```
update-connector --connector-id my-connector-id --as2-config
'BasicAuthSecretId=""'
```

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: no

Compression

Especifica si el archivo AS2 está comprimido.

Tipo: cadena

Valores válidos: `ZLIB | DISABLED`

Obligatorio: no

EncryptionAlgorithm

El algoritmo que se utiliza para cifrar el archivo.

Tenga en cuenta lo siguiente:

- No utilice 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.
- Solo puede especificar `NONE` si la URL del conector utiliza HTTPS. El uso de HTTPS garantiza que no se envíe tráfico en texto claro.

Tipo: cadena

Valores válidos: `AES128_CBC | AES192_CBC | AES256_CBC | DES_EDE3_CBC | NONE`

Obligatorio: no

LocalProfileId

Un identificador único para el perfil local de AS2.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

MdnResponse

Se utiliza para las solicitudes salientes (de un AWS Transfer Family servidor a un servidor AS2 asociado) para determinar si la respuesta del socio a las transferencias es sincrónica o asíncrona. Especifique cualquiera de los siguientes valores:

- SYNC: el sistema espera una respuesta de MDN sincrónica que confirme que el archivo se ha transferido correctamente (o no).
- NONE: especifica que no se requiere ninguna respuesta de MDN.

Tipo: cadena

Valores válidos: SYNC | NONE

Obligatorio: no

MdnSigningAlgorithm

El algoritmo de firma de la respuesta de MDN.

> **Note**
>
> Si se establece COMO PREDETERMINADO (o no se establece en absoluto), se utiliza el valor de SigningAlgorithm.

Tipo: cadena

Valores válidos: SHA256 | SHA384 | SHA512 | SHA1 | NONE | DEFAULT

Obligatorio: no

MessageSubject

Se utiliza como atributo de encabezado Subject HTTP en los mensajes AS2 que se envían con el conector.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1024 caracteres.

Patrón: [\p{Print}\p{Blank}]+

Obligatorio: no

PartnerProfileId

Un identificador único para el perfil de socio para el conector.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

SigningAlgorithm

El algoritmo que se utiliza para firmar los mensajes AS2 enviados con el conector.

Tipo: cadena

Valores válidos: `SHA256 | SHA384 | SHA512 | SHA1 | NONE`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los SDK específicos del idioma AWS , consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CopyStepDetails

Cada tipo de paso tiene su propia estructura `StepDetails`.

Contenido

DestinationFileLocation

Especifica la ubicación del archivo que se va a copiar. Utilice `${Transfer:UserName}` o `${Transfer:UploadDate}` en este campo para parametrizar el prefijo de destino por nombre de usuario o fecha de carga.

- Establezca el valor de `DestinationFileLocation` a `${Transfer:UserName}` para copiar los archivos cargados a un bucket de Amazon S3 con el prefijo del nombre del usuario de Transfer Family que cargó el archivo.
- Establezca el valor de `DestinationFileLocation` a `${Transfer:UploadDate}` para copiar los archivos cargados a un bucket de Amazon S3 con el prefijo de la fecha de carga.

> **Note**
>
> El sistema adopta `UploadDate` a un formato de fecha de AAAA-MM-DD, en función de la fecha de carga del archivo en UTC.

Tipo: objeto InputFileLocation

Obligatorio: no

Name

El nombre del paso, que se utiliza como identificador.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 30.

Patrón: `[\w-]*`

Obligatorio: no

OverwriteExisting

Un indicador que señala si se sobrescribirá un archivo existente con el mismo nombre. El valor predeterminado es `FALSE`.

Si el flujo de trabajo procesa un archivo que tiene el mismo nombre que un archivo existente, el comportamiento es el siguiente:

- Si `OverwriteExisting` es `TRUE`, el archivo existente se reemplaza por el archivo que se está procesando.
- Si `OverwriteExisting` es `FALSE`, no ocurre nada y el procesamiento del flujo de trabajo se detiene.

Tipo: cadena

Valores válidos: `TRUE | FALSE`

Obligatorio: no

SourceFileLocation

Especifica qué archivo utilizar como entrada en el paso del flujo de trabajo: ya sea el resultado del paso anterior o el archivo cargado originalmente para el flujo de trabajo.

- Para usar el archivo anterior como entrada, introduzca `${previous.file}`. En este caso, este paso del flujo de trabajo utiliza como entrada el archivo de salida del paso anterior del flujo de trabajo. Este es el valor predeterminado.
- Para usar la ubicación del archivo cargado originalmente como entrada para este paso, introduzca `${original.file}`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `\$\{(\w+.)+\w+\}`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CustomStepDetails

Cada tipo de paso tiene su propia estructura `StepDetails`.

Contenido

Name

El nombre del paso, que se utiliza como identificador.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 30.

Patrón: `[\w-]*`

Obligatorio: no

SourceFileLocation

Especifica qué archivo utilizar como entrada en el paso del flujo de trabajo: ya sea el resultado del paso anterior o el archivo cargado originalmente para el flujo de trabajo.

- Para usar el archivo anterior como entrada, introduzca `${previous.file}`. En este caso, este paso del flujo de trabajo utiliza como entrada el archivo de salida del paso anterior del flujo de trabajo. Este es el valor predeterminado.
- Para usar la ubicación del archivo cargado originalmente como entrada para este paso, introduzca `${original.file}`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `\$\{(\w+.)+\w+\}`

Obligatorio: no

Target

El ARN para la función de Lambda a la que se llama.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 170 caracteres.

Patrón: `arn:[a-z-]+:lambda:.*`

Obligatorio: no

TimeoutSeconds

El tiempo de espera, en segundos, para el paso.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 1800.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DecryptStepDetails

Cada tipo de paso tiene su propia estructura `StepDetails`.

Contenido

DestinationFileLocation

Especifica la ubicación del archivo que se va a descifrar. Utilice `${Transfer:UserName}` o `${Transfer:UploadDate}` en este campo para parametrizar el prefijo de destino por nombre de usuario o fecha de carga.

- Establezca el valor de `DestinationFileLocation` a `${Transfer:UserName}` para descifrar los archivos cargados en un bucket de Amazon S3 con el prefijo del nombre del usuario de Transfer Family que cargó el archivo.
- Establezca el valor de `DestinationFileLocation` a `${Transfer:UploadDate}` para descifrar los archivos cargados a un bucket de Amazon S3 con el prefijo de la fecha de carga.

> **Note**
>
> El sistema adopta `UploadDate` a un formato de fecha de AAAA-MM-DD, en función de la fecha de carga del archivo en UTC.

Tipo: objeto InputFileLocation

Obligatorio: sí

Type

El tipo de cifrado. Actualmente, tiene que ser `PGP`.

Tipo: cadena

Valores válidos: `PGP`

Obligatorio: sí

Name

El nombre del paso, que se utiliza como identificador.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 30.

Patrón: `[\w-]*`

Obligatorio: no

OverwriteExisting

Un indicador que señala si se sobrescribirá un archivo existente con el mismo nombre. El valor predeterminado es `FALSE`.

Si el flujo de trabajo procesa un archivo que tiene el mismo nombre que un archivo existente, el comportamiento es el siguiente:

- Si `OverwriteExisting` es `TRUE`, el archivo existente se reemplaza por el archivo que se está procesando.
- Si `OverwriteExisting` es `FALSE`, no ocurre nada y el procesamiento del flujo de trabajo se detiene.

Tipo: cadena

Valores válidos: `TRUE | FALSE`

Obligatorio: no

SourceFileLocation

Especifica qué archivo utilizar como entrada en el paso del flujo de trabajo: ya sea el resultado del paso anterior o el archivo cargado originalmente para el flujo de trabajo.

- Para usar el archivo anterior como entrada, introduzca `${previous.file}`. En este caso, este paso del flujo de trabajo utiliza como entrada el archivo de salida del paso anterior del flujo de trabajo. Este es el valor predeterminado.
- Para usar la ubicación del archivo cargado originalmente como entrada para este paso, introduzca `${original.file}`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `\$\{(\w+.)+\w+\}`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DeleteStepDetails

El nombre del paso, que se utiliza para identificar el paso de eliminación.

Contenido

Name

El nombre del paso, que se utiliza como identificador.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 30.

Patrón: `[\w-]*`

Obligatorio: no

SourceFileLocation

Especifica qué archivo utilizar como entrada en el paso del flujo de trabajo: ya sea el resultado del paso anterior o el archivo cargado originalmente para el flujo de trabajo.

- Para usar el archivo anterior como entrada, introduzca `${previous.file}`. En este caso, este paso del flujo de trabajo utiliza como entrada el archivo de salida del paso anterior del flujo de trabajo. Este es el valor predeterminado.
- Para usar la ubicación del archivo cargado originalmente como entrada para este paso, introduzca `${original.file}`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `\$\{(\w+.)+\w+\}`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedAccess

Describe las propiedades del acceso especificado.

Contenido

ExternalId

Un identificador único que se requiere para identificar grupos específicos dentro de su directorio. Los usuarios del grupo que asocie tienen acceso a sus recursos de Amazon S3 o Amazon EFS a través de los protocolos habilitados que utilizan AWS Transfer Family. Si conoce el nombre del grupo, puede ver los valores del SID ejecutando el siguiente comando en Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

En ese comando, YourGroupNamesustitúyalo por el nombre del grupo de Active Directory.

La expresión regular utilizada para validar este parámetro es una cadena de caracteres compuesta de caracteres alfanuméricos en mayúscula y minúscula, sin espacios. También puede incluir guiones bajos y cualquiera de los siguientes caracteres: =,.@:/-

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `S-1-[\d-]+`

Obligatorio: no

HomeDirectory

Directorio de destino (carpeta) de un usuario cuando inicia sesión en el servidor a través del cliente.

Un ejemplo de `HomeDirectory` es `/bucket_name/home/mydirectory`.

> **Note**
>
> El parámetro `HomeDirectory` solo se utiliza si `HomeDirectoryType` está establecido en `PATH`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

HomeDirectoryMappings

Los mapeos de directorio lógico que especifican qué rutas de acceso y claves de Amazon S3 o Amazon EFS 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. Si solo especifica un destino, se muestra tal cual. También debe asegurarse de que su función AWS Identity and Access Management (de IAM) proporcione acceso a las rutas de entrada. `Target` Este valor solo se puede establecer si `HomeDirectoryType` está establecido en LOGICAL.

En la mayoría de los casos, puede utilizar este valor en lugar de la política de sesión para limitar el acceso asociado al directorio de inicio designado ("`chroot`"). Para ello, puede establecer `Entry` en "/" y `Target` al valor del parámetro `HomeDirectory`.

Tipo: Matriz de HomeDirectoryMapEntry objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50000 artículos.

Obligatorio: no

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 la ruta absoluta 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 `HomeDirectoryMappings` que correspondan con la forma en que quiere que las rutas de acceso de Amazon S3 o de Amazon EFS sean visibles para sus usuarios.

> **Note**
>
> Si `HomeDirectoryType` es `LOGICAL`, debe proporcionar las asignaciones mediante el parámetro `HomeDirectoryMappings`. Si, por el contrario, `HomeDirectoryType` es

PATH, se proporciona una ruta absoluta mediante el parámetro HomeDirectory. No puede tener HomeDirectory y HomeDirectoryMappings en su plantilla.

Tipo: cadena

Valores válidos: PATH | LOGICAL

Obligatorio: no

Policy

Una política de sesión para su usuario, de modo que pueda usar el mismo rol AWS Identity and Access Management (IAM) en varios usuarios. Esta política reduce el ámbito de acceso de un usuario a partes de su bucket de Amazon S3. Entre las variables que puede utilizar dentro de esta política se incluyen ${Transfer:UserName}, ${Transfer:HomeDirectory} y ${Transfer:HomeBucket}.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: no

PosixProfile

La identidad POSIX completa, incluido el ID de usuario (Uid), el ID de grupo (Gid) y cualquier ID de grupo secundario (SecondaryGids) 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.

Tipo: objeto PosixProfile

Obligatorio: no

Role

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que controla el acceso de los usuarios al bucket de Amazon S3 o al sistema de archivos Amazon 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.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedAgreement

Describe las propiedades de un acuerdo.

Contenido

Arn

El nombre de recurso de Amazon (ARN) único para el acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

AccessRole

Los conectores se utilizan para enviar archivos mediante el protocolo AS2 o SFTP. Para la función de acceso, proporcione el nombre de recurso de Amazon (ARN) de la AWS Identity and Access Management función que se va a utilizar.

Para conectores AS2

Con AS2, puede enviar archivos llamando a `StartFileTransfer` y especificando las rutas de los archivos en el parámetro de solicitud, `SendFilePaths`. Utilizamos el directorio principal del archivo (por ejemplo, para `--send-file-paths /bucket/dir/file.txt`, el directorio principal es `/bucket/dir/`) para almacenar temporalmente un archivo de mensajes AS2 procesado, almacenar el MDN cuando lo recibimos del socio y escribir un archivo JSON final que contenga los metadatos relevantes de la transmisión. Por lo tanto, `AccessRole` debe proporcionar acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`. Además, debe proporcionar acceso de lectura y escritura al directorio principal de los archivos que desea enviar con `StartFileTransfer`.

Si utiliza la autenticación básica para el conector AS2, el rol de acceso requiere el permiso `secretsmanager:GetSecretValue` para el secreto. Si el secreto se cifra con una clave gestionada por el cliente en lugar de la clave AWS gestionada en Secrets Manager, el rol también necesitará el `kms:Decrypt` permiso para esa clave.

Para conectores SFTP

Asegúrese de que el acceso al 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 otorgue `secretsmanager:GetSecretValue` permiso a. AWS Secrets Manager

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

AgreementId

Un identificador único para el acuerdo. Este identificador se devuelve al crear un acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `a-([0-9a-f]{17})`

Obligatorio: no

BaseDirectory

El directorio de destino (carpeta) de los archivos que se transfieren a través del protocolo AS2.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

Description

El nombre o la descripción breve utilizados para identificar el acuerdo.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Graph}]+`

Obligatorio: no

LocalProfileId

Un identificador único para el perfil local de AS2.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

PartnerProfileId

Un identificador único para el perfil de socio utilizado en el acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

ServerId

Identificador único asignado por el sistema para una instancia del servidor. Este identificador indica el servidor específico utilizado en el acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: no

Status

El estado actual del acuerdo, ya sea `ACTIVE` o `INACTIVE`.

Tipo: cadena

Valores válidos: `ACTIVE | INACTIVE`

Obligatorio: no

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar acuerdos.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedCertificate

Describe las propiedades de un certificado.

Contenido

Arn

El nombre de recurso de Amazon (ARN) único para el certificado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

ActiveDate

Una fecha opcional que especifica cuándo se activa el certificado.

Tipo: marca temporal

Obligatorio: no

Certificate

El nombre de archivo del certificado.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 16384 caracteres.

Patrón: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Obligatorio: no

CertificateChain

La lista de certificados que forman la cadena del certificado.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 2097152.

Patrón: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Obligatorio: no

CertificateId

Una matriz de identificadores de los certificados importados. Este identificador se utiliza para trabajar con perfiles y perfiles de socios.

Tipo: cadena

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Obligatorio: no

Description

El nombre o la descripción que se usa para identificar el certificado.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Graph}]+`

Obligatorio: no

InactiveDate

Una fecha opcional que especifica cuándo el certificado pasa a estar inactivo.

Tipo: marca temporal

Obligatorio: no

NotAfterDate

La fecha límite en la que el certificado es válido.

Tipo: marca temporal

Obligatorio: no

NotBeforeDate

La fecha más temprana en la que el certificado es válido.

Tipo: marca temporal

Obligatorio: no

Serial

El número de serie para el certificado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 48.

Patrón: `[\p{XDigit}{2}:?]*`

Obligatorio: no

Status

El certificado puede tener los siguientes estados: `ACTIVE`, `PENDING_ROTATION` o `INACTIVE`. `PENDING_ROTATION` significa que este certificado sustituirá al certificado actual cuando caduque.

Tipo: cadena

Valores válidos: `ACTIVE | PENDING_ROTATION | INACTIVE`

Obligatorio: no

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar certificados.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Type

Si se ha especificado una clave privada para el certificado, su tipo es `CERTIFICATE_WITH_PRIVATE_KEY`. Si no existe una clave privada, el tipo es `CERTIFICATE`.

Tipo: cadena

Valores válidos: `CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY`

Obligatorio: no

Usage

Especifica cómo se utiliza este certificado. Se puede utilizar de las siguientes maneras:

- `SIGNING`: Para firmar mensajes AS2
- `ENCRYPTION`: Para cifrar mensajes AS2
- `TLS`: Para proteger las comunicaciones AS2 enviadas a través de HTTPS

Tipo: cadena

Valores válidos: `SIGNING | ENCRYPTION`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedConnector

Describe los parámetros del conector, tal como los identifica el `ConnectorId`.

Contenido

Arn

El nombre de recurso de Amazon (ARN) para el conector.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

AccessRole

Los conectores se utilizan para enviar archivos mediante el protocolo AS2 o SFTP. Para la función de acceso, proporcione el nombre de recurso de Amazon (ARN) de la AWS Identity and Access Management función que se va a utilizar.

Para conectores AS2

Con AS2, puede enviar archivos llamando a `StartFileTransfer` y especificando las rutas de los archivos en el parámetro de solicitud, `SendFilePaths`. Utilizamos el directorio principal del archivo (por ejemplo, para `--send-file-paths /bucket/dir/file.txt`, el directorio principal es `/bucket/dir/`) para almacenar temporalmente un archivo de mensajes AS2 procesado, almacenar el MDN cuando lo recibimos del socio y escribir un archivo JSON final que contenga los metadatos relevantes de la transmisión. Por lo tanto, `AccessRole` debe proporcionar acceso de lectura y escritura al directorio principal de la ubicación del archivo que se utiliza en la solicitud `StartFileTransfer`. Además, debe proporcionar acceso de lectura y escritura al directorio principal de los archivos que desea enviar con `StartFileTransfer`.

Si utiliza la autenticación básica para el conector AS2, el rol de acceso requiere el permiso `secretsmanager:GetSecretValue` para el secreto. Si el secreto se cifra con una clave gestionada por el cliente en lugar de la clave AWS gestionada en Secrets Manager, el rol también necesitará el `kms:Decrypt` permiso para esa clave.

Para conectores SFTP

Asegúrese de que el acceso al 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 otorgue `secretsmanager:GetSecretValue` permiso a. AWS Secrets Manager

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

As2Config

Una estructura que contiene los parámetros de un objeto de conexión AS2.

Tipo: objeto As2ConnectorConfig

Obligatorio: no

ConnectorId

Un identificador único para el conector.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Obligatorio: no

LoggingRole

El nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que permite a un conector activar el CloudWatch registro de los eventos de Amazon S3. Cuando esté configurado, podrá ver la actividad del conector en sus CloudWatch registros.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

SecurityPolicyName

El nombre textual de la política de seguridad del conector especificado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 100 caracteres.

Patrón: `TransferSFTPConnectorSecurityPolicy-[A-Za-z0-9-]+`

Obligatorio: no

ServiceManagedEgressIpAddresses

La lista de direcciones IP de salida de este conector. Estas direcciones IP se asignan automáticamente al crear el conector.

Tipo: matriz de cadenas

Patrón: `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`

Obligatorio: no

SftpConfig

Una estructura que contiene los parámetros de un objeto de conexión SFTP.

Tipo: objeto SftpConnectorConfig

Obligatorio: no

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar conectores.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Url

La URL del punto de conexión de AS2 o SFTP del socio.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 255 caracteres.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedExecution

Los detalles de un objeto de ejecución.

Contenido

ExecutionId

Un identificador único para la ejecución del flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 36.

Patrón: `[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

Obligatorio: no

ExecutionRole

Rol de IAM asociado a la ejecución.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

InitialFileLocation

Estructura que describe la ubicación de los archivos de Amazon S3 o de EFS. Esta es la ubicación del archivo cuando comienza la ejecución: si el archivo se está copiando, es la ubicación inicial (y no la de destino).

Tipo: objeto FileLocation

Obligatorio: no

LoggingConfiguration

Rol de registro de IAM asociado a la ejecución.

Tipo: objeto LoggingConfiguration

Obligatorio: no

PosixProfile

La identidad POSIX completa, incluido el ID de usuario (`Uid`), el ID de grupo (`Gid`) y cualquier ID de grupo secundario (`SecondaryGids`) 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.

Tipo: objeto PosixProfile

Obligatorio: no

Results

Estructura que describe los resultados de la ejecución. Incluye una lista de los pasos junto con los detalles de cada paso, el tipo de error y el mensaje (si lo hay) y la estructura `OnExceptionSteps`.

Tipo: objeto ExecutionResults

Obligatorio: no

ServiceMetadata

Un objeto contenedor para los detalles de la sesión asociados a un flujo de trabajo.

Tipo: objeto ServiceMetadata

Obligatorio: no

Status

El estado es uno de la ejecución de trabajo. Puede estar en curso, completarse, encontrarse una excepción o estar gestionando la excepción.

Tipo: cadena

Valores válidos: `IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedHostKey

Detalles de la clave del host de un servidor.

Contenido

Arn

El nombre de recurso de Amazon (ARN) de la clave de host.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

DateImported

Fecha en la que se agregó la clave del host al servidor.

Tipo: marca temporal

Obligatorio: no

Description

Descripción textual de esta clave del host.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Print}]*`

Obligatorio: no

HostKeyFingerprint

La huella digital de la clave pública, que es una secuencia corta de bytes que se utiliza para identificar la clave pública más larga.

Tipo: cadena

Requerido: no

HostKeyId

Un identificador único para la clave de host.

Tipo: cadena

Limitaciones de longitud: longitud fija de 25.

Patrón: `hostkey-[0-9a-f]{17}`

Obligatorio: no

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar claves de host.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Type

El algoritmo de cifrado que se utiliza para la clave de host. El parámetro `Type` se especifica mediante uno de los siguientes valores:

- `ssh-rsa`
- `ssh-ed25519`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedProfile

Detalles de un perfil AS2 local o de un socio.

Contenido

Arn

El nombre de recurso de Amazon (ARN) único del perfil.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

As2Id

El `As2Id` es el nombre AS2, tal como se define en RFC 4130. Para las transferencias entrantes, este es el encabezado `AS2-From` de los mensajes AS2 enviados por el socio. Para los conectores de salida, este es el encabezado `AS2-To` de los mensajes AS2 enviados al socio mediante la operación `StartFileTransfer` de la API. Este ID no puede incluir espacios.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `[\p{Print}\s]*`

Obligatorio: no

CertificateIds

Una matriz de identificadores de los certificados importados. Este identificador se utiliza para trabajar con perfiles y perfiles de socios.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Obligatorio: no

ProfileId

Un identificador único para el perfil local o socio de AS2.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

ProfileType

Indica si se deben enumerar solo los perfiles de tipo `LOCAL` o solo los perfiles de tipo `PARTNER`. Si no se proporciona en la solicitud, el comando muestra todos los tipos de perfiles.

Tipo: cadena

Valores válidos: `LOCAL | PARTNER`

Obligatorio: no

Tags

Pares clave-valor que se pueden utilizar para agrupar y buscar perfiles.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedSecurityPolicy

Describe las propiedades de una política de seguridad que especifique. Para obtener más información sobre las políticas de seguridad, consulte Uso de políticas de seguridad para servidores o Uso de políticas de seguridad para conectores SFTP.

Contenido

SecurityPolicyName

El nombre textual de la política de seguridad especificada.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 100 caracteres.

Patrón: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Obligatorio: sí

Fips

Especifica si esta política habilita los requisitos del estándar federal de procesamiento de información (FIPS). Este parámetro se aplica a las políticas de seguridad del servidor y del conector.

Tipo: Booleano

Obligatorio: no

Protocols

Muestra los protocolos de transferencia de archivos a los que se aplica la política de seguridad.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos.

Valores válidos: `SFTP | FTPS`

Obligatorio: no

SshCiphers

Muestra los algoritmos de cifrado Secure Shell (SSH) habilitados en la política de seguridad adjunta al servidor o conector. Este parámetro se aplica a las políticas de seguridad del servidor y del conector.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 50 caracteres.

Obligatorio: no

SshHostKeyAlgorithms

Muestra los algoritmos clave del host de la política de seguridad.

> **Note**
>
> Este parámetro solo se aplica a las políticas de seguridad de los conectores.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 50 caracteres.

Obligatorio: no

SshKexs

Muestra los algoritmos de cifrado de intercambio de claves SSH (KEX) habilitados en la política de seguridad adjunta al servidor o conector. Este parámetro se aplica a las políticas de seguridad del servidor y del conector.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 50 caracteres.

Obligatorio: no

SshMacs

Muestra los algoritmos de cifrado del código de autenticación de mensajes (MAC) SSH habilitados en la política de seguridad que está conectada al servidor o al conector. Este parámetro se aplica a las políticas de seguridad del servidor y del conector.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 50 caracteres.

Obligatorio: no

TlsCiphers

Muestra los algoritmos de cifrado de seguridad de la capa de transporte (TLS) habilitados en la política de seguridad adjunta al servidor.

> **Note**
>
> Este parámetro solo se aplica a las políticas de seguridad de los servidores.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 50 caracteres.

Obligatorio: no

Type

El tipo de recurso al que se aplica la política de seguridad, ya sea servidor o conector.

Tipo: cadena

Valores válidos: `SERVER | CONNECTOR`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedServer

Describe las propiedades de un servidor habilitado para el protocolo de File Transfer que se especificó.

Contenido

Arn

Especifica el nombre de recurso de Amazon (ARN) único del servidor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

As2ServiceManagedEgressIpAddresses

La lista de direcciones IP de salida de este servidor. Estas direcciones IP solo son relevantes para los servidores que utilizan el protocolo AS2. Se utilizan para enviar mDNS asíncronos.

Estas direcciones IP se asignan automáticamente al crear un servidor AS2. Además, si actualiza un servidor existente y agrega el protocolo AS2, también se asignan direcciones IP estáticas.

Tipo: matriz de cadenas

Patrón: `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`

Obligatorio: no

Certificate

Especifica el ARN del AWS certificado Certificate Manager (ACM). Necesario cuando `Protocols` se establece en `FTPS`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1600 caracteres.

Obligatorio: no

Domain

Especifica el dominio del sistema de almacenamiento que se utiliza para las transferencias de archivos. Hay dos dominios disponibles: Amazon Simple Storage Service (Amazon S3) y Amazon Elastic File System (Amazon EFS). El valor predeterminado es S3.

Tipo: cadena

Valores válidos: `S3 | EFS`

Obligatorio: no

EndpointDetails

Los ajustes del punto de conexión de la nube privada virtual (VPC) que está configurado para su servidor. Cuando aloja el punto de conexión dentro de la VPC, puede hacer que sea accesible solo para los recursos de la VPC, o puede adjuntar direcciones IP elásticas y hacer que sea accesible para los clientes a través de Internet. Los grupos de seguridad predeterminados de su VPC se asignan automáticamente a su punto de conexión.

Tipo: objeto EndpointDetails

Obligatorio: no

EndpointType

El tipo de punto de conexión al que está conectado el servidor. Si su servidor está conectado a un punto de conexión de VPC, su servidor no será accesible a través de la Internet pública.

Tipo: cadena

Valores válidos: `PUBLIC | VPC | VPC_ENDPOINT`

Obligatorio: no

HostKeyFingerprint

Especifica la huella digital SHA256 codificada en Base64 de la clave del host del servidor. El valor es el equivalente a la salida del comando `ssh-keygen -l -f my-new-server-key`.

Tipo: cadena

Requerido: no

IdentityProviderDetails

Especifica la información para llamar a una API de autenticación proporcionada por parte del cliente. Este campo no se rellena cuando el `IdentityProviderType` de un servidor es `AWS_DIRECTORY_SERVICE` o `SERVICE_MANAGED`.

Tipo: objeto IdentityProviderDetails

Obligatorio: no

IdentityProviderType

El modo de autenticación de un servidor. El valor predeterminado es`SERVICE_MANAGED`, que le permite almacenar las credenciales de usuario y acceder a ellas dentro del AWS Transfer Family servicio.

Úselo `AWS_DIRECTORY_SERVICE` para proporcionar acceso a los grupos de Active Directory AWS Directory Service for Microsoft Active Directory o a Microsoft Active Directory en su entorno local o AWS mediante AD Connector. Esta opción también requiere que se especifique el ID del directorio mediante el parámetro `IdentityProviderDetails`.

Utilice el valor `API_GATEWAY` para la integración con un proveedor de identidades de su elección. La configuración de `API_GATEWAY` requiere que proporcione un punto de conexión de Amazon API Gateway para solicitar la autenticación mediante el parámetro `IdentityProviderDetails`.

Usa el `AWS_LAMBDA` valor para usar directamente una AWS Lambda función como proveedor de identidades. Si elige este valor, debe especificar el ARN de la función de Lambda en el parámetro `Function` para el tipo de datos de `IdentityProviderDetails`.

Tipo: cadena

Valores válidos: `SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA`

Obligatorio: no

LoggingRole

El nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que permite a un servidor activar el CloudWatch registro de Amazon para Amazon S3 o

Amazon EFSEvents. Cuando esté configurado, podrá ver la actividad de los usuarios en sus registros. CloudWatch

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Patrón: `(|arn:.*role/\S+)`

Obligatorio: no

PostAuthenticationLoginBanner

Especifica una cadena para que se muestre cuando los usuarios se conecten a un servidor. Esta cadena se muestra después de que el usuario se autentique.

> **Note**
>
> El protocolo SFTP no admite banners de visualización posteriores a la autenticación.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 4 096 caracteres.

Patrón: `[\x09-\x0D\x20-\x7E]*`

Obligatorio: no

PreAuthenticationLoginBanner

Especifica una cadena para que se muestre cuando los usuarios se conecten a un servidor. Esta cadena se muestra antes de que el usuario se autentique. Por ejemplo, el siguiente banner muestra detalles sobre el uso del sistema:

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 4 096 caracteres.

Patrón: `[\x09-\x0D\x20-\x7E]*`

Obligatorio: no

ProtocolDetails

La configuración de protocolo configurados para su servidor.

- Use el parámetro `PassiveIp` para indicar el modo pasivo (para los protocolos FTP y FTPS). Ingrese una sola dirección IPv4 de cuatro puntos, como la dirección IP externa de un firewall, un enrutador o un equilibrador de carga.
- Utilice el parámetro `SetStatOption` para ignorar el error que se genera cuando el cliente intenta usar el comando `SETSTAT` en un archivo que esté cargando en un bucket de Amazon S3. Para que el AWS Transfer Family servidor ignore el `SETSTAT` comando y cargue archivos sin necesidad de realizar ningún cambio en el cliente SFTP, defina `ENABLE_NO_OP` el valor en. Si estableces el `SetStatOption` parámetro en`ENABLE_NO_OP`, Transfer Family generará una entrada de registro en Amazon CloudWatch Logs para que puedas determinar cuándo el cliente está realizando una `SETSTAT` llamada.
- Para determinar si su AWS Transfer Family servidor reanuda las sesiones negociadas recientes mediante un identificador de sesión único, utilice el `TlsSessionResumptionMode` parámetro.
- `As2Transports` indica el método de transporte de los mensajes de AS2. Actualmente, solo se admite HTTP.

Tipo: objeto ProtocolDetails

Obligatorio: no

Protocols

Especifica el protocolo o los protocolos de File Transfer a través de los cuales el cliente de protocolo de File Transfer puede conectarse al punto de enlace del servidor. Los protocolos disponibles son:

- `SFTP` (Protocolo de File Transfer Secure Shell (SSH)): transferencia de archivos a través de SSH
- `FTPS` (Protocolo de File Transfer seguro): transferencia de archivos con cifrado TLS
- `FTP` (Protocolo de File Transfer): transferencia de archivos sin cifrar
- `AS2`(Declaración de aplicabilidad 2): se utiliza para transportar datos estructurados business-to-business

> **Note**
>
> - Si lo seleccionaFTPS, debe elegir un certificado almacenado en AWS Certificate Manager (ACM) que se utilice para identificar el servidor cuando los clientes se conecten a él a través de FTPS.
> - Si el `Protocol` incluye `FTP` o `FTPS`, el `EndpointType` debe ser `VPC` y el `IdentityProviderType` debe ser `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
> - Si `Protocol` incluye `FTP`, entonces `AddressAllocationIds` no se puede asociar.
> - Si el `Protocol` se establece solo en `SFTP`, se puede establecer el `EndpointType` como `PUBLIC` y el `IdentityProviderType` se puede configurar como cualquiera de los tipos de identidad admitidos: `SERVICE_MANAGED`, `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
> - Si `Protocol` incluye `AS2`, `EndpointType` debe ser `VPC` y el dominio debe ser Amazon S3.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. La cantidad máxima es de 4 elementos.

Valores válidos: `SFTP | FTP | FTPS | AS2`

Obligatorio: no

S3StorageOptions

Especifica si el rendimiento de los directorios de Amazon S3 está optimizado o no. Esta opción está deshabilitada de forma predeterminada.

De forma predeterminada, las asignaciones de los directorios principales tienen un `TYPE` valor de. `DIRECTORY` Si habilita esta opción, tendrá que establecerla de forma explícita `FILE` si `HomeDirectoryMapEntry` `Type` desea que la asignación tenga un destino de archivo.

Tipo: objeto S3StorageOptions

Obligatorio: no

SecurityPolicyName

Especifica el nombre de la política de seguridad del servidor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 100 caracteres.

Patrón: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Obligatorio: no

ServerId

Especifica el identificador único asignado por parte del sistema para un servidor del que se crea una instancia.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: no

State

Estado del servidor que se describió. Un valor de `ONLINE` indica que el servidor puede aceptar trabajos y transferir archivos. Un valor `State` de `OFFLINE` significa que el servidor no puede realizar operaciones de File Transfer.

Los estados de `STARTING` y `STOPPING` indican que el servidor se encuentra en un estado intermedio; es decir, que no puede responder por completo o que no está completamente desconectado. Los valores de `START_FAILED` o `STOP_FAILED` pueden indicar una condición de error.

Tipo: cadena

Valores válidos: `OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED`

Obligatorio: no

StructuredLogDestinations

Especifica los grupos de registro a los que se envían los registros de su servidor.

Para especificar un grupo de registros, debe proporcionar el ARN de un grupo de registros existente. En este caso, el formato del grupo de registros es el siguiente:

`arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*`

Por ejemplo, `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

Si ha especificado previamente un grupo de registros para un servidor, puede borrarlo y desactivar el registro estructurado proporcionando un valor vacío para este parámetro en una llamada `update-server`. Por ejemplo:

```
update-server --server-id s-1234567890abcdef0 --structured-log-destinations
```

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: no

Tags

Especifica los pares clave-valor que puede usar para buscar y agrupar los servidores que se asignaron al servidor descrito.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

UserCount

Especifica el número de usuarios que están asignados a un servidor que especificó con el `ServerId`.

Tipo: entero

Obligatorio: no

WorkflowDetails

Especifica el ID del flujo de trabajo que se va a asignar y el rol de ejecución que se utiliza para ejecutar el flujo de trabajo.

Además de un flujo de trabajo que se ejecuta cuando un archivo se carga por completo, `WorkflowDetails` también puede contener un ID de flujo de trabajo (y un rol de ejecución) para que un flujo de trabajo se ejecute en una carga parcial. Se produce una carga parcial si la sesión de servidor se desconecta mientras se está cargando el archivo.

Tipo: objeto WorkflowDetails

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DescribedUser

Describe las propiedades de un usuario especificado.

Contenido

Arn

Especifica el nombre de recurso de Amazon (ARN) único del usuario del que se solicitó una descripción.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

HomeDirectory

Directorio de destino (carpeta) de un usuario cuando inicia sesión en el servidor a través del cliente.

Un ejemplo de `HomeDirectory` es `/bucket_name/home/mydirectory`.

> **Note**
>
> El parámetro `HomeDirectory` solo se utiliza si `HomeDirectoryType` está establecido en `PATH`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

HomeDirectoryMappings

Los mapeos de directorio lógico que especifican qué rutas de acceso y claves de Amazon S3 o Amazon EFS 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. Si solo especifica un destino, se muestra tal cual. También debe asegurarse de que su función AWS Identity and Access Management (de IAM) proporcione acceso a las rutas de entrada. `Target` Este valor solo se puede establecer si `HomeDirectoryType` está establecido en LOGICAL.

En la mayoría de los casos, puede usar este valor en lugar de la política de sesión para limitar al usuario al directorio de inicio designado ("`chroot`"). Para ello, puede `Entry` establecer el valor «/» y el valor del HomeDirectory parámetro. `Target`

Tipo: Matriz de HomeDirectoryMapEntry objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50000 artículos.

Obligatorio: no

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 la ruta absoluta 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 `HomeDirectoryMappings` que correspondan con la forma en que quiere que las rutas de acceso de Amazon S3 o de Amazon EFS sean visibles para sus usuarios.

> **Note**
>
> Si `HomeDirectoryType` es `LOGICAL`, debe proporcionar las asignaciones mediante el parámetro `HomeDirectoryMappings`. Si, por el contrario, `HomeDirectoryType` es `PATH`, se proporciona una ruta absoluta mediante el parámetro `HomeDirectory`. No puede tener `HomeDirectory` y `HomeDirectoryMappings` en su plantilla.

Tipo: cadena

Valores válidos: `PATH | LOGICAL`

Obligatorio: no

Policy

Una política de sesión para su usuario, de modo que pueda usar el mismo rol AWS Identity and Access Management (IAM) en varios usuarios. Esta política reduce el ámbito de acceso de

un usuario a partes de su bucket de Amazon S3. Entre las variables que puede utilizar dentro de esta política se incluyen `${Transfer:UserName}`, `${Transfer:HomeDirectory}` y `${Transfer:HomeBucket}`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: no

PosixProfile

Especifica la identidad POSIX completa, incluido el ID de usuario (`Uid`), el ID de grupo (`Gid`) y cualquier ID de grupo secundario (`SecondaryGids`), que controla el acceso de los usuarios a los sistemas de archivos de Amazon Elastic File System (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.

Tipo: objeto PosixProfile

Obligatorio: no

Role

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que controla el acceso de los usuarios al bucket de Amazon S3 o al sistema de archivos Amazon 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.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

SshPublicKeys

Especifica la parte de la clave pública de las claves Secure Shell (SSH) almacenadas para el usuario descrito.

Tipo: matriz de objetos SshPublicKey

Miembros de la matriz: número mínimo de 0 artículos. La cantidad máxima es de 5 artículos.

Obligatorio: no

Tags

Especifica los pares clave-valor del usuario solicitado. La etiqueta se puede utilizar para buscar y agrupar usuarios con objetivos diversos.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

UserName

Especifica el nombre del usuario del que se solicitó una descripción. Los nombres de usuario se utilizan con fines de autenticación. Esta es la cadena que utilizará el usuario cuando este inicie sesión en el servidor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

DescribedWorkflow

Describe las propiedades de flujo de trabajo especificado

Contenido

Arn

Especifica el nombre de recurso de Amazon (ARN) único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

Description

Especifica la descripción del texto del flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `[\w- ]*`

Obligatorio: no

OnExceptionSteps

Especifica los pasos (acciones) que se deben seguir si se encuentran errores durante la ejecución del flujo de trabajo.

Tipo: matriz de objetos WorkflowStep

Miembros de la matriz: número mínimo de 0 artículos. La cantidad máxima es de 8 elementos.

Obligatorio: no

Steps

Especifica los detalles de los pasos que están en el flujo de trabajo especificado.

Tipo: matriz de objetos WorkflowStep

Miembros de la matriz: número mínimo de 0 artículos. La cantidad máxima es de 8 elementos.

Obligatorio: no

Tags

Pares clave-valor que se pueden usar para agrupar y buscar flujos de trabajo. Las etiquetas son metadatos asociados a flujos de trabajo para cualquier fin.

Tipo: Matriz de Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

EfsFileLocation

Especifica los detalles de la ubicación del archivo que se está utilizando en el flujo de trabajo. Solo se aplica si utiliza Amazon Elastic File System (Amazon EFS) para el almacenamiento.

Contenido

FileSystemId

Identificador del sistema de archivos asignado por Amazon EFS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 128.

Patrón: `(arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:(access-point/fsap|file-system/fs)-[0-9a-f]{8,40}|fs(ap)?-[0-9a-f]{8,40})`

Obligatorio: no

Path

Nombre de la ruta de la carpeta que utiliza un flujo de trabajo.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 65536.

Patrón: `[^\x00]+`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

EndpointDetails

El punto de conexión de la nube privada virtual (VPC) configurado para su servidor de protocolo habilitado para la transferencia de archivos. Con un punto de enlace de la VPC, puede restringir el acceso al servidor y a los recursos solo dentro de su VPC. Para controlar el tráfico de Internet entrante, invoque la API de `UpdateServer` y adjunte una dirección IP elástica al punto de conexión del servidor.

> **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 19 de mayo de 2021 o antes, no se verá afectado. Después de esta fecha, use `EndpointType=VPC`.
> Para obtener más información, consulte Suspender el uso de VPC_ENDPOINT.

Contenido

AddressAllocationIds

Una lista de ID de asignación de direcciones necesarios para anexar una dirección IP elástica al punto de enlace del servidor.

Un ID de asignación de direcciones corresponde al ID de asignación de una dirección IP elástica. Este valor se puede recuperar del `allocationId` campo del tipo de datos Dirección Amazon EC2. Una forma de recuperar este valor consiste en llamar a la API de EC2 DescribeAddresses.

Este parámetro es opcional. Establezca este parámetro si quiere que su punto final de VPC sea público. Para obtener más información, consulte Crear un punto final con acceso a Internet para su servidor.

> **Note**
>
> Esta propiedad solo se puede establecer de la siguiente manera:
>
> - `EndpointType`debe configurarse en `VPC`
> - El servidor Transfer Family debe estar desconectado.

- No puede establecer este parámetro para los servidores Transfer Family que utilizan el protocolo FTP.
- El servidor ya debe estar `SubnetIds` poblado (`SubnetIdsy AddressAllocationIds` no se puede actualizar simultáneamente).
- `AddressAllocationIds`no puede contener duplicados y debe tener la misma longitud que`SubnetIds`. Por ejemplo, si tiene tres ID de subred, también debe especificar tres ID de asignación de direcciones.
- Llame a la `UpdateServer` API para configurar o cambiar este parámetro.

Tipo: matriz de cadenas

Obligatorio: no

SecurityGroupIds

Lista de identificadores de grupos de seguridad que están disponibles para asociarlos al punto de enlace del servidor.

> **Note**
>
> Esta propiedad solo se puede utilizar cuando `EndpointType` está establecido en `VPC`. Puedes editar la `SecurityGroupIds` propiedad en la UpdateServerAPI solo si cambias el `EndpointType` de `PUBLIC` o `VPC_ENDPOINT` el`VPC`. Para cambiar los grupos de seguridad asociados al punto final de la VPC del servidor tras su creación, utilice la API Amazon ModifyVpcEndpointEC2.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 11. La longitud máxima es de 20 caracteres.

Patrón: `sg-[0-9a-f]{8,17}`

Obligatorio: no

SubnetIds

Una lista de ID de subred necesarios para alojar el punto de enlace del servidor en la VPC.

> **Note**
>
> Esta propiedad solo se puede utilizar cuando `EndpointType` está establecido en `VPC`.

Tipo: matriz de cadenas

Obligatorio: no

VpcEndpointId

El identificador único para el punto de conexión de VPC.

> **Note**
>
> Esta propiedad solo se puede utilizar cuando `EndpointType` está establecido en `VPC_ENDPOINT`.
> Para obtener más información, consulte Suspender el uso de VPC_ENDPOINT.

Tipo: cadena

Limitaciones de longitud: longitud fija de 22.

Patrón: `vpce-[0-9a-f]{17}`

Obligatorio: no

VpcId

El identificador de VPC de la VPC en la que se hospedará el punto de conexión del servidor.

> **Note**
>
> Esta propiedad solo se puede utilizar cuando `EndpointType` está establecido en `VPC`.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ExecutionError

Especifica el mensaje y el tipo de error para un error que se produce durante la ejecución del flujo de trabajo.

Contenido

Message

Especifica el mensaje descriptivo que corresponde a `ErrorType`.

Tipo: cadena

Obligatorio: sí

Type

Especifica el tipo de error.

- `ALREADY_EXISTS`: se produce durante un paso de copia, si la opción de sobrescritura no está seleccionada y ya existe un archivo con el mismo nombre en la ubicación de destino.
- `BAD_REQUEST`: una solicitud errónea general: por ejemplo, un paso que intenta etiquetar un archivo EFS devuelve `BAD_REQUEST`, ya que solo se pueden etiquetar los archivos S3.
- `CUSTOM_STEP_FAILED`: se produce cuando el paso personalizado proporciona una llamada que indica un error.
- `INTERNAL_SERVER_ERROR`: error general que se puede producir por diversas razones.
- `NOT_FOUND`: se produce cuando la entidad solicitada, por ejemplo, el archivo fuente de un paso de copia, no existe.
- `PERMISSION_DENIED`: se produce si la política no contiene los permisos correctos para completar uno o más de los pasos del flujo de trabajo.
- `TIMEOUT`: se produce cuando se agota el tiempo de espera de la ejecución.

  > **Note**
  >
  > Puede configurar `TimeoutSeconds` para un paso personalizado, desde 1 segundo hasta 1800 segundos (30 minutos).

- `THROTTLED`: se produce si se supera la nueva tasa de recarga de ejecución de un flujo de trabajo por segundo.

Tipo: cadena

Valores válidos: `PERMISSION_DENIED | CUSTOM_STEP_FAILED | THROTTLED | ALREADY_EXISTS | NOT_FOUND | BAD_REQUEST | TIMEOUT | INTERNAL_SERVER_ERROR`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ExecutionResults

Especifica los pasos del flujo de trabajo, así como los pasos que se deben ejecutar en caso de que se produzca algún error durante la ejecución del flujo de trabajo.

Contenido

OnExceptionSteps

Especifica los pasos (acciones) que se deben seguir si se encuentran errores durante la ejecución del flujo de trabajo.

Tipo: Matriz de ExecutionStepResult objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Steps

Especifica los detalles de los pasos que están en el flujo de trabajo especificado.

Tipo: Matriz de ExecutionStepResult objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 50 artículos.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ExecutionStepResult

Especifica los siguientes detalles del paso: error (si lo hay), resultados (si los hay) y tipo de paso.

Contenido

Error

Especifica los detalles de un error, si se produjo durante la ejecución del paso del flujo de trabajo especificado.

Tipo: objeto ExecutionError

Obligatorio: no

Outputs

Los valores del par clave/valor aplicados como etiqueta al archivo. Solo se aplica si el tipo de paso es `TAG`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 65536.

Obligatorio: no

StepType

Uno de los tipos de pasos disponibles.

- **`COPY`** : copiar el archivo en otra ubicación.
- **`CUSTOM`**- Realice un paso personalizado con un objetivo de AWS Lambda función.
- **`DECRYPT`** : descifrar un archivo que se cifró antes de subir.
- **`DELETE`** : eliminar el archivo.
- **`TAG`** : agregar una etiqueta al archivo.

Tipo: cadena

Valores válidos: `COPY | CUSTOM | TAG | DELETE | DECRYPT`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

FileLocation

Especifica los detalles del archivo Amazon S3 o EFS que se utilizarán en el paso.

Contenido

EfsFileLocation

Especifica el identificador de Amazon EFS y la ruta del archivo que se utiliza.

Tipo: objeto EfsFileLocation

Obligatorio: no

S3FileLocation

Especifica los detalles de S3 del archivo que se está utilizando, como el bucket, la ETag, etc.

Tipo: objeto S3FileLocation

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

HomeDirectoryMapEntry

Representa un objeto que contiene entradas y destinos para `HomeDirectoryMappings`.

A continuación, se muestra un ejemplo del par `Entry` y `Target` para `chroot`.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Contenido

Entry

Representa una entrada de `HomeDirectoryMappings`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `/.*`

Obligatorio: sí

Target

Representa el destino del mapa que se utiliza en `HomeDirectoryMapEntry`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `/.*`

Obligatorio: sí

Type

Especifica el tipo de mapeo. Defina el tipo en `FILE` si desea que la asignación apunte a un archivo o `DIRECTORY` que el directorio apunte a un directorio.

> **Note**
>
> De forma predeterminada, las asignaciones del directorio principal tienen un `Type` de `DIRECTORY` cuando se crea un servidor Transfer Family. Deberás configurarlo explícitamente `FILE` si `Type` quieres que una asignación tenga un destino de archivo.

Tipo: cadena

Valores válidos: `FILE | DIRECTORY`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

IdentityProviderDetails

Devuelve información relacionada con el tipo de autenticación de usuario que se utiliza para los usuarios de un servidor con protocolo habilitado de File Transfer. Un servidor solo puede tener un método de autenticación.

Contenido

DirectoryId

El identificador del AWS Directory Service directorio que desea usar como proveedor de identidad.

Tipo: cadena

Limitaciones de longitud: longitud fija de 12.

Patrón: `d-[0-9a-f]{10}`

Obligatorio: no

Function

El ARN de una función de Lambda que se usa para el proveedor de identidades.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 170 caracteres.

Patrón: `arn:[a-z-]+:lambda:.*`

Obligatorio: no

InvocationRole

Este parámetro solo es aplicable si su `IdentityProviderType` es `API_GATEWAY`. Proporciona el tipo de `InvocationRole` utilizado para autenticar la cuenta de usuario.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

SftpAuthenticationMethods

Para los servidores habilitados para SFTP y solo para los proveedores de identidad personalizados, puede especificar si se debe autenticar mediante una contraseña, una clave SSH o ambas.

- `PASSWORD`: los usuarios deben proporcionar su contraseña para conectarse.
- `PUBLIC_KEY`: los usuarios deben proporcionar su clave privada para conectarse.
- `PUBLIC_KEY_OR_PASSWORD`: los usuarios pueden autenticarse con su contraseña o con su clave. Este es el valor predeterminado.
- `PUBLIC_KEY_AND_PASSWORD`: 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.

Tipo: cadena

Valores válidos: `PASSWORD | PUBLIC_KEY | PUBLIC_KEY_OR_PASSWORD | PUBLIC_KEY_AND_PASSWORD`

Obligatorio: no

Url

Proporciona la ubicación del punto de conexión de servicio utilizado para autenticar a los usuarios.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 255 caracteres.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

InputFileLocation

Especifica la ubicación del archivo que se está procesando.

Contenido

EfsFileLocation

Especifica los detalles del archivo Amazon Elastic File System (Amazon EFS) que se está descifrando.

Tipo: objeto EfsFileLocation

Obligatorio: no

S3FileLocation

Especifica los detalles del archivo Amazon S3 que se está copiando o descifrando.

Tipo: objeto S3InputFileLocation

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedAccess

Muestra las propiedades de uno o más accesos asociados especificados.

Contenido

ExternalId

Un identificador único que se requiere para identificar grupos específicos dentro de su directorio. Los usuarios del grupo que asocie tienen acceso a sus recursos de Amazon S3 o Amazon EFS a través de los protocolos habilitados que utilizan AWS Transfer Family. Si conoce el nombre del grupo, puede ver los valores del SID ejecutando el siguiente comando en Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties
* | Select SamAccountName,ObjectSid
```

En ese comando, YourGroupNamesustitúyalo por el nombre del grupo de Active Directory.

La expresión regular utilizada para validar este parámetro es una cadena de caracteres compuesta de caracteres alfanuméricos en mayúscula y minúscula, sin espacios. También puede incluir guiones bajos y cualquiera de los siguientes caracteres: =,.@:/-

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `S-1-[\d-]+`

Obligatorio: no

HomeDirectory

Directorio de destino (carpeta) de un usuario cuando inicia sesión en el servidor a través del cliente.

Un ejemplo de `HomeDirectory` es `/bucket_name/home/mydirectory`.

> **Note**
>
> El parámetro `HomeDirectory` solo se utiliza si `HomeDirectoryType` está establecido en `PATH`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

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 la ruta absoluta 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 `HomeDirectoryMappings` que correspondan con la forma en que quiere que las rutas de acceso de Amazon S3 o de Amazon EFS sean visibles para sus usuarios.

> **Note**
>
> Si `HomeDirectoryType` es `LOGICAL`, debe proporcionar las asignaciones mediante el parámetro `HomeDirectoryMappings`. Si, por el contrario, `HomeDirectoryType` es `PATH`, se proporciona una ruta absoluta mediante el parámetro `HomeDirectory`. No puede tener `HomeDirectory` y `HomeDirectoryMappings` en su plantilla.

Tipo: cadena

Valores válidos: `PATH | LOGICAL`

Obligatorio: no

Role

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que controla el acceso de los usuarios al bucket de Amazon S3 o al sistema de archivos Amazon 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.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedAgreement

Describe las propiedades de un acuerdo.

Contenido

AgreementId

Un identificador único para el acuerdo. Este identificador se devuelve al crear un acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `a-([0-9a-f]{17})`

Obligatorio: no

Arn

El nombre de recurso de Amazon (ARN) del acuerdo especificado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: no

Description

La descripción actual del acuerdo. Puede cambiarla llamando a la operación de `UpdateAgreement` y proporcionando una nueva descripción.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Graph}]+`

Obligatorio: no

LocalProfileId

Un identificador único para el perfil local de AS2.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

PartnerProfileId

Un identificador único para el perfil de socio.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

ServerId

El identificador único para el acuerdo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: no

Status

El acuerdo puede ser `ACTIVE` o `INACTIVE`.

Tipo: cadena

Valores válidos: `ACTIVE | INACTIVE`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedCertificate

Describe las propiedades de un certificado.

Contenido

ActiveDate

Una fecha opcional que especifica cuándo se activa el certificado.

Tipo: marca temporal

Obligatorio: no

Arn

El nombre de recurso de Amazon (ARN) del certificado especificado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: no

CertificateId

Una matriz de identificadores de los certificados importados. Este identificador se utiliza para trabajar con perfiles y perfiles de socios.

Tipo: cadena

Limitaciones de longitud: longitud fija de 22.

Patrón: `cert-([0-9a-f]{17})`

Obligatorio: no

Description

El nombre o la descripción corta que se usa para identificar el certificado.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Graph}]+`

Obligatorio: no

InactiveDate

Una fecha opcional que especifica cuándo el certificado pasa a estar inactivo.

Tipo: marca temporal

Obligatorio: no

Status

El certificado puede tener los siguientes estados: `ACTIVE`, `PENDING_ROTATION` o `INACTIVE`. `PENDING_ROTATION` significa que este certificado sustituirá al certificado actual cuando caduque.

Tipo: cadena

Valores válidos: `ACTIVE | PENDING_ROTATION | INACTIVE`

Obligatorio: no

Type

El tipo para el certificado. Si se ha especificado una clave privada para el certificado, su tipo es `CERTIFICATE_WITH_PRIVATE_KEY`. Si no existe una clave privada, el tipo es `CERTIFICATE`.

Tipo: cadena

Valores válidos: `CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY`

Obligatorio: no

Usage

Especifica cómo se utiliza este certificado. Se puede utilizar de las siguientes maneras:

- `SIGNING`: Para firmar mensajes AS2
- `ENCRYPTION`: Para cifrar mensajes AS2
- `TLS`: Para proteger las comunicaciones AS2 enviadas a través de HTTPS

Tipo: cadena

Valores válidos: `SIGNING | ENCRYPTION`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedConnector

Devuelve los detalles del conector especificado.

Contenido

Arn

Es el nombre de recurso de Amazon (ARN) del conector específico.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: no

ConnectorId

Un identificador único para el conector.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `c-([0-9a-f]{17})`

Obligatorio: no

Url

La URL del punto de conexión de AS2 o SFTP del socio.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 255 caracteres.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedExecution

Devuelve las propiedades de la ejecución especificada.

Contenido

ExecutionId

Un identificador único para la ejecución del flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 36.

Patrón: `[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

Obligatorio: no

InitialFileLocation

Estructura que describe la ubicación de los archivos de Amazon S3 o de EFS. Esta es la ubicación del archivo cuando comienza la ejecución: si el archivo se está copiando, es la ubicación inicial (y no la de destino).

Tipo: objeto FileLocation

Obligatorio: no

ServiceMetadata

Un objeto contenedor para los detalles de la sesión asociados a un flujo de trabajo.

Tipo: objeto ServiceMetadata

Obligatorio: no

Status

El estado es uno de la ejecución de trabajo. Puede estar en curso, completarse, encontrarse una excepción o estar gestionando la excepción.

Tipo: cadena

Valores válidos: `IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedHostKey

Devuelve las propiedades de la clave de host especificada.

Contenido

Arn

El nombre de recurso de Amazon (ARN) único de la llave de host.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

DateImported

Fecha en la que se agregó la clave del host al servidor.

Tipo: marca temporal

Obligatorio: no

Description

La descripción actual de la clave de host. Puede cambiarla llamando a la operación de `UpdateHostKey` y proporcionando una nueva descripción.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 200 caracteres.

Patrón: `[\p{Print}]*`

Obligatorio: no

Fingerprint

La huella digital de la clave pública, que es una secuencia corta de bytes que se utiliza para identificar la clave pública más larga.

Tipo: cadena

Requerido: no

HostKeyId

Un identificador único para la clave de host.

Tipo: cadena

Limitaciones de longitud: longitud fija de 25.

Patrón: `hostkey-[0-9a-f]{17}`

Obligatorio: no

Type

El algoritmo de cifrado que se utiliza para la clave de host. El parámetro `Type` se especifica mediante uno de los siguientes valores:

- `ssh-rsa`
- `ssh-ed25519`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedProfile

Devuelve las propiedades del perfil que se especificó.

Contenido

Arn

El nombre de recurso de Amazon (ARN) del perfil especificado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: no

As2Id

El `As2Id` es el nombre AS2, tal como se define en RFC 4130. Para las transferencias entrantes, este es el encabezado `AS2-From` de los mensajes AS2 enviados por el socio. Para los conectores de salida, este es el encabezado `AS2-To` de los mensajes AS2 enviados al socio mediante la operación `StartFileTransfer` de la API. Este ID no puede incluir espacios.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `[\p{Print}\s]*`

Obligatorio: no

ProfileId

Un identificador único para el perfil local o socio de AS2.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `p-([0-9a-f]{17})`

Obligatorio: no

ProfileType

Indica si se deben enumerar solo los perfiles de tipo `LOCAL` o solo los perfiles de tipo `PARTNER`. Si no se proporciona en la solicitud, el comando muestra todos los tipos de perfiles.

Tipo: cadena

Valores válidos: `LOCAL | PARTNER`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedServer

Devuelve las propiedades de un servidor habilitado para el protocolo de File Transfer que se especificó.

Contenido

Arn

Especifica el nombre de recurso de Amazon (ARN) único de un servidor que se va a incluir en la lista.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

Domain

Especifica el dominio del sistema de almacenamiento que se utiliza para las transferencias de archivos. Hay dos dominios disponibles: Amazon Simple Storage Service (Amazon S3) y Amazon Elastic File System (Amazon EFS). El valor predeterminado es S3.

Tipo: cadena

Valores válidos: `S3 | EFS`

Obligatorio: no

EndpointType

Especifica el tipo de punto de conexión de VPC al que esté conectado su servidor. Si su servidor está conectado a un punto de conexión de VPC, su servidor no será accesible a través de la Internet pública.

Tipo: cadena

Valores válidos: `PUBLIC | VPC | VPC_ENDPOINT`

Obligatorio: no

IdentityProviderType

El modo de autenticación de un servidor. El valor predeterminado es`SERVICE_MANAGED`, que le permite almacenar y acceder a las credenciales de usuario dentro del AWS Transfer Family servicio.

Úselo `AWS_DIRECTORY_SERVICE` para proporcionar acceso a los grupos de Active Directory AWS Directory Service for Microsoft Active Directory o a Microsoft Active Directory en su entorno local o AWS mediante AD Connector. Esta opción también requiere que se especifique el ID del directorio mediante el parámetro `IdentityProviderDetails`.

Utilice el valor `API_GATEWAY` para la integración con un proveedor de identidades de su elección. La configuración de `API_GATEWAY` requiere que proporcione un punto de conexión de Amazon API Gateway para solicitar la autenticación mediante el parámetro `IdentityProviderDetails`.

Usa el `AWS_LAMBDA` valor para usar directamente una AWS Lambda función como proveedor de identidades. Si elige este valor, debe especificar el ARN de la función de Lambda en el parámetro `Function` para el tipo de datos de `IdentityProviderDetails`.

Tipo: cadena

Valores válidos: `SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA`

Obligatorio: no

LoggingRole

El nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que permite a un servidor activar el CloudWatch registro de Amazon para Amazon S3 o Amazon EFSEvents. Cuando esté configurado, podrá ver la actividad de los usuarios en sus registros. CloudWatch

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

ServerId

Especifica el identificador único asignado por el sistema para los servidores que figuraban en la lista.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: no

State

Estado del servidor que se describió. Un valor de `ONLINE` indica que el servidor puede aceptar trabajos y transferir archivos. Un valor `State` de `OFFLINE` significa que el servidor no puede realizar operaciones de File Transfer.

Los estados de `STARTING` y `STOPPING` indican que el servidor se encuentra en un estado intermedio; es decir, que no puede responder por completo o que no está completamente desconectado. Los valores de `START_FAILED` o `STOP_FAILED` pueden indicar una condición de error.

Tipo: cadena

Valores válidos: `OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED`

Obligatorio: no

UserCount

Especifica el número de usuarios que están asignados a un servidor que especificó con el `ServerId`.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedUser

Devuelve las propiedades del usuario que especifique.

Contenido

Arn

Proporciona el Nombre de Recurso de Amazon (ARN) único para el usuario del que desea obtener información.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: sí

HomeDirectory

Directorio de destino (carpeta) de un usuario cuando inicia sesión en el servidor a través del cliente.

Un ejemplo de `HomeDirectory` es `/bucket_name/home/mydirectory`.

> **Note**
>
> El parámetro `HomeDirectory` solo se utiliza si `HomeDirectoryType` está establecido en `PATH`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `(|/.*)`

Obligatorio: no

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

la ruta absoluta 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 `HomeDirectoryMappings` que correspondan con la forma en que quiere que las rutas de acceso de Amazon S3 o de Amazon EFS sean visibles para sus usuarios.

> **Note**
>
> Si `HomeDirectoryType` es `LOGICAL`, debe proporcionar las asignaciones mediante el parámetro `HomeDirectoryMappings`. Si, por el contrario, `HomeDirectoryType` es `PATH`, se proporciona una ruta absoluta mediante el parámetro `HomeDirectory`. No puede tener `HomeDirectory` y `HomeDirectoryMappings` en su plantilla.

Tipo: cadena

Valores válidos: `PATH | LOGICAL`

Obligatorio: no

Role

El nombre del recurso de Amazon (ARN) del rol AWS Identity and Access Management (IAM) que controla el acceso de los usuarios al bucket de Amazon S3 o al sistema de archivos Amazon 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.

> **Note**
>
> El rol de IAM que controla el acceso de los usuarios al bucket de Amazon S3 para los servidores con `Domain=S3` o al sistema de archivos EFS para los servidores con `Domain=EFS`.
>
> Las políticas asociadas con este rol determinarán el nivel de acceso que desea ofrecer a los usuarios cuando se transfieran archivos dentro y fuera de su bucket de S3 o de los sistemas de archivos de EFS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

SshPublicKeyCount

Especifica el número de claves públicas de SSH almacenadas para el usuario que especificó.

Tipo: entero

Obligatorio: no

UserName

Especifica el nombre del usuario cuyo ARN se especificó. Los nombres de usuario se utilizan con fines de autenticación.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ListedWorkflow

Contiene el identificador, la descripción de texto y el nombre de recurso de Amazon (ARN) para el flujo de trabajo.

Contenido

Arn

Especifica el nombre de recurso de Amazon (ARN) único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 1600 caracteres.

Patrón: `arn:\S+`

Obligatorio: no

Description

Especifica la descripción del texto del flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `[\w- ]*`

Obligatorio: no

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

LoggingConfiguration

Consta de el rol de registro y el nombre del grupo de registro.

Contenido

LoggingRole

El nombre de recurso de Amazon (ARN) de la función AWS Identity and Access Management (IAM) que permite a un servidor activar el CloudWatch registro de Amazon para Amazon S3 o Amazon EFSEvents. Cuando esté configurado, podrá ver la actividad de los usuarios en sus registros. CloudWatch

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: no

LogGroupName

El nombre del grupo de CloudWatch registro del AWS Transfer Family servidor al que pertenece este flujo de trabajo.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es 512.

Patrón: `[\.\-_/#A-Za-z0-9]*`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

PosixProfile

La identidad POSIX completa, incluido el ID de usuario (`Uid`), el ID de grupo (`Gid`) y cualquier ID de grupo secundario (`SecondaryGids`) 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.

Contenido

Gid

El ID de grupo POSIX utilizado para todas las operaciones EFS de este usuario.

Tipo: largo

Rango válido: valor mínimo de 0. Valor máximo de 4294967295.

Obligatorio: sí

Uid

El ID de usuario POSIX utilizado para todas las operaciones de EFS de este usuario.

Tipo: largo

Rango válido: valor mínimo de 0. Valor máximo de 4294967295.

Obligatorio: sí

SecondaryGids

Los ID de grupo POSIX secundarios utilizados para todas las operaciones de EFS de este usuario.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 16 elementos.

Rango válido: valor mínimo de 0. Valor máximo de 4294967295.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ProtocolDetails

La configuración de protocolo configurados para su servidor.

Contenido

As2Transports

Indica el método de transporte de los mensajes de AS2. Actualmente, solo se admite HTTP.

Tipo: matriz de cadenas

Miembros de la matriz: número fijo de 1 elemento.

Valores válidos: `HTTP`

Obligatorio: no

PassiveIp

Indica el modo pasivo para los protocolos FTP y FTPS. Ingrese una sola dirección IPv4, como la dirección IP pública de un cortafuegos, un enrutador o un equilibrador de carga. Por ejemplo:

```
aws transfer update-server --protocol-details PassiveIp=0.0.0.0
```

Reemplace `0.0.0.0` en el ejemplo anterior con la dirección IP real que desea utilizar.

> **Note**
>
> Si cambia el valor `PassiveIp`, debe detener y reiniciar el servidor de Transfer Family para que el cambio tenga efecto. Para obtener más información sobre el uso del modo pasivo (PASV) en un entorno NAT, consulte Configuración del servidor FTPS detrás de un firewall o NAT con. AWS Transfer Family

Valores especiales

`AUTO` y `0.0.0.0` son valores especiales para el parámetro `PassiveIp`. El valor `PassiveIp=AUTO` se asigna de forma predeterminada a los servidores de tipo FTP y FTPS. En este caso, el servidor responde automáticamente con una de las IP de punto de conexión dentro de la respuesta PASV. `PassiveIp=0.0.0.0` tiene una aplicación más exclusiva para su uso. Por ejemplo, si tiene un entorno de equilibrador de carga de red (NLB) de alta disponibilidad (HA), en el que tiene 3 subredes, solo puede especificar una dirección IP mediante el parámetro

`PassiveIp`. Esto reduce la eficacia de tener una alta disponibilidad. En este caso, puede especificar `PassiveIp=0.0.0.0`. Esto indica al cliente que utilice la misma dirección IP que la conexión de control y que utilice todas las zonas de disponibilidad para sus conexiones. Sin embargo, tenga en cuenta que no todos los clientes FTP admiten la `PassiveIp=0.0.0.0` respuesta. FileZilla y WinSCP sí lo admite. Si está utilizando otros clientes, compruebe si su cliente admite la respuesta `PassiveIp=0.0.0.0`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 15.

Obligatorio: no

SetStatOption

Utilice `SetStatOption` para ignorar el error que se genera cuando el cliente intenta usar `SETSTAT` en un archivo que carga en un bucket de S3.

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.

Establezca el valor en `ENABLE_NO_OP` para que el servidor de Transfer Family ignore el comando `SETSTAT` y cargue archivos sin necesidad de hacer ningún cambio en su cliente SFTP. Si bien la `SetStatOption` `ENABLE_NO_OP` configuración ignora el error, genera una entrada de registro en Amazon CloudWatch Logs para que pueda determinar cuándo el cliente está realizando una `SETSTAT` llamada.

> **Note**
>
> Si desea conservar la marca temporal original del archivo y modificar otros de sus atributos mediante `SETSTAT`, puede utilizar Amazon EFS como el almacenamiento de backend con Transfer Family.

Tipo: cadena

Valores válidos: `DEFAULT | ENABLE_NO_OP`

Obligatorio: no

TlsSessionResumptionMode

Propiedad utilizada con los servidores de Transfer Family que utilizan el protocolo FTPS. La reanudación de la sesión TLS proporciona un mecanismo para reanudar o compartir una clave secreta negociada entre el control y la conexión de datos de una sesión de FTPS. `TlsSessionResumptionMode` determina si el servidor reanuda o no las sesiones negociadas recientes mediante un identificador de sesión único. Este establecimiento está disponible en las llamadas `CreateServer` y `UpdateServer`. Si un valor `TlsSessionResumptionMode` no se especifica durante `CreateServer`, se establece en `ENFORCED` de forma predeterminada.

- `DISABLED`: el servidor no procesa las solicitudes del cliente de reanudación de la sesión TLS y crea una nueva sesión TLS para cada solicitud.
- `ENABLED`: el servidor procesa y acepta clientes que realizan la reanudación de la sesión TLS. El servidor no rechaza las conexiones de datos del cliente que no realizan el procesamiento del cliente de reanudación de la sesión TLS.
- `ENFORCED`: el servidor procesa y acepta clientes que realizan la reanudación de la sesión TLS. El servidor rechaza las conexiones de datos del cliente que no realizan el procesamiento del cliente de reanudación de la sesión TLS. Antes de establecer el valor en `ENFORCED`, ponga a prueba a sus clientes.

> **Note**
>
> No todos los clientes FTPS reanudan la sesión TLS. Por lo tanto, si decide imponer la reanudación de la sesión TLS, evitará cualquier conexión de clientes FTPS que no realicen la negociación del protocolo. Para determinar si puede utilizar o no el valor `ENFORCED`, debe poner a prueba a sus clientes.

Tipo: cadena

Valores válidos: `DISABLED | ENABLED | ENFORCED`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

S3FileLocation

Especifica los detalles de la ubicación del archivo que se está utilizando en el flujo de trabajo. Solo se aplica si utiliza el almacenamiento S3.

Contenido

Bucket

Especifica el bucket de S3 que contiene el archivo que se utiliza.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 63 caracteres.

Patrón: `[a-z0-9][\.\-a-z0-9]{1,61}[a-z0-9]`

Obligatorio: no

Etag

La etiqueta de entidad es un hash del objeto. La ETag solo refleja los cambios en el contenido de un objeto, no en sus metadatos.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 65536.

Patrón: `.+`

Obligatorio: no

Key

El nombre asignado al archivo cuando se creó en Amazon S3. La clave de objeto se utiliza para recuperar el objeto.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `[\P{M}\p{M}]*`

Obligatorio: no

VersionId

Especifica la versión del archivo.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1024 caracteres.

Patrón: `.+`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

S3InputFileLocation

Especifica la ubicación del archivo Amazon S3 introducido por el cliente. Si se usa en el interior de `copyStepDetails.DestinationFileLocation`, debe ser el destino de la copia de S3.

Tiene que proporcionar el bucket y la clave. La clave puede representar una ruta o un archivo. Esto se determina si se finaliza o no el valor de la clave con el carácter de la barra diagonal (/). Si el último carácter es “/”, el archivo se copia en la carpeta, y su nombre no cambia. Si, por el contrario, el último carácter es alfanumérico, se cambiará el nombre del archivo cargado al valor de la ruta. En este caso, si ya existe un archivo con ese nombre, se sobrescribe.

Por ejemplo, si la ruta es `shared-files/bob/`, los archivos cargados se copian en la carpeta `shared-files/bob/`. Si la ruta es `shared-files/today`, cada archivo cargado se copia en la carpeta `shared-files` y se le asigna un nombre `today`: cada carga sobrescribe la versión anterior del archivo bob.

Contenido

Bucket

Especifica el bucket de S3 para el archivo de entrada del cliente.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 63 caracteres.

Patrón: `[a-z0-9][\.\-a-z0-9]{1,61}[a-z0-9]`

Obligatorio: no

Key

El nombre asignado al archivo cuando se creó en Amazon S3. La clave de objeto se utiliza para recuperar el objeto.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `[\P{M}\p{M}]*`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

S3StorageOptions

Las opciones de almacenamiento de Amazon S3 configuradas para su servidor.

Contenido

DirectoryListingOptimization

Especifica si el rendimiento de los directorios de Amazon S3 está optimizado o no. Esta opción está deshabilitada de forma predeterminada.

De forma predeterminada, las asignaciones de los directorios principales tienen un `TYPE` valor de. `DIRECTORY` Si habilita esta opción, tendrá que establecerla de forma explícita `FILE` si `HomeDirectoryMapEntry` `Type` desea que la asignación tenga un destino de archivo.

Tipo: cadena

Valores válidos: `ENABLED | DISABLED`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

S3Tag

Especifica el par clave-valor que se asigna a un archivo durante la ejecución de un paso de etiquetado.

Contenido

Key

El nombre que se ha asignado a la etiqueta que ha creado.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `([\p{L}\p{Z}\p{N}_.:/=+\-@]*)`

Obligatorio: sí

Value

El valor que corresponde a la clave.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `([\p{L}\p{Z}\p{N}_.:/=+\-@]*)`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ServiceMetadata

Un objeto contenedor para los detalles de la sesión asociados a un flujo de trabajo.

Contenido

UserDetails

El ID de servidor (`ServerId`), el ID de sesión (`SessionId`) y el usuario (`UserName`) forman el `UserDetails`.

Tipo: objeto UserDetails

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

SftpConnectorConfig

Contiene los detalles de un objeto conector SFTP. El objeto conector se utiliza para transferir archivos desde y hacia el servidor SFTP de un socio.

> **Note**
>
> Como el tipo de `SftpConnectorConfig` datos se utiliza tanto para crear como para actualizar los conectores SFTP, `TrustedHostKeys` sus parámetros `UserSecretId` están marcados como no obligatorios. Esto es un poco engañoso, ya que no son necesarios cuando se actualiza un conector SFTP existente, pero sí cuando se crea un conector SFTP nuevo.

Contenido

TrustedHostKeys

La parte pública de la clave o claves de host que se utilizan para identificar el servidor externo al que se está conectando. Puede utilizar el comando `ssh-keyscan` en el servidor SFTP para recuperar la clave necesaria.

Los tres elementos del formato de la clave pública SSH estándar son `<key type>`, `<body base64>` y uno opcional, `<comment>`, con espacios entre cada elemento. Especifique únicamente `<key type>` y `<body base64>`: no introduzca la `<comment>` parte de la clave.

Para la clave de host de confianza, AWS Transfer Family acepta las claves RSA y ECDSA.

- En el caso de las claves RSA, la cadena `<key type>` es `ssh-rsa`.
- En el caso de las claves ECDSA, la cadena `<key type>` es `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384`, o `ecdsa-sha2-nistp521`, según el tamaño de la clave que haya generado.

Ejecute este comando para recuperar la clave de host del servidor SFTP, donde está el nombre del servidor SFTP. `ftp.host.com`

```
ssh-keyscan ftp.host.com
```

Esto imprime la clave de host público en la salida estándar.

```
ftp.host.com ssh-rsa AAAAB3Nza...<long-string-for-public-key
```

Copia y pega esta cadena en el `TrustedHostKeys` campo del `create-connector` comando o en el campo Trusted host keys de la consola.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 2048 caracteres.

Obligatorio: no

UserSecretId

El identificador del secreto (en AWS Secrets Manager) que contiene la clave privada, la contraseña o ambas del usuario de SFTP. El identificador debe ser el nombre de recurso de Amazon (ARN) del secreto.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 2048 caracteres.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

SshPublicKey

Proporciona información acerca de la clave Secure Shell (SSH) pública asociada a una cuenta de usuario para el servidor específico habilitado para protocolo de File Transfer (identificada mediante `ServerId`). La información devuelta incluye la fecha en que se importó clave, el contenido de la clave pública y el ID de la clave pública Los usuarios pueden almacenar más de una clave pública SSH asociada con su nombre de usuario en un servidor específico.

Contenido

DateImported

Especifica la fecha en la que se agregó la clave pública al usuario Transfer Family.

Tipo: marca temporal

Obligatorio: sí

SshPublicKeyBody

Especifica el contenido de la clave pública SSH según lo especificado por el `PublicKeyId`.

AWS Transfer Family acepta claves RSA, ECDSA y ED25519.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Obligatorio: sí

SshPublicKeyId

Especifica el parámetro `SshPublicKeyId` que contiene el identificador de la clave pública.

Tipo: cadena

Limitaciones de longitud: longitud fija de 21.

Patrón: `key-[0-9a-f]{17}`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los SDK específicos del idioma AWS , consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Tag

Crea un par clave-valor para un recurso específico. Las etiquetas son metadatos que usted puede utilizar para buscar y agrupar un recurso con diferentes objetivos. Puede aplicar etiquetas a servidores, usuarios y roles. Una clave de etiqueta puede tener más de un valor. Por ejemplo, para agrupar servidores con fines contables, puede crear una etiqueta llamada `Group` y asignar los valores `Research` y `Accounting` a ese grupo.

Contenido

Key

El nombre que se ha asignado a la etiqueta que ha creado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 128 caracteres.

Obligatorio: sí

Value

Contiene uno o más valores que ha asignado al nombre de clave que usted ha creado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

TagStepDetails

Cada tipo de paso tiene su propia estructura `StepDetails`.

Los pares clave/valor que se utilizan para etiquetar un archivo durante la ejecución de un paso del flujo de trabajo.

Contenido

Name

El nombre del paso, que se utiliza como identificador.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 30.

Patrón: `[\w-]*`

Obligatorio: no

SourceFileLocation

Especifica qué archivo utilizar como entrada en el paso del flujo de trabajo: ya sea el resultado del paso anterior o el archivo cargado originalmente para el flujo de trabajo.

- Para usar el archivo anterior como entrada, introduzca `${previous.file}`. En este caso, este paso del flujo de trabajo utiliza como entrada el archivo de salida del paso anterior del flujo de trabajo. Este es el valor predeterminado.
- Para usar la ubicación del archivo cargado originalmente como entrada para este paso, introduzca `${original.file}`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `\$\{(\w+.)+\w+\}`

Obligatorio: no

Tags

Matriz que contiene de 1 a 10 pares clave/valor.

Tipo: Matriz de S3Tag objetos

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 10 artículos.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

UserDetails

Especifica el nombre de usuario, el ID del servidor y el ID de sesión de un flujo de trabajo.

Contenido

ServerId

Identificador único asignado por el sistema para una instancia del servidor Transfer.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `s-([0-9a-f]{17})`

Obligatorio: sí

UserName

Una cadena única que identifica un usuario Transfer Family asociado a un servidor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 100 caracteres.

Patrón: `[\w][\w@.-]{2,99}`

Obligatorio: sí

SessionId

Identificador único asignado por el sistema para una sesión que corresponde al flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. La longitud máxima es de 32 caracteres.

Patrón: `[\w-]*`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

WorkflowDetail

Especifica el ID del flujo de trabajo que se va a asignar y el rol de ejecución que se utiliza para ejecutar el flujo de trabajo.

Además de un flujo de trabajo que se ejecuta cuando un archivo se carga por completo, `WorkflowDetails` también puede contener un ID de flujo de trabajo (y un rol de ejecución) para que un flujo de trabajo se ejecute en una carga parcial. Se produce una carga parcial si la sesión de servidor se desconecta mientras se está cargando el archivo.

Contenido

ExecutionRole

Incluye los permisos necesarios para las operaciones de S3, EFS y Lambda que Transfer puede asumir, de modo que todos los pasos del flujo de trabajo puedan operar en los recursos necesarios

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `arn:.*role/\S+`

Obligatorio: sí

WorkflowId

Un identificador único para el flujo de trabajo.

Tipo: cadena

Limitaciones de longitud: longitud fija de 19.

Patrón: `w-([a-z0-9]{17})`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

WorkflowDetails

Contenedor del tipo de datos `WorkflowDetail`. Lo utilizan las acciones que activan un flujo de trabajo para iniciar la puesta en marcha.

Contenido

OnPartialUpload

Un disparador que inicia un flujo de trabajo si un archivo se carga solo de forma parcial. Puede adjuntar un flujo de trabajo a un servidor que se ejecute siempre que haya una carga parcial.

Se produce una carga parcial si un archivo está abierto cuando se desconecta la sesión.

> **Note**
>
> `OnPartialUpload`puede contener un máximo de un `WorkflowDetail` objeto.

Tipo: matriz de objetos WorkflowDetail

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Obligatorio: no

OnUpload

Un desencadenador que inicia un flujo de trabajo: el flujo de trabajo se comienza a poner en marcha después de cargar un archivo.

Para eliminar un flujo de trabajo asociado de un servidor, puede proporcionar un objeto `OnUpload` vacío, tal y como se muestra en el siguiente ejemplo.

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details '{"OnUpload":[]}'
```

> **Note**
>
> `OnUpload`puede contener un máximo de un `WorkflowDetail` objeto.

Tipo: matriz de objetos WorkflowDetail

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 1 elemento.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

WorkflowStep

El componente básico de un flujo de trabajo.

Contenido

CopyStepDetails

Detalles de un paso que realiza una copia de un archivo.

Consta de los siguientes valores:

- Una descripción
- Una ubicación de Amazon S3 para el destino de la copia del archivo.
- Un indicador que indica si se sobrescribirá un archivo existente con el mismo nombre. El valor predeterminado es `FALSE`.

Tipo: objeto CopyStepDetails

Obligatorio: no

CustomStepDetails

Detalles de un paso que invoca una AWS Lambda función.

Consiste en el nombre de la función de Lambda, el destino y el tiempo de espera (en segundos).

Tipo: objeto CustomStepDetails

Obligatorio: no

DecryptStepDetails

Detalles de un paso que descifra un archivo cifrado.

Consta de los siguientes valores:

- Indique un nombre descriptivo
- Ubicación de Amazon S3 o Amazon Elastic File System (Amazon EFS) para que se descifre el archivo de origen.
- Una ubicación de Amazon S3 o EFD para el destino de la copia del archivo.
- Un indicador que señala si se sobrescribirá un archivo existente con el mismo nombre. El valor predeterminado es `FALSE`.
- El tipo de clave que se utiliza para el cifrado. Actualmente, solo se permite el cifrado con PGP.

Tipo: objeto DecryptStepDetails

Obligatorio: no

DeleteStepDetails

Detalles de un paso que elimina el archivo.

Tipo: objeto DeleteStepDetails

Obligatorio: no

TagStepDetails

Detalles de un paso que crea una o varias etiquetas.

También especifica una o varias etiquetas. Cada etiqueta contiene un par clave-valor.

Tipo: objeto TagStepDetails

Obligatorio: no

Type

Actualmente, se admiten los siguientes tipos de pasos:

- **`COPY`** : copiar el archivo en otra ubicación.
- **`CUSTOM`**- Realice un paso personalizado con un objetivo de AWS Lambda función.
- **`DECRYPT`** : descifrar un archivo que se cifró antes de subir.
- **`DELETE`** : eliminar el archivo.
- **`TAG`** : agregar una etiqueta al archivo.

Tipo: cadena

Valores válidos: `COPY | CUSTOM | TAG | DELETE | DECRYPT`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

Realizar solicitudes a la API

Además de utilizar la consola, puede utilizar la API de AWS Transfer Family para configurar y administrar sus servidores mediante programación. En esta sección se describen las operaciones de AWS Transfer Family, la solicitud de formas para la autenticación y la administración de errores. Para obtener más información acerca de las regiones y los puntos de conexión disponibles para Transfer Family, consulte AWS Transfer FamilyPuntos de conexión y cuotas en la Referencia general de AWS

> **Note**
>
> También puede utilizar los AWS SDK cuando desarrolle 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.

Temas

- Cabeceras de solicitud obligatorias para Transfer Family
- Entrada y firma de la solicitud de Transfer Family
- Respuestas de error
- Bibliotecas disponibles

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.

En el siguiente ejemplo, se muestran los encabezados que se utilizan en la operación ListServers.

```
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 siguientes que comienzan con "x-amz" son encabezados específicos para AWS. El resto de los encabezados que se muestran son encabezados comunes utilizados en transacciones HTTP.

Encabezado	Descripción
`Authorization`	Se requiere el encabezado de autorización. El formato es la firma de solicitud Sigv4 estándar, que se documenta en la sección Firmar solicitudes en la API de AWS.
`Content-Type`	Utiliza `application/x-amz-json-1.1` como tipo de contenido para todas las solicitudes a Transfer Family. `Content-Type: application/x-amz-json-1.1`
`Host`	Utilice el encabezado de host para especificar el punto de conexión de Transfer Family donde desea enviar la solicitud. Por ejemplo, `transfer.us-east-1.amazonaws.com` es el punto de conexión para la región Este de EE. UU. (Ohio). Para obtener más informaci ón acerca de las regiones y los puntos de conexión disponibles para Transfer Family, consulte AWS Transfer Family Puntos de conexión y cuotas de Referencia general de AWS. `Host: transfer.` *region*`.amazonaws.com`

Encabezado	Descripción
`x-amz-date`	Debe proporcionar la marca temporal que figura en el encabezado HTTP `Date`, o en el encabezado AWS `x-amz-date` . (Algunas bibliotecas de cliente HTTP no permiten configurar el encabezado `Date`). Cuando hay un encabezado `x-amz-date` presente, Transfer Family hace caso omiso de cualquier encabezado `Date` durante la autenticación de la solicitud. El formato `x-amz-date` debe ser ISO8601 con el formato AAAAMMDD'T'HHMMSS'Z'. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	Este encabezado especifica la versión de la API y la operación que se está solicitando. Los valores de encabezado de destino se forman concatenando la versión de la API con el nombre de la API y están en el siguiente formato. `x-amz-target: TransferService. operationName` El valor OperationName (por ejemplo, `ListServers`) se encuentra en la lista de API, ListServers.
`x-amz-security-token`	Este encabezado es obligatorio cuando las credenciales utilizadas para firmar la solicitud son temporales o de sesión (para obtener más información, consulte Uso de credenciales temporales con recursos de AWS en la Guía del usuario de IAM). Para obtener más información, consulte la sección Adición de la firma a la solicitud HTTP en Referencia general de Amazon Web Services para más información.

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 solicitud/respuesta de la carga útil de Transfer Family está documentada en la referencia de la API existente, por ejemplo, DescribeServer.

Transfer Family admite la autenticación mediante AWS Signature Version 4. Para obtener más información, consulta 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, puedes probar cada opción para ver cuál funciona.

Tipo: cadena

Recurso

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 al que se ha producido 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 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, código de muestra, tutoriales y otros recursos para los desarrolladores de software que prefieren crear aplicaciones usando API de un lenguaje específico en lugar de las herramientas de comandos y consulta de API. 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 para crear en AWS

Para ver las bibliotecas y código de ejemplo en todos los idiomas, consulte Código de muestra y bibliotecas.

Parámetros comunes

La siguiente lista contiene los parámetros que utilizan todas las acciones para firmar solicitudes de Signature Version 4 con una cadena de consulta. Los parámetros específicos de acción se

enumeran en el tema correspondiente a la acción. Para obtener más información sobre Signature Version 4, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Action

Las acciones que se van a realizar.

Tipo: cadena

Obligatorio: sí

Version

La versión de la API para la que está escrita la solicitud, expresada en el formato AAAA-MM-DD.

Tipo: String

Obligatorio: sí

X-Amz-Algorithm

El algoritmo de hash que utilizó para crear la solicitud de firma.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: String

Valores válidos: `AWS4-HMAC-SHA256`

Obligatorio: condicional

X-Amz-Credential

El valor del ámbito de la credencial, que es una cadena que incluye la clave de acceso, la fecha, la región a la que se dirige, el servicio que solicita y una cadena de terminación (“aws4_request”). El valor se expresa en el siguiente formato: access_key/AAAAMMDD/region/service/aws4_request.

Para obtener más información, consulte Crear una solicitud API de AWS firmada en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-Date

La fecha utilizada para crear la firma. El formato debe ser ISO 8601 formato básico (AAAAMMDD'T'HHMMSS'Z'). Por ejemplo, la siguiente fecha y hora es un valor válido de X-Amz-Date para `20120325T120000Z`.

Condición: X-Amz-Date es opcional en todas las solicitudes; se puede utilizar para anular la fecha empleada a fin de firmar las solicitudes. Si el encabezado Date se especifica en el formato básico ISO 8601, no se requiere X-Amz-Date. Cuando se usa X-Amz-Date, siempre anula el valor del encabezado Date. Para obtener más información, consulte Elementos de una firma de solicitud API de AWS en la Guía del usuario de IAM.

Tipo: cadena

Obligatorio: condicional

X-Amz-Security-Token

El token de seguridad temporal que se obtuvo mediante una llamada a AWS Security Token Service (AWS STS). Para obtener una lista de servicios compatibles con las credenciales de seguridad temporales de AWS STS, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Condición: si utiliza credenciales de seguridad temporales de AWS STS, debe incluir el token de seguridad.

Tipo: cadena

Obligatorio: condicional

X-Amz-Signature

Especifica la firma codificada hexadecimal que se calculó a partir de la cadena que se va a firmar y la clave de firma derivada.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-SignedHeaders

Especifica todos los encabezados HTTP que se incluyeron como parte de la solicitud canónica. Para obtener más información acerca de especificar encabezados firmados, consulte Crear una solicitud API de AWS firmada en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

Errores comunes

En esta sección, se enumeran los errores comunes a las acciones de la API de todos los servicios de AWS. En el caso de los errores específicos de una acción de la API de este servicio, consulte el tema de dicha acción de la API.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

IncompleteSignature

La firma de solicitud no se ajusta a los estándares de AWS.

Código de estado HTTP: 400

InternalFailure

El procesamiento de la solicitud ha devuelto un error debido a un error o una excepción desconocidos.

Código de estado HTTP: 500

InvalidAction

La acción u operación solicitada no es válida. Compruebe que la acción se ha escrito correctamente.

Código de estado HTTP: 400

InvalidClientTokenId

El certificado X.509 o el ID de clave de acceso de AWS proporcionado no existen en nuestros registros.

Código de estado HTTP: 403

NotAuthorized

No tiene permiso para realizar esta acción.

Código de estado HTTP: 400

OptInRequired

El ID de clave de acceso de AWS necesita una suscripción al servicio.

Código de estado HTTP: 403

RequestExpired

La solicitud llegó al servicio más de 15 minutos después de la marca de fecha en la solicitud o más de 15 minutos después de la fecha de vencimiento de la solicitud (por ejemplo, para las URL prefirmadas) o la marca de fecha de la solicitud corresponde a una hora futura en más de 15 minutos.

Código de estado HTTP: 400

ServiceUnavailable

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 503

ThrottlingException

La solicitud se denegó debido a una limitación controlada.

Código de estado HTTP: 400

ValidationError

La entrada no satisface las limitaciones que especifica un servicio de AWS.

Código de estado HTTP: 400

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: 23 de abril 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 conectore s 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 Declaraci ón 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 detalles, consulte Políticas AWS Transfer Family	5 de abril de 2024

Cambio	Descripción	Fecha
	de seguridad para conectores SFTP.	
Integre 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 detalles, consulte Gestión de Transfer Family eventos mediante 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 detalles, consulte Políticas de seguridad para servidores AWS Transfer Family.	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 informaci ón, 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 Enviar y recuperar archivos mediante un conector 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 Amazon CloudWatch inicia sesión para AWS Transfer Family.	24 de junio de 2023

Cambio	Descripción	Fecha
Soporte para múltiples métodos de autenticación	Transfer Family admite la autenticación mediante una contraseña, un par de claves público-privadas o ambos. Está disponibl e para los servidores que utilizan el protocolo SFTP y un proveedor de identidad personalizado. Para obtener más información, consulte Cree un servidor compatible con SFTP.	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 Genere y administre 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 entorno. AWS 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 Cree un servidor compatible con SFTP, Cree un servidor compatible con FTPS, o Cree un servidor compatible con FTP.	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. Anteriorm ente, tenías que proporcionar un URL Amazon API Gateway para integrar un proveedor de identidades personalizado. Para obtener más informaci ón, 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 posterior es 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 del proveedor de identidad de AWS Directory Service.	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 (Bahréin). 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 totalment e 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 aplicacio nes 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 informaci ón 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 informaci ón sobre el uso de Transfer Family en las AWS GovCloud (US) regiones, consulte AWS Transfer Familyla 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 informaci ón, consulte Políticas de seguridad para servidores AWS Transfer Family.	12 de agosto de 2020

Cambio	Descripción	Fecha
Compatibilidad con los puntos de conexión del estándar federal de procesamiento de información (FIPS).	Los puntos de conexión compatibles con FIPS ya están disponibles en las Regiones de AWS de Norteamérica. Para obtener una lista de las regiones disponibles, consulte Puntos de conexión y cuotas de AWS Transfer Family en Referencia general de AWS. Para habilitar el FIPS en un punto de conexión de servidor con SFTP, consulte Cree un servidor compatible con SFTP. Para habilitar FIPS en un punto de conexión de servidor compatible con FTPS, consulte Cree un servidor compatible con FTPS. Para habilitar FIPS en un punto de conexión de servidor con FTP, consulte Cree un servidor compatible con FTP.	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 Cree un servidor compatible con SFTP, Cree un servidor compatible con FTPS, o Cree un servidor compatible con FTP.	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 transfere ncia 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 direccion es, 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

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

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.