Guida per l'utente

AWS Transfer Family

AWS Transfer Family: Guida per l'utente

Table of Contents

Che cos'è AWS Transfer Family?

AWS Transfer Family è un servizio di trasferimento sicuro che consente di trasferire file da e verso i servizi di AWS archiviazione. Transfer Family fa parte della Cloud AWS piattaforma. AWS Transfer Family offre un supporto completamente gestito per il trasferimento di file tramite SFTP, AS2, FTPS e FTP direttamente da e verso Amazon S3 o Amazon EFS. Puoi migrare, automatizzare e monitorare senza problemi i flussi di lavoro di trasferimento dei file mantenendo le configurazioni lato client esistenti per l'autenticazione, l'accesso e i firewall, in modo che non cambi nulla per i tuoi clienti, partner e team interni o per le loro applicazioni.

AWS Per ulteriori informazioni e per iniziare a creare applicazioni cloud con Amazon Web Services, consulta la sezione Guida introduttiva.

AWS Transfer Family supporta il trasferimento di dati da o verso i seguenti servizi AWS di archiviazione.

- Archiviazione Amazon Simple Storage Service (Amazon S3). Per informazioni su Amazon S3, consulta la pagina Guida introduttiva ad Amazon Simple Storage Service.
- File system di rete NFS (Amazon Elastic File System) di Amazon Elastic File System (Amazon EFS). Per informazioni su Amazon EFS, consulta What is Amazon Elastic File System?

AWS Transfer Family supporta il trasferimento di dati tramite i seguenti protocolli:

- Secure File Transfer Protocol (SFTP): versione 3

  Il documento ufficiale IETF si trova qui: SSH File Transfer Protocol -02.txt. draft-ietf-secsh-filexfer
- Protocollo di trasferimento file sicuro (FTPS)
- Protocollo di trasferimento file (FTP)
- Dichiarazione di applicabilità 2 (AS2)

> **Note**
>
> Per le connessioni dati FTP e FTPS, l'intervallo di porte utilizzato da Transfer Family per stabilire il canale dati è 8192—8200.

I protocolli di trasferimento dei file vengono utilizzati nei flussi di lavoro per lo scambio di dati in diversi settori come i servizi finanziari, la sanità, la pubblicità e la vendita al dettaglio, tra gli altri. Transfer Family semplifica la migrazione dei flussi di lavoro di trasferimento file verso. AWS

Di seguito sono riportati alcuni casi d'uso comuni per l'utilizzo di Transfer Family con Amazon S3:

- I data lake vengono AWS utilizzati per i caricamenti da terze parti, come fornitori e partner.
- Distribuzione di dati in abbonamento con i clienti.
- I trasferimenti all'interno dell'organizzazione.

Di seguito sono riportati alcuni casi d'uso comuni per l'utilizzo di Transfer Family con Amazon EFS:

- Distribuzione dei dati
- Catena di fornitura
- Gestione dei contenuti
- Applicazioni di servizio Web

Di seguito sono riportati alcuni casi d'uso comuni per l'utilizzo di Transfer Family con AS2:

- Flussi di lavoro con requisiti di conformità che si basano sull'integrazione nel protocollo di funzionalità di protezione e sicurezza dei dati
- Logistica della catena di approvvigionamento
- Flussi di lavoro per i pagamenti
- Transazioni B usiness-to-business (B2B)
- Integrazioni con i sistemi di pianificazione delle risorse aziendali (ERP) e di gestione delle relazioni con i clienti (CRM)

Con Transfer Family, puoi accedere a un server abilitato al protocollo di trasferimento file AWS senza la necessità di eseguire alcuna infrastruttura server. È possibile utilizzare questo servizio per migrare i flussi di lavoro basati sul trasferimento di file AWS mantenendo invariati i client e le configurazioni degli utenti finali. Per prima cosa associ il tuo hostname all'endpoint del server, quindi aggiungi gli utenti e fornisci loro il giusto livello di accesso. Dopo aver eseguito questa operazione, le richieste di trasferimento degli utenti vengono gestite direttamente dall'endpoint del server Transfer Family.

Transfer Family offre i seguenti vantaggi:

- Un servizio completamente gestito scalabile in tempo reale per soddisfare le esigenze.
- Non è necessario modificare le applicazioni o eseguire alcuna infrastruttura del protocollo di trasferimento dei file.
- Con i tuoi dati nello storage durevole di Amazon S3, puoi utilizzare funzioni native Servizi AWS per l'elaborazione, l'analisi, il reporting, il controllo e l'archiviazione.
- Con Amazon EFS come archivio dati, ottieni un file system elastico completamente gestito da utilizzare con Cloud AWS servizi e risorse locali. Amazon EFS è progettato per eseguire il dimensionamento on-demand fino a svariati petabyte senza interrompere le applicazioni, aumentando e riducendo automaticamente le dimensioni man mano che aggiungi e rimuovi i file. Questo aiuta a eliminare la necessità di fornire e gestire la capacità necessaria per far fronte alla crescita.
- Un servizio di flusso di lavoro di trasferimento di file completamente gestito e senza server che semplifica la configurazione, l'esecuzione, l'automazione e il monitoraggio dell'elaborazione dei file caricati utilizzando. AWS Transfer Family
- Non ci sono costi anticipati e paghi solo per l'utilizzo del servizio.

Nelle sezioni seguenti, puoi trovare una descrizione delle diverse funzionalità di Transfer Family, un tutorial introduttivo, istruzioni dettagliate su come configurare i diversi server abilitati al protocollo, come utilizzare diversi tipi di provider di identità e il riferimento API del servizio.

Per iniziare con Transfer Family, consulta quanto segue:

- Come AWS Transfer Family funziona
- Prerequisiti
- Guida introduttiva agli endpoint del server AWS Transfer Family

Come AWS Transfer Family funziona

AWS Transfer Family è un AWS servizio completamente gestito che puoi utilizzare per trasferire file da e verso lo storage di Amazon Simple Storage Service (Amazon S3) o dai file system Amazon Elastic File System (Amazon EFS) tramite i seguenti protocolli:

- Secure File Transfer Protocol (SFTP): versione 3

  Il documento ufficiale IETF si trova qui: SSH File Transfer Protocol -02.txt. draft-ietf-secsh-filexfer
- Protocollo di trasferimento file sicuro (FTPS)

- Protocollo di trasferimento file (FTP)
- Dichiarazione di applicabilità 2 (AS2)

AWS Transfer Family supporta fino a 3 zone di disponibilità ed è supportato da una flotta ridondante con scalabilità automatica per le richieste di connessione e trasferimento. Per un esempio su come creare una maggiore ridondanza e ridurre al minimo la latenza di rete utilizzando il routing basato sulla latenza, consulta il post sul blog Minimizza la latenza di rete con il trasferimento per server SFTP. AWS

Transfer Family Managed File Transfer Workflows (MFTW) è un servizio di flusso di lavoro di trasferimento di file completamente gestito e senza server che semplifica la configurazione, l'esecuzione, l'automazione e il monitoraggio dell'elaborazione dei file caricati utilizzando. AWS Transfer Family I clienti possono utilizzare MFTW per automatizzare varie fasi di elaborazione come copia, etichettatura, scansione, filtraggio, compressione/decompressione e crittografia/decrittografia dei dati trasferiti tramite Transfer Family. Ciò fornisce una visibilità completa per il monitoraggio e la verificabilità. Per ulteriori dettagli, consulta AWS Transfer Family flussi di lavoro gestiti.

AWS Transfer Family supporta qualsiasi client di protocollo di trasferimento file standard. Alcuni client di uso comune sono i seguenti:

- OpenSSH — Un'utilità a riga di comando per Macintosh e Linux.
- WinSCP: un client grafico solo per Windows.
- Cyberduck: un client grafico per Linux, Macintosh e Microsoft Windows.
- FileZilla— Un client grafico per Linux, Macintosh e Windows.

AWS offre i seguenti workshop Transfer Family.

- Crea una soluzione di trasferimento di file che sfrutti gli endpoint SFTP/FTPS gestiti e Amazon Cognito e DynamoDB AWS Transfer Family per la gestione degli utenti. Puoi visualizzare i dettagli di questo workshop qui.
- Crea un endpoint Transfer Family con AS2 abilitato e un connettore Transfer Family AS2 Puoi visualizzare i dettagli di questo workshop qui.
- Crea una soluzione che fornisca indicazioni prescrittive e un laboratorio pratico su come creare un'architettura di trasferimento dei file scalabile e sicura AWS senza dover modificare le applicazioni esistenti o gestire l'infrastruttura del server. Puoi visualizzare i dettagli di questo workshop qui.

Post del blog pertinenti per Transfer Family

La tabella seguente elenca i post del blog che contengono informazioni utili per i clienti Transfer Family. La tabella è in ordine cronologico inverso, in modo che i post più recenti si trovino all'inizio della tabella.

Titolo e link del post del blog	Data
Progettazione di trasferimenti di file gestiti sicuri e conformi con connettori AWS Transfer Family SFTP e crittografia PGP	16 maggio 2024
Utilizzo di Amazon Cognito come provider di identità con Amazon AWS Transfer Family S3	14 maggio 2024
In che modo Transfer Family può aiutarti a creare una soluzione di trasferimento di file gestita sicura e conforme	3 gennaio 2024
Rileva le minacce di malware utilizzando AWS Transfer Family	20 luglio 2023
Estendere i carichi di lavoro SAP con AWS Transfer Family	13 luglio 2023
Crittografa e decrittografa i file con PGP e AWS Transfer Family	21 giugno 2023
Autenticazione con Azure Active Directory e AWS Transfer FamilyAWS Lambda	15 dicembre 2022
Personalizza le notifiche di consegna dei file usando flussi di lavoro gestiti AWS Transfer Family	14 ottobre 2022
Creazione di una piattaforma di trasferimento file nativa per il cloud utilizzando flussi di lavoro AWS Transfer Family	5 gennaio 2022

Titolo e link del post del blog	Data
Abilitazione della gestione delle chiavi self-service degli utenti con A e.AWS Transfer Family AWS Lambda	17 dicembre 2021
Migliora il controllo dell'accesso ai dati con AWS Transfer Family Amazon S3	5 ottobre 2021
Migliora la velocità effettiva per i trasferimenti di file tramite Internet utilizzando AWS Global Accelerator servizi e AWS Transfer Family	7 giugno 2021
Protezione AWS Transfer Family con AWS Web Application Firewall e Amazon API Gateway	5 maggio 2021
Protezione AWS Transfer Family con AWS Web Application Firewall e Amazon API Gateway	15 gennaio 2021
AWS Transfer Family supporto per Amazon Elastic File System	7 gennaio 2021
Abilita l'autenticazione tramite password per AWS Transfer Family l'utilizzo AWS Secrets Manager	5 novembre 2020
Centralizza l'accesso ai dati utilizzando AWS Transfer Family e AWS Storage Gateway	22 giugno 2020
Utilizzo di Amazon EFS per AWS Lambda le tue applicazioni serverless	18 giugno 2020
Usa l'elenco degli indirizzi IP consentiti per proteggere i tuoi server AWS Transfer Family	8 aprile 2020
Riduci al minimo la latenza di rete con il AWS trasferimento per server SFTP	19 febbraio 2020

Titolo e link del post del blog	Data
Migrazione Lift and Shift dei server SFTP su AWS	12 febbraio 2020
Semplifica la struttura AWS SFTP con chroot e directory logiche	26 settembre 2019
Usare Okta come provider di identità con AWS Transfer Family	30 maggio 2019

Prerequisiti

Le sezioni seguenti descrivono i prerequisiti richiesti per utilizzare il AWS Transfer Family servizio. Come minimo, devi creare un bucket Amazon Simple Storage Service (Amazon S3) e fornire l'accesso a quel bucket tramite AWS Identity and Access Management un ruolo (IAM). Il ruolo deve inoltre stabilire una relazione di trust. Questa relazione di fiducia consente a Transfer Family di assumere il ruolo IAM per accedere al tuo bucket in modo che possa soddisfare le richieste di trasferimento di file degli utenti.

Argomenti

AWS Regioni, endpoint e quote supportati

Per connettersi a livello di codice a un AWS servizio, si utilizza un endpoint. Ad esempio, l'endpoint per i clienti nella regione Stati Uniti orientali (Ohio) (), è. `us-east-2` `transfer.us-east-2.amazonaws.com` Le service quotas (o quote di servizio), a cui si fa riferimento anche come limiti, rappresentano il numero massimo di risorse di servizio o operazioni per l' Account AWS. In questa guida, puoi trovare le quote in e. Quote AS2 Quote per i connettori SFTP

Per ulteriori informazioni sulle AWS regioni, gli endpoint e le quote di servizio supportati, consulta AWS Transfer Family endpoint e quote nel. Riferimenti generali di Amazon Web Services

Registrati per AWS

Quando ti registri ad Amazon Web Services (AWS), il tuo AWS account viene automaticamente registrato per tutti i servizi in AWS, inclusi AWS Transfer Family. Ti vengono addebitati solo i servizi che utilizzi.

Se hai già un AWS account, passa all'attività successiva. Se non disponi di un account AWS , utilizza la seguente procedura per crearne uno.

Se non ne possiedi uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

Per informazioni sui prezzi e da utilizzare per AWS Pricing Calculator ottenere una stima del costo di utilizzo di Transfer Family, consulta AWS Transfer Family i prezzi.

Per informazioni sulla disponibilità AWS regionale, consulta gli AWS Transfer Family endpoint e le quote nel. Riferimenti generali di AWS

Configura lo storage da utilizzare con AWS Transfer Family

Questo argomento descrive le opzioni di archiviazione che è possibile utilizzare AWS Transfer Family. Puoi utilizzare Amazon S3 o Amazon EFS come storage per i server Transfer Family.

Indice

Configurazione di un bucket Amazon S3

AWS Transfer Family accede al tuo bucket Amazon S3 per soddisfare le richieste di trasferimento degli utenti, quindi devi fornire un bucket Amazon S3 come parte della configurazione del server abilitato al protocollo di trasferimento file. Puoi utilizzare un bucket esistente o crearne uno nuovo.

> **Note**
>
> Non è necessario utilizzare un server e un bucket Amazon S3 che si trovano nella stessa AWS regione, ma consigliamo questa procedura come best practice.

Quando configuri i tuoi utenti, assegni a ciascuno di loro un ruolo IAM. Questo ruolo determina il livello di accesso che hanno al tuo bucket Amazon S3.

Per informazioni sulla creazione di un nuovo bucket, vedi Come si crea un bucket S3? nella Guida per l'utente di Amazon Simple Storage Service.

> **Note**
>
> Puoi usare Amazon S3 Object Lock per impedire che gli oggetti vengano sovrascritti per un periodo di tempo fisso o indefinitamente. Funziona allo stesso modo con Transfer Family come con altri servizi. Se un oggetto esiste ed è protetto, non è consentito scriverlo o eliminarlo. Per ulteriori dettagli su Amazon S3 Object Lock, consulta Using Amazon S3 Object Lock nella Amazon Simple Storage Service User Guide.

Punti di accesso Amazon S3

AWS Transfer Family supporta Amazon S3 Access Points, una funzionalità di Amazon S3 che consente di gestire facilmente l'accesso granulare ai set di dati condivisi. Puoi utilizzare gli alias di S3 Access Point ovunque utilizzi un nome di bucket S3. Puoi creare centinaia di punti di accesso in Amazon S3 per utenti che dispongono di autorizzazioni diverse per accedere ai dati condivisi in un bucket Amazon S3.

Ad esempio, puoi utilizzare i punti di accesso per consentire a tre team diversi di accedere allo stesso set di dati condiviso, in cui un team può leggere i dati da S3, un secondo team può scrivere dati su S3 e il terzo team può leggere, scrivere ed eliminare dati da S3. Per implementare un controllo granulare

degli accessi come indicato sopra, puoi creare un punto di accesso S3 che contenga una policy che fornisca un accesso asimmetrico a diversi team. Puoi utilizzare gli access point S3 con il tuo server Transfer Family per ottenere un controllo granulare degli accessi, senza creare una complessa policy sui bucket S3 che copra centinaia di casi d'uso. Per ulteriori informazioni su come utilizzare gli access point S3 con un server Transfer Family, consulta il post di blog Enhance data access control with AWS Transfer Family and Amazon S3.

> **Note**
>
> AWS Transfer Family attualmente non supporta punti di accesso multiregionali Amazon S3.

Comportamento di Amazon S3 HeadObject

> **Note**
>
> Quando crei o aggiorni un server Transfer Family, puoi ottimizzare le prestazioni per le tue directory Amazon S3, eliminando le chiamate. `HeadObject`

In Amazon S3 bucket e oggetti sono le risorse primarie e gli oggetti sono archiviati nei bucket. Amazon S3 può simulare un file system gerarchico, ma a volte può comportarsi in modo diverso rispetto a un file system tipico. Ad esempio, le directory non sono un concetto di prima classe in Amazon S3, ma si basano invece su chiavi oggetto. AWS Transfer Family deduce il percorso di una directory dividendo la chiave di un oggetto con il carattere barra (/), trattando l'ultimo elemento come nome del file, quindi raggruppando i nomi di file che hanno lo stesso prefisso nello stesso percorso. Gli oggetti a byte zero vengono creati per rappresentare il percorso di una cartella quando crei una directory vuota utilizzando `mkdir` o utilizzando la console Amazon S3. La chiave per questi oggetti termina con una barra finale. Questi oggetti a zero byte sono descritti in Organizing objects in the Amazon S3 console using folders nella Amazon S3 User Guide.

Quando esegui un `ls` comando e alcuni risultati sono oggetti Amazon S3 a zero byte (questi oggetti hanno chiavi che terminano con il carattere barra), Transfer Family invia una `HeadObject` richiesta per ciascuno di questi oggetti (consulta il riferimento all'API di Amazon HeadObjectSimple Storage Service per i dettagli). Ciò può causare i seguenti problemi quando si utilizza Amazon S3 come storage con Transfer Family.

Concedi la possibilità di scrivere ed elencare solo file

In alcuni casi, potresti voler offrire solo l'accesso in scrittura ai tuoi oggetti Amazon S3. Ad esempio, potresti voler fornire l'accesso per scrivere (o caricare) ed elencare oggetti in un bucket, ma non per leggere (scaricare) oggetti. Per eseguire `mkdir` comandi utilizzando `ls` i client di trasferimento file, devi disporre di Amazon S3 `ListObjects` e `PutObject` delle autorizzazioni. Tuttavia, quando Transfer Family deve effettuare una `HeadObject` chiamata per scrivere o elencare file, la chiamata fallisce con un errore di Accesso negato, poiché questa chiamata richiede l'`GetObject`autorizzazione.

> **Note**
>
> Quando crei o aggiorni un server Transfer Family, puoi ottimizzare le prestazioni per le tue directory Amazon S3, eliminando le chiamate. `HeadObject`

In questo caso, puoi concedere l'accesso aggiungendo una condizione di policy AWS Identity and Access Management (IAM) che aggiunge l'`GetObject`autorizzazione solo per gli oggetti che terminano con una barra (). `/` Questa condizione impedisce `GetObject` le chiamate ai file (in modo che non possano essere letti), ma consente all'utente di elencare e attraversare le cartelle. La seguente policy di esempio offre solo l'accesso in scrittura ed elenco ai bucket Amazon S3. Per utilizzare questa policy, sostituiscila *`DOC-EXAMPLE-BUCKET`* con il nome del tuo 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**
>
> Questa politica non consente agli utenti di aggiungere file. In altre parole, un utente a cui viene assegnata questa politica non può aprire file per aggiungervi contenuto o modificarli. Inoltre, se il tuo caso d'uso richiede una `HeadObject` chiamata prima di caricare un file, questa politica non funzionerà per te.

Un gran numero di oggetti a zero byte che causano problemi di latenza

Se i bucket Amazon S3 contengono un gran numero di questi oggetti a zero byte, Transfer Family emette molte chiamate, il che può causare `HeadObject` ritardi nell'elaborazione. La soluzione consigliata per questo problema è abilitare Optimized Directories per ridurre la latenza.

Si supponga, ad esempio, di accedere alla propria home directory e di disporre di 10.000 sottodirectory. In altre parole, il tuo bucket Amazon S3 ha 10.000 cartelle. In questo scenario, se si esegue il comando `ls` (list), l'operazione list richiede dai sei agli otto minuti. Tuttavia, se ottimizzi le directory, questa operazione richiede solo pochi secondi. È possibile impostare questa opzione nella schermata Configura dettagli aggiuntivi durante la procedura di creazione o aggiornamento del server. Queste procedure sono descritte in dettaglio nell'Configurazione di un endpoint server SFTP, FTPS o FTPargomento.

> **Note**
>
> I client GUI possono emettere un `ls` comando che sfugge al controllo dell'utente, quindi è importante abilitare questa impostazione, se possibile.

Se non riuscite o non riuscite a ottimizzare le vostre directory, una soluzione alternativa a questo problema consiste nell'eliminare tutti gli oggetti a zero byte. Tieni presente quanto segue:

- Le cartelle vuote non esisteranno più. Le directory esistono solo perché i loro nomi sono nella chiave di un oggetto.
- Non impedisce a qualcuno di chiamare `mkdir` e rompere nuovamente le cose. È possibile mitigare questo problema creando una politica che impedisca la creazione di directory.
- Alcuni scenari utilizzano questi oggetti da 0 byte. Ad esempio, hai una struttura come /inboxes/customer1000 e la directory della posta in arrivo viene pulita ogni giorno.

Infine, un'altra soluzione possibile è limitare il numero di oggetti visibili attraverso una condizione politica per ridurre il numero di chiamate. `HeadObject` Affinché questa sia una soluzione praticabile, devi accettare il fatto che potresti essere in grado di visualizzare solo un insieme limitato di tutte le tue sottodirectory.

Configurazione di un file system Amazon EFS

AWS Transfer Family accede ad Amazon Elastic File System (Amazon EFS) per soddisfare le richieste di trasferimento degli utenti. Pertanto, è necessario fornire un file system Amazon EFS come parte della configurazione del server abilitato al protocollo di trasferimento file. Puoi utilizzare un file system esistente o crearne uno nuovo.

Tieni presente quanto segue:

- Quando utilizzi un server Transfer Family e un file system Amazon EFS, il server e il file system devono trovarsi nello stesso sistema Regione AWS.
- Il server e il file system non devono necessariamente avere lo stesso account. Se il server e il file system non si trovano nello stesso account, la politica del file system deve fornire un'autorizzazione esplicita al ruolo utente.

  Per informazioni su come configurare più account, consulta Gestione degli AWS account nell'organizzazione nella Guida per l'AWS Organizations utente.

- Quando configuri i tuoi utenti, assegni a ciascuno di loro un ruolo IAM. Questo ruolo determina il livello di accesso che hanno al tuo file system Amazon EFS.
- Per dettagli sul montaggio di un file system Amazon EFS, consulta Mounting Amazon EFS file system.

Per ulteriori dettagli sulla collaborazione con AWS Transfer Family Amazon EFS, consulta Using AWS Transfer Family to access files in your Amazon EFS file system nella Amazon Elastic File System User Guide.

Proprietà dei file Amazon EFS

Amazon EFS utilizza il modello di autorizzazione dei file POSIX (Portable Operating System Interface) per rappresentare la proprietà dei file.

In POSIX, gli utenti del sistema sono classificati in tre classi di autorizzazione distinte: quando consenti a un utente di accedere ai file archiviati in un file system Amazon EFS utilizzando AWS Transfer Family, devi assegnargli un «profilo POSIX». Questo profilo viene utilizzato per determinare il loro accesso a file e directory nel file system Amazon EFS.

- Utente (u): proprietario del file o della directory. Di solito, il creatore di un file o di una directory ne è anche il proprietario.
- Gruppo (g): insieme di utenti che necessitano di un accesso identico ai file e alle directory che condividono.
- Altri (o): tutti gli altri utenti che hanno accesso al sistema ad eccezione del proprietario e dei membri del gruppo. Questa classe di autorizzazione viene anche chiamata «Pubblica».

Nel modello di autorizzazione POSIX, ogni oggetto del file system (file, directory, link simbolici, named pipe e socket) è associato ai tre set di permessi precedentemente menzionati. Agli oggetti Amazon EFS è associata una modalità in stile UNIX. Questo valore di modalità definisce le autorizzazioni per l'esecuzione di azioni su quell'oggetto.

Inoltre, sui sistemi in stile Unix, utenti e i gruppi sono mappati a identificatori numerici, che sono impiegati da Amazon EFS per rappresentare la proprietà dei file. Per Amazon EFS, gli oggetti sono di proprietà di un singolo proprietario e di un singolo gruppo. Amazon EFS utilizza questi ID numerici per controllare le autorizzazioni quando un utente cerca di accedere a un oggetto del file system.

Configurazione degli utenti Amazon EFS per Transfer Family

Prima di configurare gli utenti Amazon EFS, puoi eseguire una delle seguenti operazioni:

- Puoi creare utenti e configurare le loro cartelle home in Amazon EFS. Per informazioni dettagliate, vedi Configurazione degli utenti Transfer Family su Amazon EFS.
- Se ti senti a tuo agio nell'aggiungere un utente root, puoi farloCrea un utente root Amazon EFS.

> **Note**
>
> I server Transfer Family non supportano i punti di accesso Amazon EFS per impostare le autorizzazioni POSIX. I profili POSIX degli utenti di Transfer Family (descritti nella sezione precedente) offrono la possibilità di impostare i permessi POSIX. Queste autorizzazioni sono impostate a livello di utente, per un accesso granulare, in base a UID, GID e GID secondari.

Configurazione degli utenti Transfer Family su Amazon EFS

Transfer Family mappa gli utenti all'UID/GID e alle directory specificate. Se gli UID/GID/directory non esistono già in EFS, è necessario crearli prima di assegnarli in Transfer a un utente. I dettagli per la creazione di utenti Amazon EFS sono descritti in Lavorare con utenti, gruppi e autorizzazioni a livello di Network File System (NFS) nella Amazon Elastic File System User Guide.

Passaggi per configurare gli utenti Amazon EFS in Transfer Family

1. Mappa l'UID e il GID EFS per il tuo utente in Transfer Family utilizzando i `PosixProfile`campi.
2. Se desideri che l'utente inizi in una cartella specifica al momento dell'accesso, puoi specificare la directory EFS sotto il `HomeDirectory`campo.

È possibile automatizzare il processo utilizzando una CloudWatch regola e una funzione Lambda. Per un esempio di funzione Lambda che interagisce con EFS, consulta Using Amazon EFS for AWS Lambda in your serverless application.

Inoltre, puoi configurare le directory logiche per gli utenti di Transfer Family. Per i dettagli, consulta la Configurazione di directory logiche per Amazon EFS sezione dell'Utilizzo di directory logiche per semplificare le strutture di directory Transfer Familyargomento.

Crea un utente root Amazon EFS

Se la tua organizzazione ritiene opportuno abilitare l'accesso degli utenti root tramite SFTP/FTPS per la configurazione degli utenti, puoi creare un utente con UID e GID pari a 0 (utente root), quindi utilizzare quell'utente root per creare cartelle e assegnare i proprietari degli ID POSIX agli altri utenti. Il vantaggio di questa opzione è che non è necessario montare il file system Amazon EFS.

Esegui i passaggi descritti in eAggiungere utenti gestiti dal servizio Amazon EFS, sia per l'ID utente che per l'ID del gruppo, inserisci 0 (zero).

Comandi Amazon EFS supportati

I seguenti comandi sono supportati per Amazon EFS for AWS Transfer Family.

- `cd`
- `ls/dir`
- `pwd`
- `put`
- `get`
- `rename`
- `chown`: Solo i root (ovvero gli utenti con uid=0) possono modificare la proprietà e le autorizzazioni di file e directory.
- `chmod`: Solo root può modificare la proprietà e le autorizzazioni di file e directory.
- `chgrp`: Supportato sia per root che per il proprietario del file, che può solo modificare il gruppo di file in uno dei propri gruppi secondari.
- `ln -s/symlink`
- `mkdir`
- `rm/delete`
- `rmdir`
- `chmtime`

Crea un ruolo e una policy IAM

Questo argomento descrive i tipi di politiche e ruoli che è possibile utilizzare e illustra il processo di creazione di un ruolo utente. AWS Transfer Family Descrive inoltre come funzionano i criteri di sessione e fornisce un esempio di ruolo utente.

AWS Transfer Family utilizza i seguenti tipi di ruoli:

- Ruolo utente: consente agli utenti gestiti dal servizio di accedere alle risorse Transfer Family necessarie. AWS Transfer Family assume questo ruolo nel contesto dell'ARN di un utente Transfer Family.
- Ruolo di accesso: fornisce l'accesso solo ai file Amazon S3 che vengono trasferiti. Per i trasferimenti AS2 in entrata, il ruolo di accesso utilizza l'Amazon Resource Name (ARN) per l'accordo. Per i trasferimenti AS2 in uscita, il ruolo di accesso utilizza l'ARN per il connettore.
- Ruolo di chiamata: da utilizzare con Amazon API Gateway come provider di identità personalizzato del server. Transfer Family assume questo ruolo nel contesto di un ARN del server Transfer Family.
- Ruolo di registrazione: utilizzato per registrare le voci in Amazon CloudWatch. Transfer Family utilizza questo ruolo per registrare i dettagli relativi al successo e all'errore insieme alle informazioni sui trasferimenti di file. Transfer Family assume questo ruolo nel contesto di un ARN del server Transfer Family. Per i trasferimenti AS2 in uscita, il ruolo di registrazione utilizza il connettore ARN.
- Ruolo di esecuzione: consente a un utente Transfer Family di chiamare e avviare flussi di lavoro. Transfer Family assume questo ruolo nel contesto di un flusso di lavoro Transfer Family ARN.

Oltre a questi ruoli, puoi anche utilizzare i criteri di sessione. Una politica di sessione viene utilizzata per limitare l'accesso quando necessario. Tieni presente che queste politiche sono autonome: ovvero non le aggiungi a un ruolo. Piuttosto, aggiungi una politica di sessione direttamente a un utente Transfer Family.

> **Note**
>
> Quando crei un utente Transfer Family gestito dal servizio, puoi selezionare la politica di generazione automatica in base alla cartella home. Questa è una scorciatoia utile se desideri limitare l'accesso degli utenti alle proprie cartelle. Inoltre, è possibile visualizzare dettagli sulle politiche di sessione e un esempio inCome funzionano le politiche di sessione. Puoi anche trovare ulteriori informazioni sulle policy di sessione in Session policies nella IAM User Guide.

Argomenti

Creazione di un ruolo utente

Quando crei un utente, prendi una serie di decisioni sull'accesso degli utenti. Queste decisioni includono a quali bucket Amazon S3 o file system Amazon EFS l'utente può accedere, a quali parti di ogni bucket Amazon S3 e quali file nel file system sono accessibili e quali autorizzazioni dispone l'utente (ad esempio, o). `PUT` `GET`

Per impostare l'accesso, crei una politica e un ruolo basati sull'identità AWS Identity and Access Management (IAM) che forniscono tali informazioni di accesso. Come parte di questo processo, fornisci l'accesso al tuo utente al bucket Amazon S3 o al file system Amazon EFS che è la destinazione o l'origine per le operazioni sui file. A questo scopo, esegui la seguente procedura dettagliata, descritta di seguito:

Creazione di un ruolo utente

1. Crea una policy IAM per. AWS Transfer Family Ciò è descritto inPer creare una policy IAM per AWS Transfer Family.
2. Crea un ruolo IAM e allega la nuova policy IAM. Per vedere un esempio, consulta Esempio di politica di accesso in lettura/scrittura.
3. Stabilisci una relazione di fiducia tra AWS Transfer Family e il ruolo IAM. Questo è descritto inPer stabilire una relazione di trust.

Le seguenti procedure descrivono come creare una policy e un ruolo IAM.

Per creare una policy IAM per AWS Transfer Family

1. Apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, seleziona Policy e quindi Crea policy.
3. Nella pagina Create Policy (Crea policy), selezionare la scheda JSON.
4. Nell'editor visualizzato, sostituisci il contenuto dell'editor con la policy IAM che desideri allegare al ruolo IAM.

Puoi concedere l'accesso in lettura/scrittura o limitare gli utenti alla loro home directory. Per ulteriori informazioni, consulta Esempio di politica di accesso in lettura/scrittura.

5. Scegli Rivedi politica e fornisci un nome e una descrizione per la tua politica, quindi scegli Crea politica.

Quindi, crea un ruolo IAM e collegalo alla nuova policy IAM.

Per creare un ruolo IAM per AWS Transfer Family

1. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.

   Nella pagina Crea ruolo, assicurati che il AWS servizio sia selezionato.

2. Scegliere Transfer (Trasferisci) dall'elenco di servizi, quindi selezionare Next: Permissions (Successivo: Autorizzazioni). Ciò stabilisce una relazione di fiducia tra AWS Transfer Family e AWS.
3. Nella sezione Allega criteri di autorizzazione, individua e scegli la politica che hai appena creato e scegli Avanti: Tag.
4. (Facoltativo) Immettere una chiave e un valore per un tag e scegliere Next: Review (Successivo: Rivedi).
5. Nella pagina Review (Rivedi), immettere un nome e una descrizione per il nuovo ruolo, quindi scegliere Create role (Crea ruolo).

Successivamente, stabilisci una relazione di fiducia tra AWS Transfer Family e AWS.

Per stabilire una relazione di trust

> **Note**
>
> Nei nostri esempi, utilizziamo entrambi `ArnLike` e`ArnEquals`. Sono identici dal punto di vista funzionale e pertanto è possibile utilizzarli entrambi quando si creano le proprie politiche. La documentazione di Transfer Family utilizza `ArnLike` quando la condizione contiene un carattere jolly e `ArnEquals` indica una condizione di corrispondenza esatta.

1. Nella console IAM, scegliere il ruolo appena creato.

2. Nella pagina Riepilogo, scegliere Relazioni di trust e selezionare Edit trust relationship (Modifica relazione di trust).
3. Nell'editor Edit Trust Relationship, assicurati che il servizio sia **`"transfer.amazonaws.com"`** attivo. La politica di accesso è mostrata di seguito.

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

Si consiglia di utilizzare le chiavi di condizione `aws:SourceAccount` e `aws:SourceArn` per proteggersi dal problema del "confused deputy". L'account di origine è il proprietario del server e l'ARN di origine è l'ARN dell'utente. Per esempio:

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

Puoi utilizzare la `ArnLike` condizione anche se desideri limitarti a un determinato server anziché a qualsiasi server dell'account utente. Per esempio:

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

> **Note**
>
> Negli esempi precedenti, sostituisci ogni *segnaposto di input dell'utente* con le tue informazioni.

Per dettagli sul problema del vice confuso e altri esempi, vedi. Prevenzione del problema "confused deputy" tra servizi

4. Scegli Aggiorna politica di fiducia per aggiornare la politica di accesso.

Ora hai creato un ruolo IAM che consente di AWS Transfer Family chiamare AWS i servizi per tuo conto. Hai associato al ruolo la policy IAM che hai creato per consentire l'accesso al tuo utente. Nella Guida introduttiva agli endpoint del server AWS Transfer Family sezione, questo ruolo e questa policy vengono assegnati al tuo utente o ai tuoi utenti.

Consulta anche

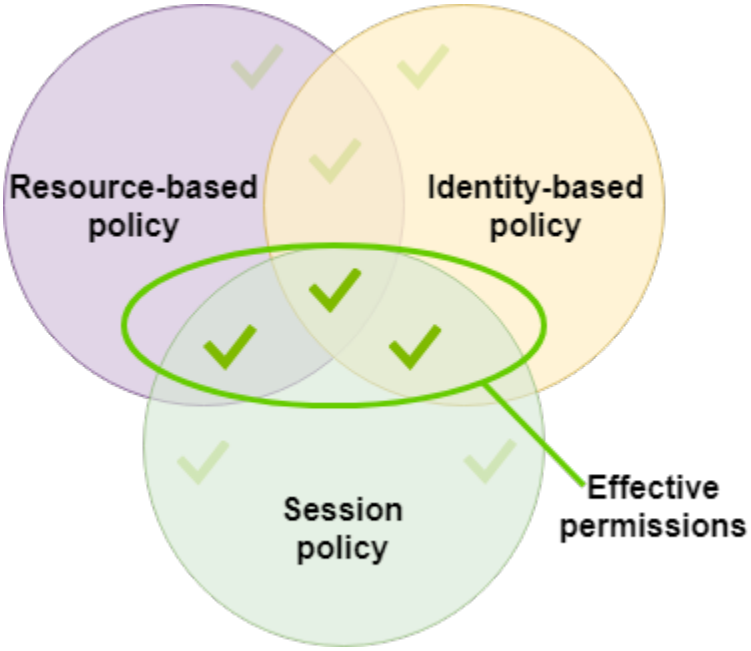
- Per informazioni più generali sui ruoli IAM, consulta Creating a role to delegate permissions to an AWS service nella IAM User Guide.
- Per ulteriori informazioni sulle politiche basate sull'identità per le risorse Amazon S3, consulta Gestione delle identità e degli accessi in Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.
- Per ulteriori informazioni sulle politiche basate sull'identità per le risorse Amazon EFS, consulta Using IAM to control data access nel file system nella Amazon Elastic File System User Guide.

Come funzionano le politiche di sessione

Quando un amministratore crea un ruolo, il ruolo spesso include ampie autorizzazioni per coprire più casi d'uso o membri del team. Se un amministratore configura l'URL di una console, può ridurre le autorizzazioni per la sessione risultante utilizzando una politica di sessione. Ad esempio, se crei un ruolo con accesso in lettura/scrittura, puoi configurare un URL che limiti l'accesso degli utenti solo alle loro home directory.

I criteri di sessione sono criteri avanzati che vengono trasmessi come parametro quando si crea a livello di codice una sessione temporanea per un ruolo o un utente. Le policy di sessione sono utili per bloccare gli utenti in modo che abbiano accesso solo alle parti del bucket in cui i prefissi degli

oggetti contengono il loro nome utente. Il diagramma seguente mostra che le autorizzazioni dei criteri di sessione sono l'intersezione tra i criteri di sessione e i criteri basati sulle risorse più l'intersezione dei criteri di sessione e i criteri basati sull'identità.



Per maggiori dettagli, consulta le politiche di sessione nella Guida per l'utente IAM.

Nel AWS Transfer Family, una policy di sessione è supportata solo durante il trasferimento da o verso Amazon S3. La seguente politica di esempio è una politica di sessione che limita l'accesso degli utenti solo alle loro home directory. Tieni presente quanto segue:

- Le `PutObjectACL` istruzioni `GetObjectACL` e sono necessarie solo se è necessario abilitare Cross Account Access. Cioè, il tuo server Transfer Family deve accedere a un bucket in un altro account.
- La lunghezza massima di una politica di sessione è di 2048 caratteri. Per maggiori dettagli, consulta il parametro Policy request per l'`CreateUser`azione nel riferimento API.
- Se il tuo bucket Amazon S3 è crittografato utilizzando AWS Key Management Service (AWS KMS), devi specificare autorizzazioni aggiuntive nella tua policy. Per informazioni dettagliate, vedi Crittografia dei dati in 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**
>
> L'esempio di policy precedente presuppone che le directory home degli utenti siano impostate in modo da includere una barra finale, a indicare che si tratta di una directory. Se, al contrario, imposti quella di un utente `HomeDirectory` senza la barra finale, dovresti includerla come parte della tua politica.

Nella politica di esempio precedente, nota l'uso dei parametri `transfer:HomeFoldertransfer:HomeBucket`, e `transfer:HomeDirectory` policy. Questi parametri sono impostati per `HomeDirectory` i parametri configurati per l'utente, come descritto in HomeDirectoryandImplementazione del metodo API Gateway. Questi parametri hanno le seguenti definizioni:

- Il `transfer:HomeBucket` parametro viene sostituito con il primo componente di`HomeDirectory`.
- Il `transfer:HomeFolder` parametro viene sostituito con le parti rimanenti del `HomeDirectory` parametro.
- Al `transfer:HomeDirectory` parametro è stata rimossa la barra anteriore (`/`) iniziale in modo che possa essere utilizzata come parte di un Amazon Resource Name (ARN) di S3 in un'istruzione. `Resource`

> **Note**
>
> Se utilizzi directory logiche, ovvero quelle dell'utente, `LOGICAL` questi parametri di policy (`HomeBucket`, e) `homeDirectoryType` non sono supportati. `HomeDirectory` `HomeFolder`

Ad esempio, supponiamo che il `HomeDirectory` parametro configurato per l'utente Transfer Family sia`/home/bob/amazon/stuff/`.

- `transfer:HomeBucket`è impostato su`/home`.
- `transfer:HomeFolder`è impostato su`/bob/amazon/stuff/`.
- `transfer:HomeDirectory`diventa`home/bob/amazon/stuff/`.

Il primo `"Sid"` consente all'utente di elencare tutte le directory a partire da`/home/bob/amazon/stuff/`.

Il secondo `"Sid"` limita l'`get`accesso dell'utente `put` e quello dello stesso percorso,. `/home/bob/amazon/stuff/`

Esempio di politica di accesso in lettura/scrittura

Concedi l'accesso in lettura/scrittura al bucket Amazon S3

La seguente politica di esempio AWS Transfer Family concede l'accesso in lettura/scrittura agli oggetti nel tuo bucket Amazon S3.

Tieni presente quanto segue:

- Sostituisci *DOC-EXAMPLE-BUCKET* con il nome del bucket Amazon S3.
- Le `PutObjectACL` istruzioni `GetObjectACL` e sono obbligatorie solo se devi abilitare Cross Account Access. Cioè, il tuo server Transfer Family deve accedere a un bucket in un altro account.
- `DeleteObjectVersion`Le istruzioni `GetObjectVersion` and sono necessarie solo se il controllo delle versioni è abilitato sul bucket Amazon S3 a cui si accede.

> **Note**
>
> Se hai già abilitato il controllo delle versioni per il tuo bucket, allora hai bisogno di queste autorizzazioni, poiché puoi solo sospendere il controllo delle versioni in Amazon S3 e non disattivarlo completamente. Per maggiori dettagli, consulta Unversioned, versioning-enabled e versioning-suspended bucket.

```
{
    "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/*"
        }
    ]
}
```

Concedi l'accesso al file system ai file nel file system Amazon EFS

> **Note**
>
> Oltre alla policy, devi anche assicurarti che le autorizzazioni dei tuoi file POSIX garantiscano l'accesso appropriato. Per ulteriori informazioni, consulta Working with users, groups, and permissions at the Network File System (NFS) Level (Utilizzo di utenti, gruppi e autorizzazioni a livello NFS (Network File System) nella Guida per l'utente di Amazon Elastic File System.

La seguente policy di esempio concede l'accesso al file system root ai file del tuo file system Amazon EFS.

> **Note**
>
> Negli esempi seguenti, sostituisci la *regione* con la tua regione, l'*ID account* con l'account in cui si trova il file e *file-system-id*con l'ID del tuo 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"
        }
    ]
}
```

La seguente policy di esempio concede all'utente l'accesso ai file system del file system 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"
        }
    ]
}
```

Tutorial Transfer Family

La guida per AWS Transfer Family l'utente fornisce procedure dettagliate per diversi casi d'uso.

- Guida introduttiva agli endpoint del server AWS Transfer Family: questo tutorial illustra la creazione di un server SFTP Transfer Family e di un utente gestito dal servizio, quindi mostra come trasferire un file utilizzando un client.
- Configurazione e utilizzo dei connettori SFTP: questo tutorial illustra come configurare un connettore SFTP e quindi trasferire file tra lo storage Amazon S3 e un server SFTP.
- Configurazione di un metodo Amazon API Gateway come provider di identità personalizzato : questo tutorial illustra come configurare un metodo Amazon API Gateway e utilizzarlo come provider di identità personalizzato per caricare file su un AWS Transfer Family server.
- Configurazione di un flusso di lavoro gestito per la decrittografia di un file: questo tutorial illustra come configurare un flusso di lavoro gestito che contenga una fase di decrittografia e come caricare un file crittografato in un bucket Amazon S3 e quindi visualizzare il file decrittografato.
- Configurazione di una configurazione AS2: questo tutorial illustra i passaggi necessari per configurare un server AS2 Transfer Family. Sono disponibili istruzioni per importare certificati, creare profili e accordi, facoltativamente creare un connettore AS2 e quindi testare la configurazione.

Argomenti

Guida introduttiva agli endpoint del server AWS Transfer Family

Usa questo tutorial per iniziare a usare AWS Transfer Family (Transfer Family). Imparerai come creare un server compatibile con SFTP con endpoint accessibile al pubblico utilizzando lo storage Amazon S3, aggiungere un utente con autenticazione gestita dal servizio e trasferire un file con Cyberduck.

Argomenti

Prerequisiti

Prima di iniziare, assicurati di completare i requisiti in. Prerequisiti Come parte di questa configurazione, crei un bucket Amazon Simple Storage Service (Amazon S3) e AWS Identity and Access Management un ruolo utente (IAM).

Sono necessarie autorizzazioni per l'utilizzo della AWS Transfer Family console e autorizzazioni necessarie per configurare altri AWS servizi utilizzati da Transfer Family, come Amazon Simple Storage Service AWS Certificate Manager, Amazon Elastic File System e Amazon Route 53. Ad esempio, per gli utenti che trasferiscono file da e verso l'esterno AWS utilizzando Transfer Family, AmazonS3 FullAccess concede le autorizzazioni per configurare e utilizzare un bucket Amazon S3. Alcune delle autorizzazioni contenute in questa politica sono necessarie per creare bucket Amazon S3.

Per utilizzare la console Transfer Family, è necessario quanto segue:

- AWSTransferConsoleFullAccessconcede all'utente SFTP le autorizzazioni per creare risorse Transfer Family.
- IAM FullAccess (o in particolare una politica che consente la creazione di ruoli IAM) è necessario solo se desideri che Transfer Family crei automaticamente un ruolo di registrazione per il tuo server in Amazon CloudWatch Logs o un ruolo utente per un utente che accede a un server.
- Per creare ed eliminare tipi di server VPC, devi aggiungere le azioni ec2: CreateVpc Endpoint ed ec2: DeleteVpc Endpoints alla tua policy.

> **Note**
>
> Le FullAccess policy AmazonS3 FullAccess e IAM, di per sé, non sono necessarie per l'utilizzo generale di. AWS Transfer Family Vengono presentate qui come un modo semplice per assicurarsi che tutte le autorizzazioni necessarie siano coperte. Inoltre, si tratta di

politiche AWS gestite, ovvero politiche standard disponibili per tutti i AWS clienti. È possibile visualizzare le singole autorizzazioni in queste politiche e determinare il set minimo necessario per i propri scopi.

Fase 1: Accesso alla console di AWS Transfer Family

Per accedere a Transfer Family

1. Accedi AWS Management Console e apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Per ID account o alias, inserisci l'ID del tuo Account AWS.
3. Per il nome utente IAM, inserisci il nome del ruolo utente che hai creato per Transfer Family.
4. Per Password, inserisci la password AWS del tuo account.
5. Selezionare Sign in (Accedi).

Fase 2: Creare un server compatibile con SFTP

Secure Shell (SSH) File Transfer Protocol (SFTP) è un protocollo di rete utilizzato per il trasferimento sicuro di dati su Internet. Il protocollo supporta tutte le funzionalità di sicurezza e autenticazione di SSH. È ampiamente utilizzato per lo scambio di dati, comprese informazioni sensibili tra partner commerciali in una varietà di settori come i servizi finanziari, la sanità, la vendita al dettaglio e la pubblicità.

Per creare un server compatibile con SFTP

1. Seleziona Server dal pannello di navigazione, quindi scegli Crea server.
2. In Scegli protocolli, seleziona SFTP, quindi scegli Avanti.
3. In Scegli un provider di identità, scegli Servizio gestito per archiviare le identità e le chiavi degli utenti in Transfer Family, quindi scegli Avanti.
4. In Scegli un endpoint, procedi come segue:
    a. Per Tipo di endpoint, scegli il tipo di endpoint accessibile pubblicamente.
    b. Per Nome host personalizzato, scegli Nessuno.
    c. Seleziona Successivo.
5. In Scegli un dominio, scegli Amazon S3.

6. In Configura dettagli aggiuntivi, per le opzioni degli algoritmi crittografici, scegli una politica di sicurezza che contenga gli algoritmi crittografici abilitati all'uso dal tuo server. La nostra politica di sicurezza più recente è quella predefinita: per i dettagli, consulta. Politiche di sicurezza per AWS Transfer Family i server

   > **Note**
   >
   > Solo se stai aggiungendo un flusso di lavoro gestito per il tuo server, scegli Crea un nuovo ruolo per la CloudWatchregistrazione. Per registrare gli eventi del server, non è necessario creare un ruolo IAM.

7. In Rivedi e crea, scegli Crea server. Verrai indirizzato alla pagina Server.

Possono essere necessari un paio di minuti prima che lo stato del nuovo server passi a Online. A quel punto, il server sarà in grado di eseguire operazioni sui file, ma dovrai prima creare un utente. Per informazioni dettagliate sulla creazione di utenti, consultaGestione degli utenti per gli endpoint del server.

Passaggio 3: Aggiungere un utente gestito dal servizio

Per aggiungere un utente al server compatibile con SFTP

1. Nella pagina Server, selezionate il server a cui desiderate aggiungere un utente.
2. Scegli Add user (Aggiungi utente).
3. Nella sezione Configurazione utente, per Nome utente, inserisci il nome utente. Questo nome utente deve contenere un minimo di 3 e un massimo di 100 caratteri. È possibile utilizzare i seguenti caratteri nel nome utente: a—z, A-Z, 0—9, trattino basso '_', trattino '-', punto ' . ', e al segno (@). Il nome utente non può iniziare con un trattino, un punto o un segno di chiavetta.
4. Per Access, scegli il ruolo IAM in Crea un ruolo e una policy IAM cui hai creato. Questo ruolo IAM include una policy IAM che contiene le autorizzazioni per accedere al tuo bucket Amazon S3, oltre a una relazione di fiducia con il servizio. AWS Transfer Family La procedura descritta in seguito Per stabilire una relazione di trust mostra come stabilire la corretta relazione di fiducia.
5. Per Politica, scegli Nessuno.
6. Per la directory Home, scegli il bucket Amazon S3 in cui desideri archiviare i dati che trasferisci utilizzando. AWS Transfer Family Inserisci il percorso della directory. `home` Questa è la directory che i tuoi utenti vedono quando accedono utilizzando il loro client.

Ti consigliamo di utilizzare un percorso di directory che contenga il nome utente in modo da avere la possibilità di utilizzare una politica di sessione. Una policy di sessione limita l'accesso di un utente nel bucket Amazon S3 alla directory di quell'utente. `home` Per ulteriori informazioni sull'utilizzo delle politiche di sessione, consulta. Come funzionano le politiche di sessione

Se preferisci, puoi lasciare vuoto questo parametro per utilizzare la directory del tuo bucket Amazon S3. `root` Se scegli questa opzione, assicurati che il tuo ruolo IAM fornisca l'accesso alla `root` directory.

7. Seleziona la casella di controllo con restrizioni per impedire agli utenti di accedere a qualsiasi elemento al di fuori della loro `home` directory. Ciò impedisce inoltre agli utenti di visualizzare il nome del bucket Amazon S3 o il nome della cartella.
8. Per la chiave pubblica SSH, inserisci la parte della chiave SSH pubblica della coppia di chiavi SSH nel formato. `ssh-rsa` *`<string>`*

   La chiave deve essere convalidata dal servizio prima di poter aggiungere il nuovo utente. Per ulteriori informazioni su come generare una coppia di chiavi SSH, vedereGenera chiavi SSH per gli utenti gestiti dal servizio.
9. (Facoltativo) Per Chiave e Valore, inserite uno o più tag come coppie chiave-valore e scegliete Aggiungi tag.
10. Scegliere Add (Aggiungi) per aggiungere il nuovo utente al server scelto.

    Il nuovo utente viene visualizzato nella sezione Utenti della pagina dei dettagli del server.

Passaggio 4: Trasferire un file utilizzando un client

I file vengono trasferiti tramite il AWS Transfer Family servizio specificando l'operazione di trasferimento in un client. AWS Transfer Family supporta diversi client. Per maggiori dettagli, consulta Trasferimento di file su un endpoint server utilizzando un client.

Questa sezione contiene le procedure per l'utilizzo di Cyberduck e OpenSSH.

Argomenti

- Usa Cyberduck
- Usa OpenSSH

Usa Cyberduck

Per trasferire file tramite Cyberduck AWS Transfer Family

1. Apri il client Cyberduck.
2. Scegli Apri connessione.
3. Nella finestra di dialogo Apri connessione, scegli SFTP (SSH File Transfer Protocol).
4. Per Server, inserite l'endpoint del server. L'endpoint del server si trova nella pagina dei dettagli del server, vedi. Visualizza i dettagli dei server SFTP, FTPS e FTP
5. Per il numero di porta, immettere **22** SFTP.
6. Per Username (Nome utente), immettere il nome per l'utente creato in Gestione degli utenti per gli endpoint del server.
7. Per Chiave privata SSH, scegli o inserisci la chiave privata SSH.
8. Scegli Connetti.
9. Esegui il trasferimento dei file.

   In base alla posizione dei file, eseguire una delle seguenti operazioni:

   - Nella tua directory locale (l'origine), scegli i file che desideri trasferire e trascinali nella directory Amazon S3 (la destinazione).
   - Nella directory Amazon S3 (l'origine), scegli i file che desideri trasferire e trascinali nella tua directory locale (la destinazione).

Usa OpenSSH

Utilizza le istruzioni che seguono per trasferire i file dalla riga di comando tramite OpenSSH.

> **Note**
>
> Questo client funziona solo con un server compatibile con SFTP.

Per trasferire file AWS Transfer Family utilizzando l'utilità da riga di comando OpenSSH

1. Su Linux o Macintosh, aprire un terminale di comando.
2. Al prompt, immettete il seguente comando: `% sftp -i transfer-key sftp_user@service_endpoint`

Nel comando precedente, `sftp_user` è il nome utente e la chiave `transfer-key` privata SSH. Qui `service_endpoint` è l'endpoint del server come mostrato nella AWS Transfer Family console per il server selezionato.

Viene visualizzato un prompt `sftp`.

3. (Facoltativo) Per visualizzare la home directory dell'utente, immettete il seguente comando al `sftp` prompt: `sftp> pwd`
4. Nella riga successiva, immettere il testo seguente: `sftp> cd /mybucket/home/sftp_user`

   In questo esercizio introduttivo, questo bucket Amazon S3 è la destinazione del trasferimento di file.
5. Nella riga successiva, immettere il comando seguente: `sftp> put filename.txt`

   Il `put` comando trasferisce il file nel bucket Amazon S3.

   Viene visualizzato un messaggio simile al seguente che indica che il trasferimento file è in corso o è completato.

   ```
   Uploading filename.txt to /my-bucket/home/sftp_user/filename.txt

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

Configurazione di un flusso di lavoro gestito per la decrittografia di un file

Questo tutorial illustra come configurare un flusso di lavoro gestito che contenga una fase di decrittografia. Il tutorial mostra anche come caricare un file crittografato in un bucket Amazon S3 e quindi visualizzare il file decrittografato nello stesso bucket.

> **Note**
>
> Il blog AWS sullo storage ha un post che descrive come decrittografare semplicemente i file senza scrivere alcun codice utilizzando i flussi di lavoro Transfer Family Managed, crittografare e decrittografare i file con PGP e. AWS Transfer Family

Argomenti

Fase 1: Configurare un ruolo di esecuzione

Crea un ruolo di esecuzione AWS Identity and Access Management (IAM) che Transfer Family possa utilizzare per avviare un flusso di lavoro. Il processo di creazione di un ruolo di esecuzione è descritto inPolitiche IAM per i flussi di lavoro.

> **Note**
>
> Come parte della creazione di un ruolo di esecuzione, assicurati di stabilire una relazione di fiducia tra il ruolo di esecuzione e Transfer Family, come descritto inPer stabilire una relazione di trust.

La seguente politica sul ruolo di esecuzione contiene tutte le autorizzazioni necessarie per avviare il flusso di lavoro creato in questo tutorial. Per utilizzare questa policy di esempio, sostituisci *`user input placeholders`* con le tue informazioni. Sostituiscilo `DOC-EXAMPLE-BUCKET` con il nome del bucket Amazon S3 in cui carichi i file crittografati.

> **Note**
>
> Non tutti i flussi di lavoro richiedono tutte le autorizzazioni elencate in questo esempio. Puoi limitare le autorizzazioni in base ai tipi di passaggi del tuo flusso di lavoro specifico. Le autorizzazioni necessarie per ogni tipo di passaggio predefinito sono descritte in. Utilizza passaggi predefiniti Le autorizzazioni necessarie per un passaggio personalizzato sono descritte in. Autorizzazioni IAM per un passaggio personalizzato

```
{
```

```
    "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/
*"
        }
    ]
}
```

Fase 2: Creare un flusso di lavoro gestito

Ora devi creare un flusso di lavoro che contenga una fase di decrittografia.

Per creare un flusso di lavoro che contenga una fase di decrittografia

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Flussi di lavoro, quindi scegli Crea flusso di lavoro.
3. Inserisci i seguenti dettagli:
   - Inserisci una descrizione, ad esempio**`Decrypt workflow example`**.
   - Nella sezione Passaggi nominali, scegliete Aggiungi fase.
4. Per Scegli il tipo di passaggio, scegli Decrittografa il file, quindi scegli Avanti.
5. Nella finestra di dialogo Configura parametri, specificate quanto segue:
   - Immettete un nome descrittivo per la fase, **`decrypt-step`** ad esempio. Gli spazi non sono consentiti nei nomi delle fasi.
   - Per la destinazione dei file decrittografati, scegli Amazon S3.
   - Per il nome del bucket di destinazione, scegli lo stesso bucket Amazon S3 che hai specificato `DOC-EXAMPLE-BUCKET` nella policy IAM che hai creato nella fase 1.
   - Per il prefisso della chiave di destinazione, inserisci il nome del prefisso (cartella) in cui desideri archiviare i file decrittografati nel bucket di destinazione, ad esempio. **`decrypted-files/`**

     > **Note**
     >
     > Assicurati di aggiungere una barra finale () al prefisso. **`/`**

   - Per questo tutorial, lascia deselezionata l'opzione Sovrascrivi esistente. Quando questa impostazione è deselezionata, se si tenta di decrittografare un file con lo stesso nome di un file esistente, l'elaborazione del flusso di lavoro si interrompe e il nuovo file non viene elaborato.

   Scegli Avanti per passare alla schermata di revisione.
6. Esamina i dettagli del passaggio. Se tutto è corretto, scegli Crea passaggio.
7. Il flusso di lavoro richiede solo una singola fase di decrittografia, quindi non ci sono passaggi aggiuntivi da configurare. Scegli Crea flusso di lavoro per creare il nuovo flusso di lavoro.

Annota l'ID del flusso di lavoro per il nuovo flusso di lavoro. Questo ID ti servirà per il passaggio successivo. Questo tutorial utilizza *`w-1234abcd5678efghi`*come esempio l'ID del flusso di lavoro.

Fase 3: Aggiungere il flusso di lavoro a un server e creare un utente

Ora che hai un flusso di lavoro con una fase di decrittografia, devi associarlo a un server Transfer Family. Questo tutorial mostra come collegare il flusso di lavoro a un server Transfer Family esistente. In alternativa, puoi creare un nuovo server da utilizzare con il tuo flusso di lavoro.

Dopo aver collegato il flusso di lavoro a un server, è necessario creare un utente in grado di accedere al server tramite SFTP e attivare l'esecuzione del flusso di lavoro.

Per configurare un server Transfer Family per eseguire un flusso di lavoro

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server, quindi scegli un server dall'elenco. Assicurati che questo server supporti il protocollo SFTP.
3. Nella pagina dei dettagli del server, scorri verso il basso fino alla sezione Dettagli aggiuntivi, quindi scegli Modifica.
4. Nella pagina Modifica dettagli aggiuntivi, nella sezione Flussi di lavoro gestiti, scegli il tuo flusso di lavoro e scegli il ruolo di esecuzione corrispondente.
   - Per Workflow per caricamenti completi di file, scegli il flusso di lavoro in cui hai creatoFase 2: Creare un flusso di lavoro gestito, ad esempio,. **`w-1234abcd5678efghi`**
   - Per il ruolo di esecuzione dei flussi di lavoro gestiti, scegli il ruolo IAM in cui hai creato. Fase 1: Configurare un ruolo di esecuzione
5. Scorri fino alla fine della pagina e scegli Salva per salvare le modifiche.

Annota l'ID del server che stai utilizzando. Il nome del AWS Secrets Manager segreto utilizzato per memorizzare le chiavi PGP si basa in parte sull'ID del server.

Per aggiungere un utente in grado di attivare il flusso di lavoro

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server, quindi scegli il server che stai utilizzando per il flusso di lavoro di decrittografia.
3. Nella pagina dei dettagli del server, scorri verso il basso fino alla sezione Utenti e scegli Aggiungi utente.
4. Per il tuo nuovo utente, inserisci i seguenti dettagli:

- Per Username (Nome utente), inserisci **`decrypt-user`**.
- Per Ruolo, scegli un ruolo utente che possa accedere al tuo server.
- Per la directory Home, scegli il bucket Amazon S3 che hai usato in precedenza, ad esempio. `DOC-EXAMPLE-BUCKET`
- Per le chiavi pubbliche SSH, incolla una chiave pubblica che corrisponde a una chiave privata che possiedi. Per informazioni dettagliate, vedi Genera chiavi SSH per gli utenti gestiti dal servizio.

5. Scegli Aggiungi per salvare il tuo nuovo utente.

Annota il nome del tuo utente Transfer Family per questo server. Il segreto si basa in parte sul nome dell'utente. Per semplicità, questo tutorial utilizza un segreto predefinito che può essere utilizzato da qualsiasi utente del server.

Fase 4: Creare una coppia di key pair PGP

Usa uno dei client PGP supportati per generare una coppia di key pair PGP. Questo processo è descritto in dettaglio in. Genera chiavi PGP

Per generare una coppia di key pair PGP

1. Per questo tutorial, puoi utilizzare il client `gpg` (`GnuPG`) versione 2.0.22 per generare una coppia di chiavi PGP che utilizza RSA come algoritmo di crittografia. Per questo client, esegui il comando seguente e fornisci un indirizzo email e una passphrase. Puoi usare qualsiasi nome o indirizzo email che preferisci. Assicurati di ricordare i valori che usi, perché dovrai inserirli più avanti nel tutorial.

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

> **Note**
>
> Se stai usando la `GnuPG` versione 2.3.0 o successiva, devi eseguire. `gpg --full-gen-key` Quando viene richiesto il tipo di chiave da creare, scegli RSA o ECC. Tuttavia, se scegli ECC, assicurati di scegliere uno dei due NIST o BrainPool per la curva ellittica. Non scegliete. Curve 25519

2. Esporta la chiave privata eseguendo il comando seguente. Sostituiscila *user@example.com* con l'indirizzo e-mail che hai usato quando hai generato la chiave.

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

   Questo comando esporta la chiave privata nel **workflow-tutorial-key.pgp** file. Puoi assegnare al file di output il nome che preferisci. Puoi anche eliminare il file della chiave privata dopo averlo aggiunto AWS Secrets Manager.

Passaggio 5: Memorizza la chiave privata PGP in AWS Secrets Manager

È necessario archiviare la chiave privata in Secrets Manager, in un modo molto specifico, in modo che il flusso di lavoro possa trovare la chiave privata quando il flusso di lavoro esegue una fase di decrittografia su un file caricato.

> **Note**
>
> Quando memorizzi segreti in Secrets Manager, ti vengono Account AWS addebitati dei costi. Per informazioni sui prezzi, consulta Prezzi di AWS Secrets Manager.

Per memorizzare una chiave privata PGP in Secrets Manager

1. Accedi AWS Management Console e apri la AWS Secrets Manager console all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Nel pannello di navigazione a sinistra, seleziona Segreti.
3. Nella pagina Segreti, scegli Memorizza un nuovo segreto.
4. Nella pagina Scegli il tipo di segreto, per Tipo segreto, scegli Altro tipo di segreto.
5. Nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.
   - Chiave: Invio. **PGPPrivateKey**
   - valore: incolla il testo della tua chiave privata nel campo del valore.
6. Scegli Aggiungi riga e, nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.
   - Chiave: Invio. **PGPPassphrase**

- value — Inserisci la passphrase che hai usato quando hai generato la tua key pair PGP. Fase 4: Creare una coppia di key pair PGP

7. Seleziona Successivo.
8. Nella pagina Configura segreto, inserisci un nome e una descrizione per il tuo segreto. Puoi creare un segreto per un utente specifico o uno che può essere utilizzato da tutti gli utenti. Se l'ID del server è *s-11112222333344445*, assegnate al segreto il nome seguente.

   - Per creare un segreto predefinito per tutti gli utenti, assegna un nome al segreto**aws/transfer/*s-11112222333344445*/@pgp-default**.
   - Per creare un segreto solo per l'utente che hai creato in precedenza, assegna un nome al segreto**aws/transfer/*s-11112222333344445*/decrypt-user**.
9. Scegliete Avanti, quindi accettate le impostazioni predefinite nella pagina Configura rotazione. Quindi scegli Successivo.
10. Nella pagina Revisione, scegli Store per creare e archiviare il segreto.

Per ulteriori informazioni sull'aggiunta della chiave privata PGP a Secrets Manager, consulta Utilizzare AWS Secrets Manager per memorizzare la chiave PGP.

Fase 6: Crittografare un file

Usa il gpg programma per crittografare un file da utilizzare nel tuo flusso di lavoro. Eseguite il comando seguente per crittografare un file:

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

Prima di eseguire questo comando, tenete presente quanto segue:

- Per l'`-r`argomento, *marymajor@example.com* sostituiscilo con l'indirizzo email che hai usato quando hai creato la key pair PGP.
- La `--openpgp` bandiera è facoltativa. Questo flag rende il file criptato conforme allo standard OpenPGP RFC4880.
- Questo comando crea un file denominato nella stessa posizione di. **testfile.txt.gpg testfile.txt**

Passaggio 7: Eseguire il flusso di lavoro e visualizzare i risultati

Per eseguire il flusso di lavoro, ti connetti al server Transfer Family con l'utente che hai creato nel passaggio 3. Quindi puoi cercare nel bucket Amazon S3 che hai specificato nel passaggio 2.5, configurare i parametri di destinazione per vedere il file decrittografato.

Per eseguire il flusso di lavoro di decrittografia

1. Aprire un terminale di comando.
2. Esegui il comando seguente, sostituendolo *your-endpoint* con l'endpoint attuale e *transfer-key* con la chiave privata SSH dell'utente:

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

   Ad esempio, se la chiave privata è archiviata in `~/.ssh/decrypt-user` e l'endpoint lo è`s-11112222333344445.server.transfer.us-east-2.amazonaws.com`, il comando è il seguente:

   ```
   sftp -i  ~/.ssh/decrypt-user decrypt-user@s-11112222333344445.server.transfer.us-
   east-2.amazonaws.com
   ```
3. Esegui il comando pwd. In caso di successo, questo comando restituirà quanto segue:

   ```
   Remote working directory: /DOC-EXAMPLE-BUCKET/decrypt-user
   ```

   La tua directory riflette il nome del tuo bucket Amazon S3.
4. Esegui il comando seguente per caricare il file e attivare l'esecuzione del flusso di lavoro:

   ```
   put testfile.txt.gpg
   ```
5. Per la destinazione dei file decrittografati, hai specificato la `decrypted-files/` cartella al momento della creazione del flusso di lavoro. Ora puoi accedere a quella cartella ed elencarne il contenuto.

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

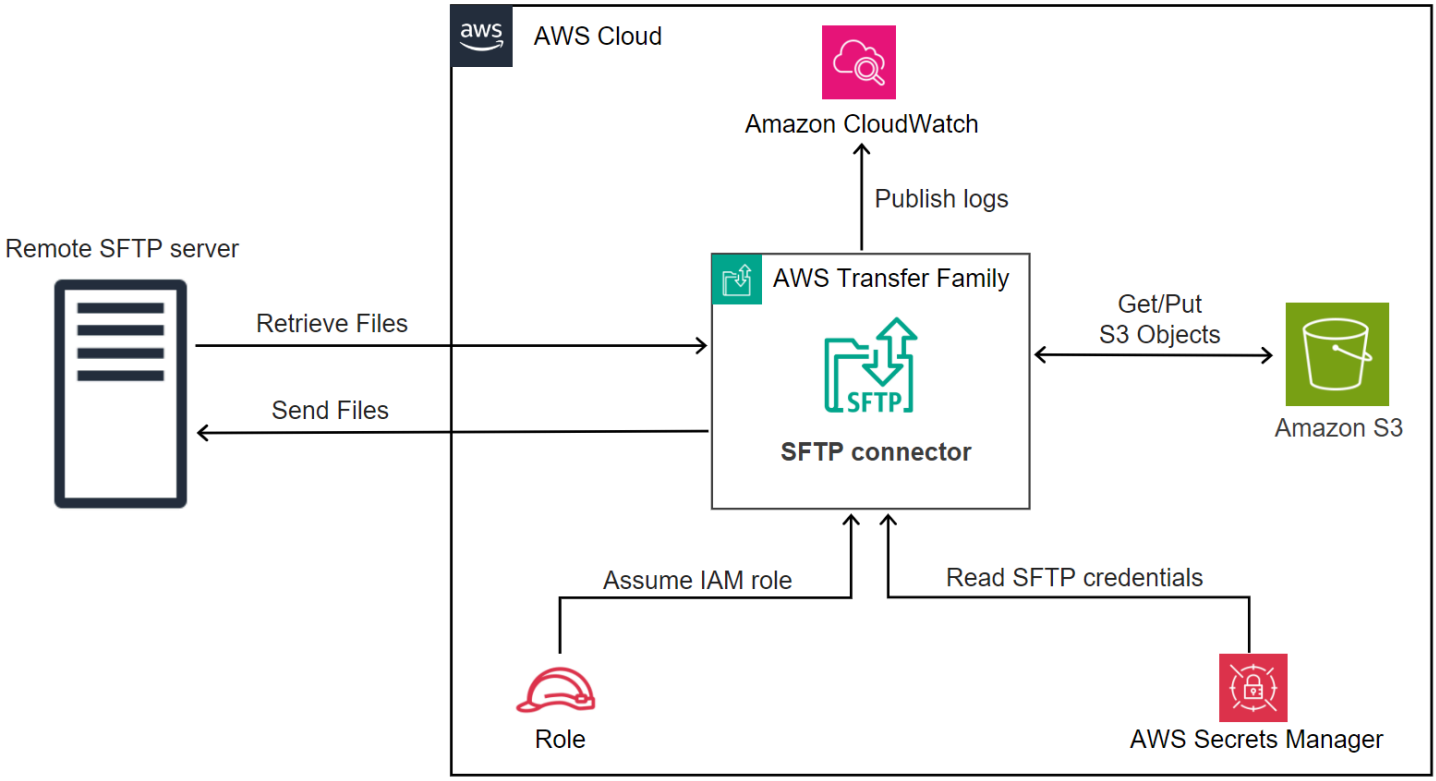
In caso di successo, il `ls` comando elenca il `testfile.txt` file. È possibile scaricare questo file e verificare che sia uguale al file originale crittografato in precedenza.

Configurazione e utilizzo dei connettori SFTP

Lo scopo di un connettore è stabilire una relazione tra AWS lo storage e il server SFTP di un partner. Puoi inviare file da Amazon S3 a una destinazione esterna di proprietà del partner. Puoi anche utilizzare un connettore SFTP per recuperare file dal server SFTP di un partner.

Questo tutorial illustra come configurare un connettore SFTP e quindi trasferire file tra lo storage Amazon S3 e un server SFTP.

Un connettore SFTP recupera le credenziali SFTP da cui autenticarsi su un server SFTP remoto e AWS Secrets Manager stabilire una connessione. Il connettore invia o recupera file dal server remoto e li archivia in Amazon S3. Un ruolo IAM viene utilizzato per consentire l'accesso al bucket Amazon S3 e alle credenziali archiviate in Secrets Manager. E puoi accedere ad Amazon CloudWatch.



I seguenti post del blog forniscono un'architettura di riferimento per creare un flusso di lavoro MFT utilizzando connettori SFTP, inclusa la crittografia dei file tramite PGP prima di inviarli a un server

SFTP remoto utilizzando connettori SFTP: Progettazione di trasferimenti di file gestiti sicuri e conformi con connettori SFTP e crittografia PGP. AWS Transfer Family

Argomenti

Fase 1: Creare le risorse di supporto necessarie

Puoi utilizzare i connettori SFTP per copiare file tra Amazon S3 e qualsiasi server SFTP remoto. Per questo tutorial, utilizziamo un AWS Transfer Family server come server SFTP remoto. Dobbiamo creare e configurare le seguenti risorse:

- Crea bucket Amazon S3 per archiviare file nel tuo AWS ambiente e per inviare e recuperare file dal server SFTP remoto:. Crea bucket Amazon S3
- Crea un AWS Identity and Access Management ruolo per accedere allo storage Amazon S3 e al nostro segreto in Secrets Manager:. Crea un ruolo IAM con le autorizzazioni necessarie
- Crea un server Transfer Family che utilizza il protocollo SFTP e un utente gestito dal servizio che utilizza il connettore SFTP per trasferire file da o verso il server SFTP:. Creare un server SFTP Transfer Family e un utente
- Crea un AWS Secrets Manager segreto che memorizzi le credenziali utilizzate dal connettore SFTP per accedere al server SFTP remoto:. Crea e archivia un segreto in AWS Secrets Manager

Crea bucket Amazon S3

Come creare un bucket Amazon S3.

1. Accedi alla AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/s3/.
2. Scegli una regione e inserisci un nome.

   Per questo tutorial, il nostro bucket è inserito **`US East (N. Virginia) us-east-1`** e il nome è**`sftp-server-storage-east`**.
3. Accetta le impostazioni predefinite e scegli Crea bucket.

Per informazioni complete sulla creazione di bucket Amazon S3, vedi Come posso creare un bucket S3? nella Guida per l'utente di Amazon Simple Storage Service.

Crea un ruolo IAM con le autorizzazioni necessarie

Per il ruolo di accesso, crea una policy con le seguenti autorizzazioni.

L'esempio seguente concede le autorizzazioni necessarie per accedere al *DOC-EXAMPLE-BUCKET* in Amazon S3 e al segreto specificato archiviato in 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"
    }
  ]
}
```

Sostituisci gli articoli come segue:

- Per *DOC-EXAMPLE-BUCKET*, il tutorial utilizza. **s3-storage-east**
- *Per la regione, il tutorial utilizza.* **us-east-1**
- Per l'*account-id*, usa il tuo Account AWS ID.
- Per *SecretName-6 RandomCharacters*, siamo **using sftp-connector1** per il nome (avrai i tuoi sei caratteri casuali per il tuo segreto).

È inoltre necessario assicurarsi che questo ruolo contenga una relazione di fiducia che consenta al connettore di accedere alle risorse dell'utente durante la gestione delle richieste di trasferimento degli utenti. Per i dettagli su come stabilire una relazione di fiducia, vedere. Per stabilire una relazione di trust

> **Note**
>
> Per vedere i dettagli del ruolo che stiamo utilizzando per il tutorial, vediUtente e ruolo di accesso combinati.

Crea e archivia un segreto in AWS Secrets Manager

Dobbiamo memorizzare un segreto in Secrets Manager per memorizzare le credenziali utente per il connettore SFTP. È possibile utilizzare una password, una chiave privata SSH o entrambe. Per il tutorial, stiamo usando una chiave privata.

> **Note**
>
> Quando memorizzi segreti in Secrets Manager, ti vengono Account AWS addebitati dei costi. Per informazioni sui prezzi, consulta Prezzi di AWS Secrets Manager.

Prima di iniziare la procedura di archiviazione del segreto, recuperate e formatta la chiave privata. La chiave privata deve corrispondere alla chiave pubblica configurata per l'utente sul server SFTP remoto. Per il nostro tutorial, la chiave privata deve corrispondere alla chiave pubblica archiviata per il nostro utente di prova sul server SFTP Transfer Family che stiamo utilizzando come server remoto.

Per fare ciò, esegui il seguente comando:

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

Ad esempio, se il file della chiave privata si trova in`~/.ssh/sftp-testuser-privatekey`, il comando è il seguente.

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

Ciò restituisce la chiave nel formato corretto (con caratteri di nuova riga incorporati) sullo standard output. Copia questo testo da qualche parte, poiché devi incollarlo nella procedura seguente (nel passaggio 6).

Per memorizzare le credenziali utente in Secrets Manager per un connettore SFTP

1. Accedere AWS Management Console e aprire la AWS Secrets Manager console all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Nel pannello di navigazione a sinistra, seleziona Segreti.
3. Nella pagina Segreti, scegli Memorizza un nuovo segreto.
4. Nella pagina Scegli il tipo di segreto, per Tipo segreto, scegli Altro tipo di segreto.
5. Nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.
   - Chiave: Invio. **`Username`**
   - valore — Inserisci il nome del nostro utente,**`sftp-testuser`**.
6. Per inserire la chiave, ti consigliamo di utilizzare la scheda Plaintext.
   a. Scegli Aggiungi riga, quindi inserisci. **`PrivateKey`**
   b. Scegli la scheda Testo normale. Il campo ora contiene il seguente testo:

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

   c. Incolla il testo della tua chiave privata (salvato in precedenza) tra le virgolette doppie vuote («»).

La schermata dovrebbe apparire come segue (i dati chiave sono visualizzati in grigio).

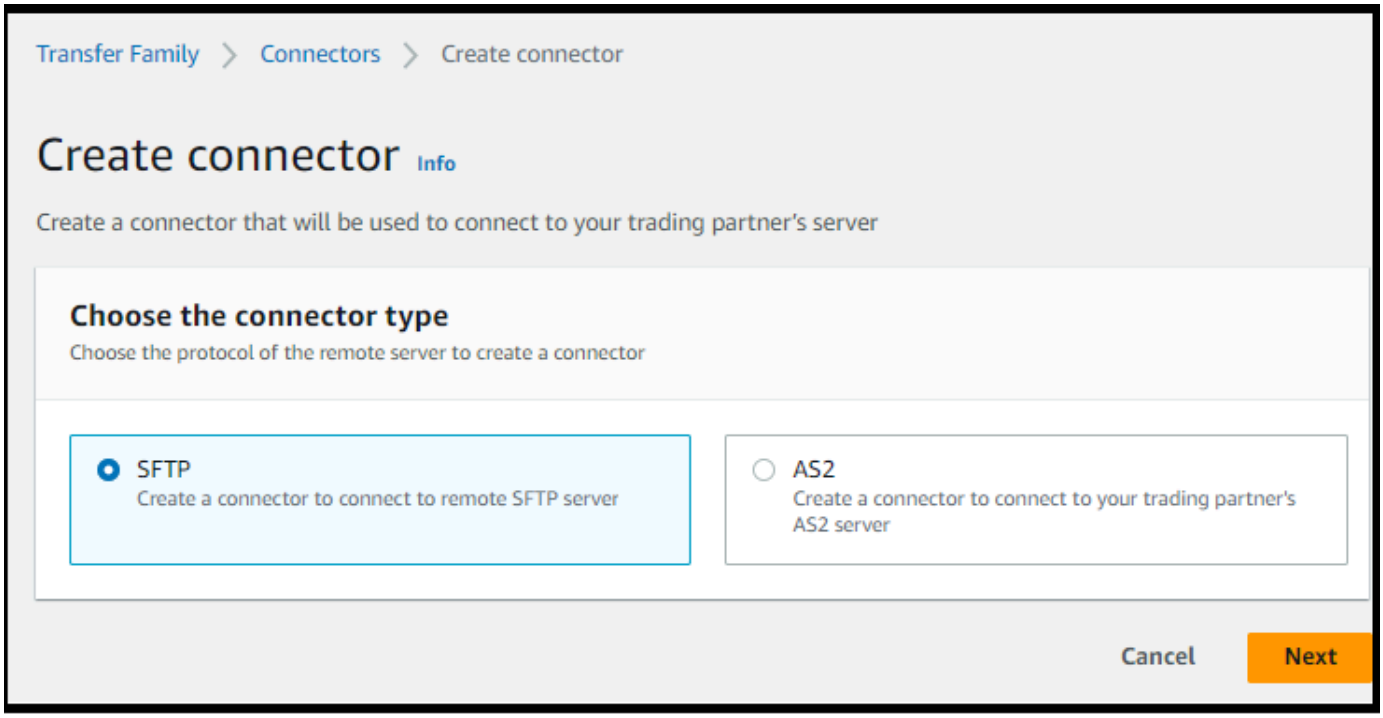
7. Seleziona Successivo.
8. Nella pagina Configura segreto, inserisci un nome per il tuo segreto. Per questo tutorial, diamo un nome al segreto**`aws/transfer/sftp-connector1`**.
9. Scegli Avanti, quindi accetta le impostazioni predefinite nella pagina Configura rotazione. Quindi scegli Successivo.
10. Nella pagina Revisione, scegli Store per creare e archiviare il segreto.

Fase 2: Creare e testare un connettore SFTP

In questa sezione, creiamo un connettore SFTP che utilizza tutte le risorse che abbiamo creato in precedenza. Per ulteriori dettagli, consulta Configurare i connettori SFTP.

Per creare un connettore SFTP

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Connettori, quindi scegli Crea connettore.
3. Scegli SFTP come tipo di connettore per creare un connettore SFTP, quindi scegli Avanti.



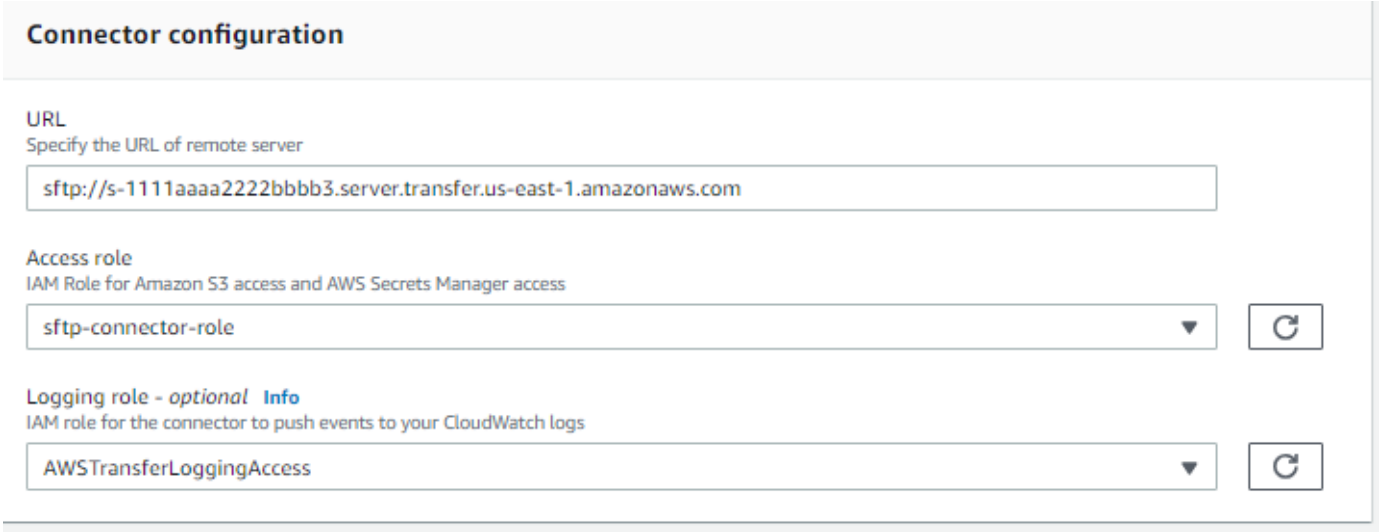
4. Nella sezione Configurazione del connettore, fornite le seguenti informazioni:

   - Per l'URL, inserite l'URL del server SFTP remoto. Per il tutorial, inseriamo l'URL del server Transfer Family che stiamo utilizzando come server SFTP remoto.

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

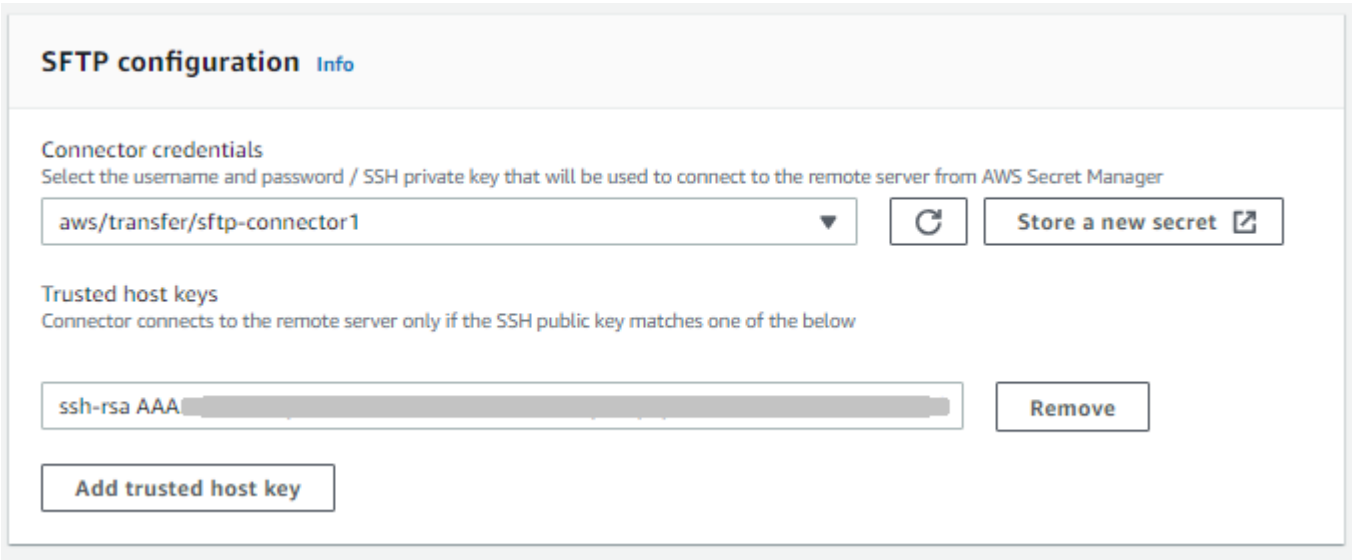
     Sostituisci *1111aaaa2222bbbb3 con* il tuo ID server Transfer Family.
   - Per il ruolo Access, inserisci il ruolo creato in precedenza,. **`sftp-connector-role`**
   - Per il ruolo Logging, scegli**`AWSTransferLoggingAccess`**.

     > **Note**
     >
     > AWSTransferLoggingAccess è una politica AWS gestita. Questa politica è descritta in dettaglio in[AWS politica gestita: AWSTransferLoggingAccess](#).



5. Nella sezione Configurazione SFTP, fornite le seguenti informazioni:

   - Per le credenziali del connettore, scegliete il nome della risorsa Secrets Manager che contiene le credenziali SFTP. Per il tutorial, scegliete. **`aws/transfer/sftp-connector1`**
   - Per le chiavi host affidabili, incolla la parte pubblica della chiave host. Puoi recuperare questa chiave `ssh-keyscan` eseguendola sul tuo server SFTP. Per i dettagli su come formattare e archiviare la chiave host affidabile, consulta la documentazione SftpConnectorConfigsui tipi di dati.



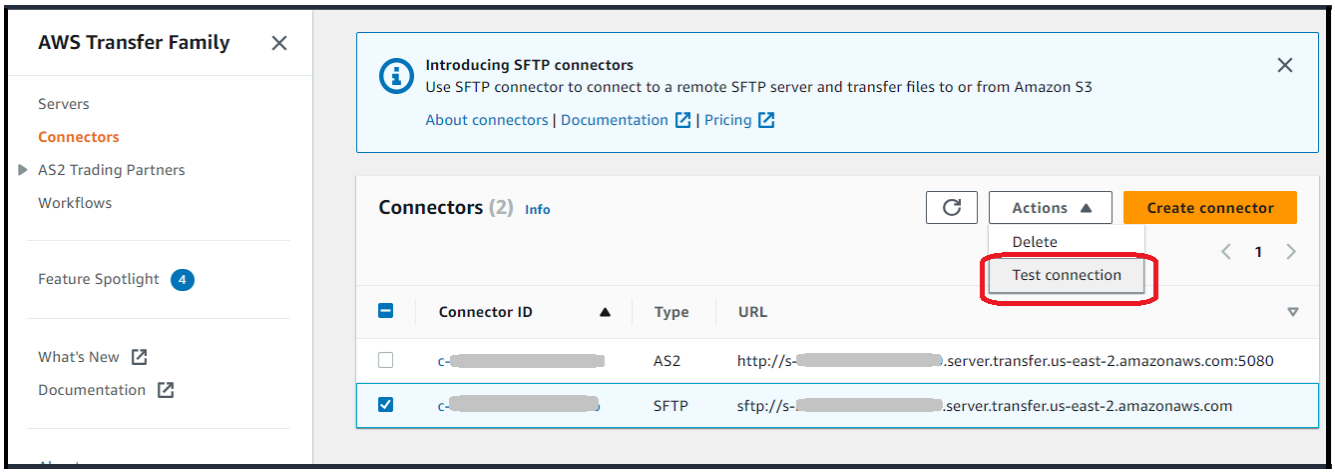
6. Dopo aver confermato tutte le impostazioni, scegli Crea connettore per creare il connettore SFTP.

Dopo aver creato un connettore SFTP, ti consigliamo di testarlo prima di tentare di trasferire qualsiasi file utilizzando il nuovo connettore.

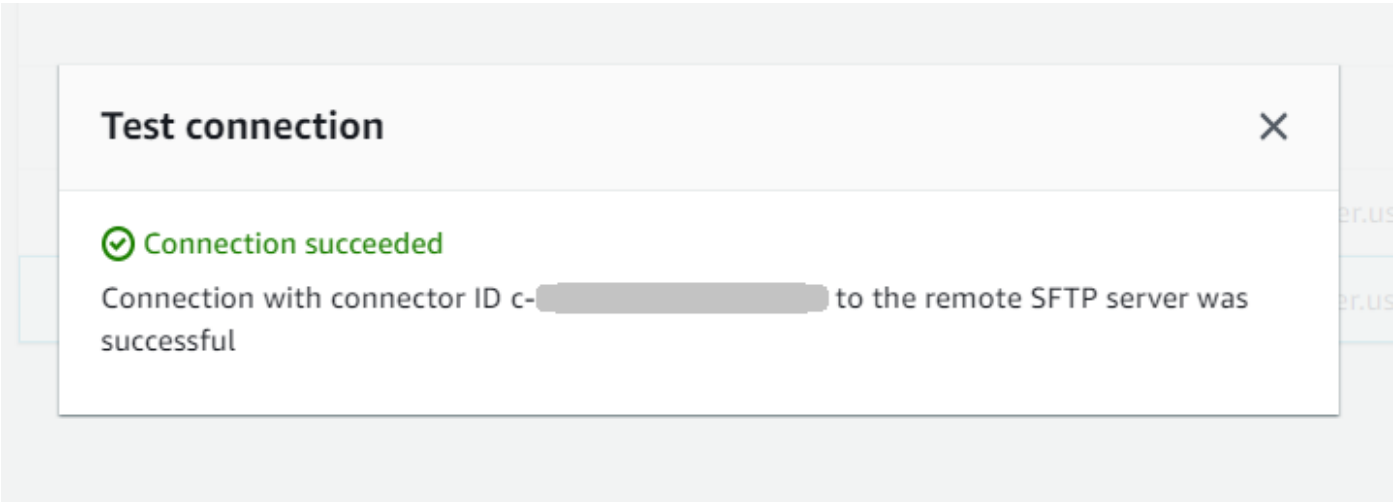
Test a connector using the console

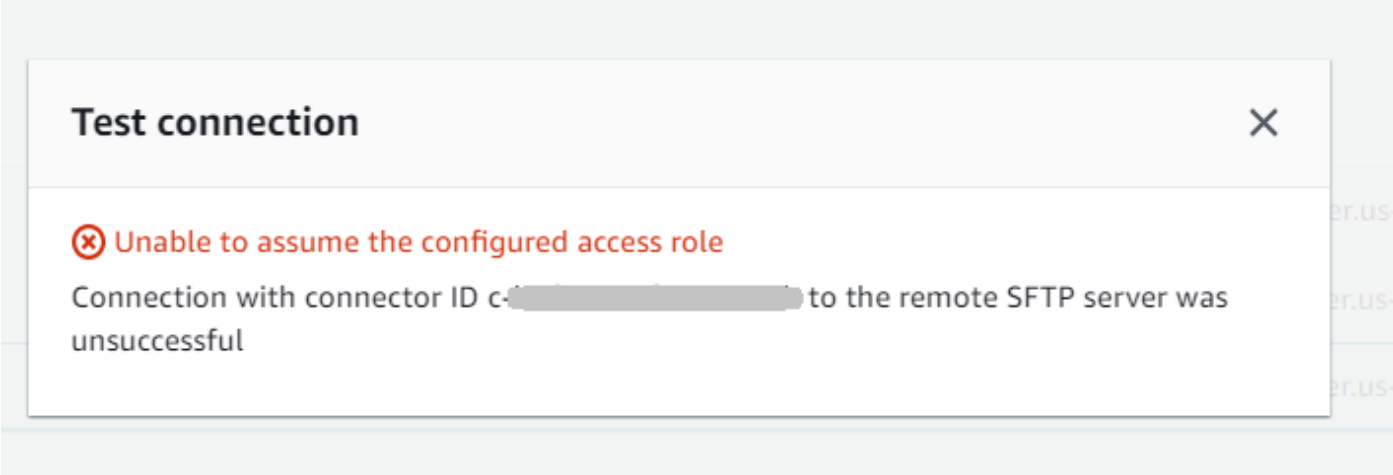
Per testare un connettore SFTP

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Connettori e seleziona un connettore.
3. Dal menu Azioni, scegli Verifica connessione.



Il sistema restituisce un messaggio che indica se il test ha esito positivo o negativo. Se il test fallisce, il sistema fornisce un messaggio di errore in base al motivo per cui il test non è riuscito.





Test a connector using the CLI

Per testare un connettore utilizzando il AWS Command Line Interface, esegui il comando seguente al prompt dei comandi (sostituisci *connector-id con l'ID* effettivo del connettore):

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

Se il test ha esito positivo, vengono restituite le seguenti righe:

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

Se il test non ha esito positivo, viene visualizzato un messaggio di errore descrittivo, ad esempio:

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

Passaggio 3: invio e recupero di file utilizzando il connettore SFTP

Per semplicità, supponiamo che tu abbia già dei file nel tuo bucket Amazon S3.

> **Note**
>
> Il tutorial utilizza i bucket Amazon S3 per le posizioni di storage di origine e destinazione. Se il tuo server SFTP non utilizza lo storage Amazon S3, ovunque tu `sftp-server-storage-east` veda nei seguenti comandi, puoi sostituire il percorso con un percorso verso le posizioni dei file accessibili dal tuo server SFTP.

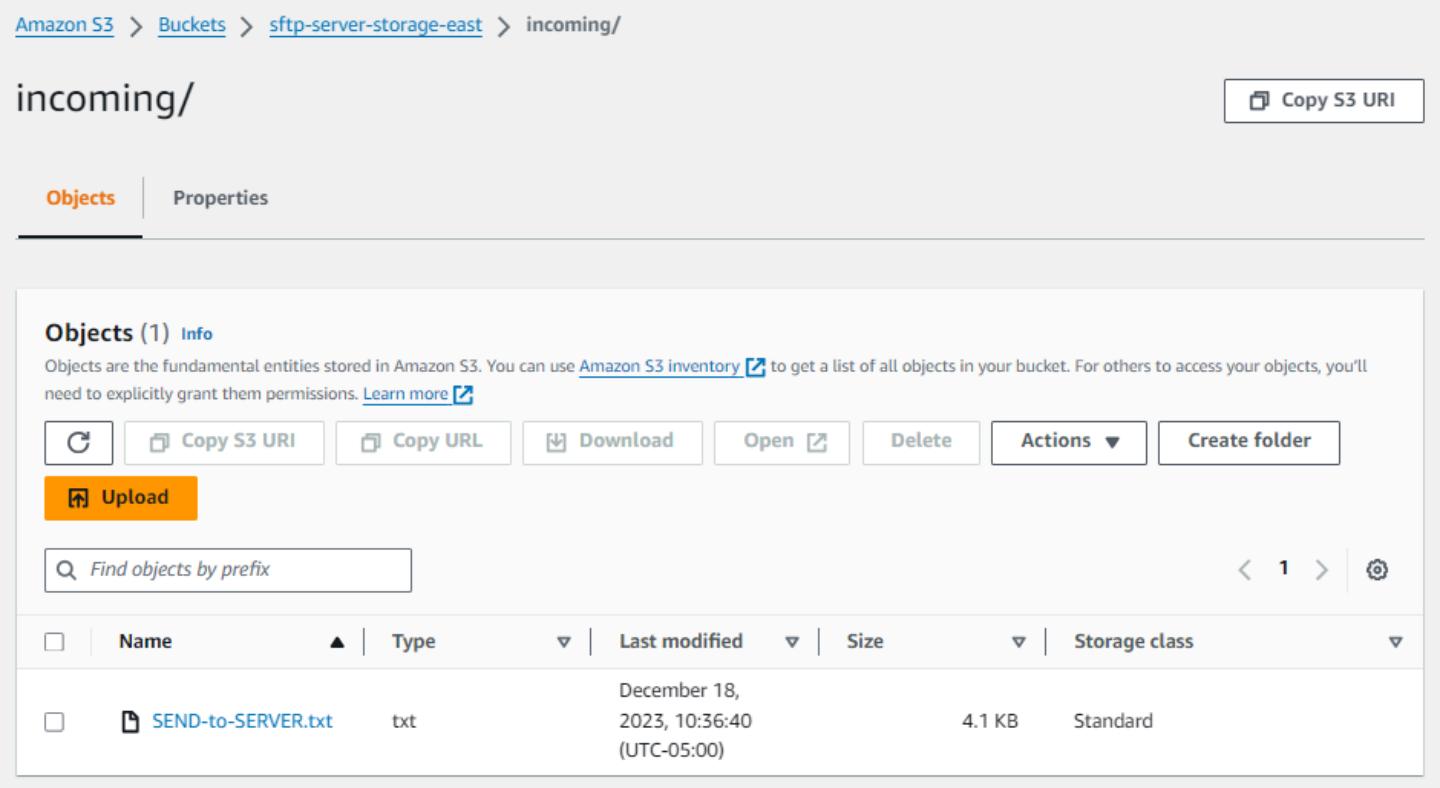
- Inviamo un file denominato `SEND-to-SERVER.txt` dallo storage Amazon S3 al server SFTP.
- Recuperiamo un file denominato `RETRIEVE-to-S3.txt` dal server SFTP nello storage Amazon S3.

> **Note**
>
> Nei seguenti comandi, sostituisci *`connector-id con il tuo ID del connettore`*.

Innanzitutto, inviamo un file dal nostro bucket Amazon S3 al server SFTP remoto. Da un prompt dei comandi, esegui il seguente 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"
```

Il tuo `sftp-server-storage-east` bucket dovrebbe ora avere questo aspetto.



Se non vedi il file come previsto, controlla i CloudWatch log.

Per controllare i tuoi registri CloudWatch

1. Apri la CloudWatch console Amazon all'indirizzo https://console.aws.amazon.com/cloudwatch/
2. Seleziona Log groups dal menu di navigazione a sinistra.
3. Inserisci l'ID del connettore nella barra di ricerca per trovare i log.
4. Seleziona il flusso di log che viene restituito dalla ricerca.
5. Espandi la voce di registro più recente.

In caso di successo, la voce di registro ha il seguente aspetto:

```
{
    "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",
```

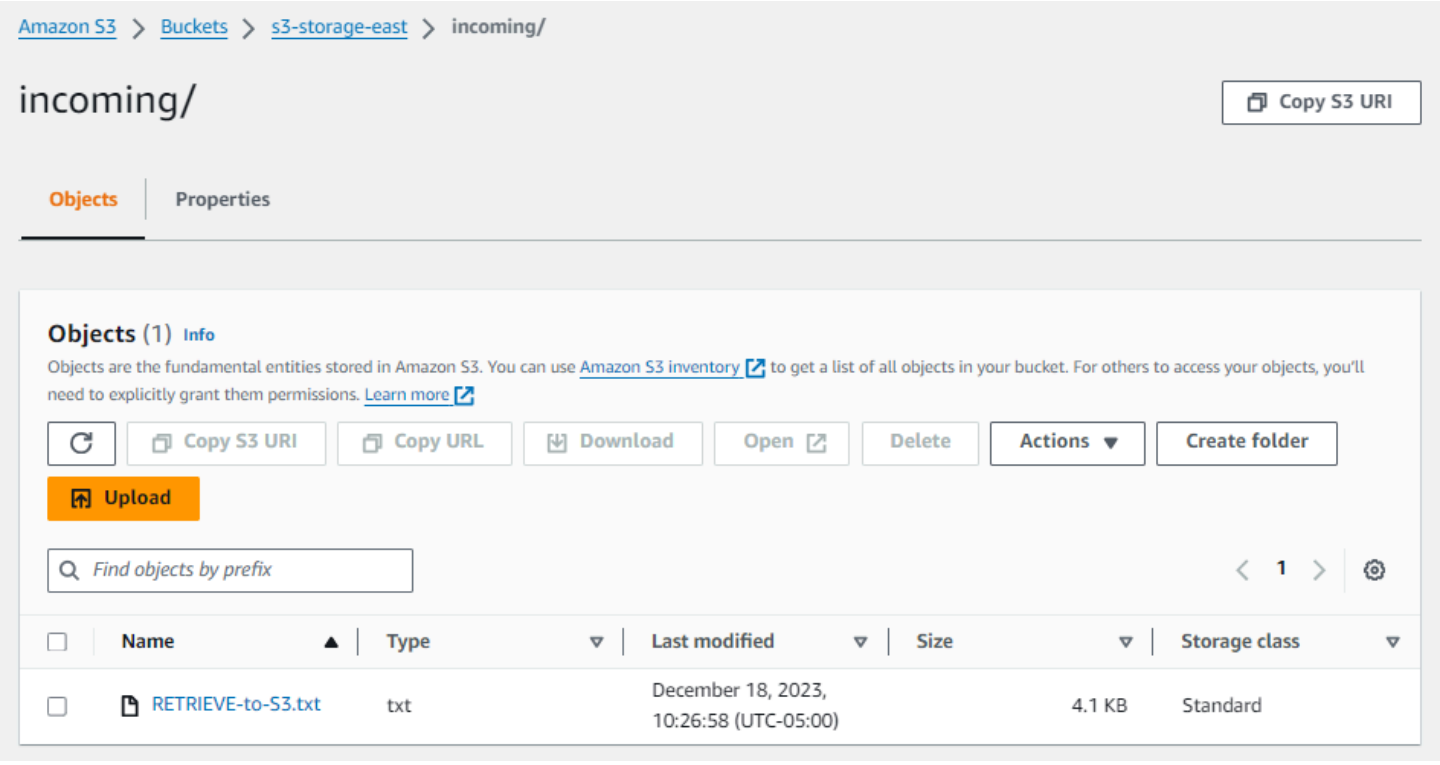
```
    "status-code": "COMPLETED",
    "start-time": "2023-12-18T15:26:56.915864Z",
    "end-time": "2023-12-18T15:26:57.298122Z",
    "account-id": "500655546075",
    "connector-arn": "arn:aws:transfer:us-east-1:500655546075:connector/connector-id",
    "remote-directory-path": "/sftp-server-storage-east/incoming"
}
```

Se il trasferimento del file non è riuscito, la voce di registro contiene un messaggio di errore che specifica il problema. Le cause più comuni degli errori sono i problemi con le autorizzazioni IAM e i percorsi di file errati.

Successivamente, recuperiamo un file dal server SFTP in un bucket Amazon S3. Da un prompt dei comandi, esegui il seguente 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"
```

Se il trasferimento ha esito positivo, il bucket Amazon S3 contiene il file trasferito, come illustrato di seguito.



In caso di successo, la voce di registro è simile alla seguente:

```
{
    "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"
}
```

Procedure per creare un server Transfer Family da utilizzare come server SFTP remoto

Di seguito, descriviamo i passaggi per creare un server Transfer Family che funga da server SFTP remoto per questo tutorial. Tieni presente quanto segue:

- Utilizziamo un server Transfer Family per rappresentare un server SFTP remoto. Gli utenti tipici del connettore SFTP dispongono di un proprio server SFTP remoto. Per informazioni, consulta Creare un server SFTP Transfer Family e un utente.
- Poiché utilizziamo un server Transfer Family, utilizziamo anche un utente SFTP gestito dal servizio. E, per semplicità, abbiamo combinato le autorizzazioni di cui questo utente ha bisogno per accedere al server Transfer Family con le autorizzazioni necessarie per utilizzare il nostro connettore. Anche in questo caso, la maggior parte dei casi d'uso del connettore SFTP prevede un utente SFTP separato che non è associato a un server Transfer Family. Per informazioni, consulta Creare un server SFTP Transfer Family e un utente.
- Per il tutorial, poiché utilizziamo lo storage Amazon S3 per il nostro server SFTP remoto, dobbiamo creare un secondo bucket**`s3-storage-east`**, in modo da poter trasferire i file da un bucket all'altro.

Creare un server SFTP Transfer Family e un utente

La maggior parte degli utenti non avrà bisogno di creare un server SFTP Transfer Family e un utente, poiché hai già un server SFTP con utenti e puoi utilizzare questo server per trasferire file da e verso. Tuttavia, per questo tutorial, per semplicità, utilizziamo un server Transfer Family per funzionare come server SFTP remoto.

Segui la procedura descritta in Crea un server compatibile con SFTP Per creare un server e Passaggio 3: Aggiungere un utente gestito dal servizio aggiungere un utente. Questi sono i dettagli utente che utilizziamo per il tutorial:

- Crea il tuo utente gestito dal servizio,. `sftp-testuser`
  - Imposta la home directory su `/sftp-server-storage-east/sftp-testuser`
  - Quando crei l'utente, memorizzi una chiave pubblica. Successivamente, quando crei il segreto in Secrets Manager, devi fornire la chiave privata corrispondente.
- Ruolo:`sftp-connector-role`. Per il tutorial, utilizziamo lo stesso ruolo IAM sia per il nostro utente SFTP che per accedere al connettore SFTP. Quando crei connettori per la tua organizzazione, potresti avere ruoli utente e di accesso separati.
- Chiave host del server: è necessario utilizzare la chiave host del server quando si crea il connettore. Puoi recuperare questa chiave eseguendo l'esecuzione `ssh-keyscan` sul tuo server. Ad esempio, se l'ID del server è `s-1111aaaa2222bbbb3` e il relativo endpoint è inserito`us-east-1`, il comando seguente recupera la chiave dell'host del server:

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

  Copia questo testo da qualche parte, poiché devi incollarlo nella Fase 2: Creare e testare un connettore SFTP procedura.

Utente e ruolo di accesso combinati

Per il tutorial, utilizziamo un singolo ruolo combinato. Utilizziamo questo ruolo sia per il nostro utente SFTP, sia per l'accesso al connettore. L'esempio seguente contiene i dettagli per questo ruolo, nel caso in cui si desideri eseguire le attività del tutorial.

L'esempio seguente concede le autorizzazioni necessarie per accedere ai nostri due bucket in Amazon S3 e al segreto denominato archiviato in `aws/transfer/sftp-connector1` Secrets Manager. Nel tutorial, questo ruolo è denominato. `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"
        }
    ]
}
```

Per i dettagli completi sulla creazione di ruoli per Transfer Family, segui la procedura descritta in Creazione di un ruolo utente Per creare un ruolo.

Configurazione di un metodo Amazon API Gateway come provider di identità personalizzato

Questo tutorial illustra come configurare un metodo Amazon API Gateway e utilizzarlo come provider di identità personalizzato per caricare file su un AWS Transfer Family server. Questo tutorial utilizza il modello di stack Basic e altre funzionalità di base solo come esempio.

Argomenti

Prerequisiti

Prima di creare le risorse Transfer Family in AWS CloudFormation, crea il tuo spazio di archiviazione e il tuo ruolo utente.

Per specificare lo spazio di archiviazione e creare un ruolo utente

1. A seconda dello storage in uso, consulta la seguente documentazione:
   - Per creare un bucket Amazon S3, vedi Come si crea un bucket S3? nella Guida per l'utente di Amazon Simple Storage Service.
   - Per creare un file system Amazon EFS, consultaConfigurazione di un file system Amazon EFS.
2. Per creare un ruolo utente, vedi Crea un ruolo e una policy IAM

I dettagli relativi allo spazio di archiviazione e al ruolo utente vengono immessi quando si crea AWS CloudFormation lo stack nella sezione successiva.

Fase 1: Creare uno stack CloudFormation

Per creare uno AWS CloudFormation stack a partire dal modello fornito

1. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
2. Seleziona Crea stack e scegli Con nuove risorse (standard).
3. Nel riquadro Prerequisito - Prepara il modello, scegli Il modello è pronto.
4. Copia questo link, modello di stack Basic, e incollalo nel campo URL di Amazon S3.
5. Fai clic su Next (Successivo).
6. Specificate i parametri, incluso un nome per lo stack. Assicuratevi di fare quanto segue:
   - Sostituite i valori predefiniti per UserNamee UserPassword.
   - Per UserHomeDirectory, inserisci i dettagli dello storage (un bucket Amazon S3 o un file system Amazon EFS) che hai creato in precedenza.
   - Sostituisci l'impostazione predefinita UserRoleArncon il ruolo utente creato in precedenza. Il ruolo AWS Identity and Access Management (IAM) deve disporre delle autorizzazioni appropriate. Per un esempio di politica del ruolo e del bucket di IAM, vedi. Passaggio 6: Limita l'accesso al bucket
   - Se desideri autenticarti utilizzando una chiave pubblica anziché una password, inserisci la tua chiave pubblica nel campo UserPublicKey1. La prima volta che ti connetti al server tramite SFTP, fornisci la chiave privata anziché una password.
7. Scegli Avanti, quindi scegli nuovamente Avanti nella pagina Configura le opzioni dello stack.
8. Esamina i dettagli dello stack che stai creando, quindi scegli Crea pila.

> **Note**
>
> Nella parte inferiore della pagina, in Capacità, devi riconoscere che AWS CloudFormation potrebbe creare risorse IAM.

Passaggio 2: verifica la configurazione del metodo API Gateway per il tuo server

> **Note**
>
> Per migliorare la sicurezza, puoi configurare un firewall per applicazioni Web. AWS WAF è un firewall per applicazioni Web che consente di monitorare le richieste HTTP e HTTPS inoltrate a un Amazon API Gateway. Per informazioni dettagliate, vedi Aggiungi un firewall per applicazioni Web.

Per verificare la configurazione del metodo API Gateway per il server e distribuirlo

1. Aprire la console Gateway API all'indirizzo https://console.aws.amazon.com/apigateway/.
2. Scegli l'API del modello di base di Transfer Custom Identity Provider generata dal AWS CloudFormation modello.
3. Nel riquadro Risorse, scegli GET, quindi scegli Method Request.
4. Per Azioni, scegli Deploy API. Per la fase di distribuzione, scegli prod, quindi scegli Deploy.

   Dopo che il metodo API Gateway è stato distribuito correttamente, visualizzane le prestazioni nella sezione Stage Editor.

   > **Note**
   >
   > Copia l'indirizzo URL di Invoke visualizzato nella parte superiore della pagina. Ti servirà per il passaggio successivo.

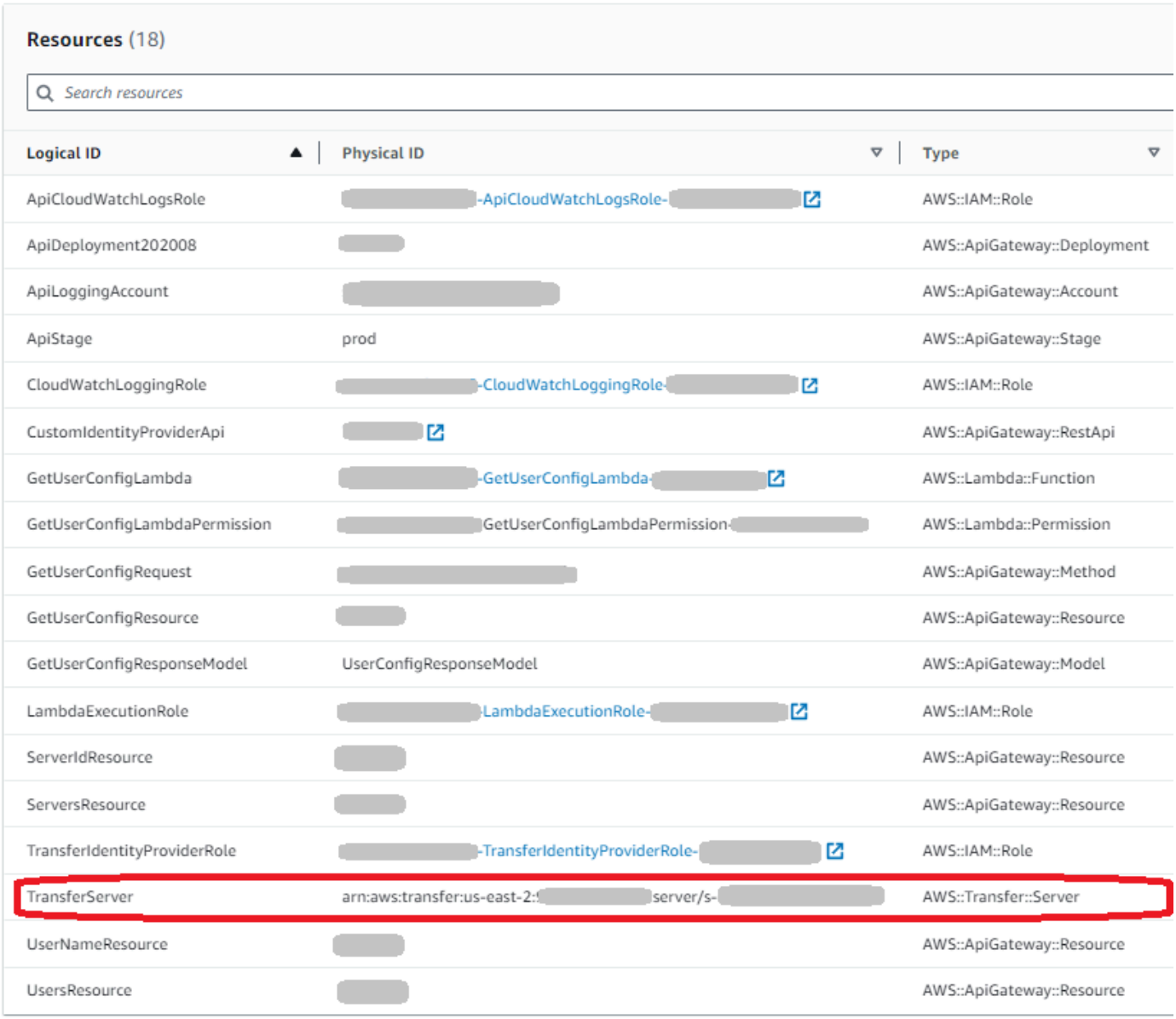
Fase 3: Visualizzare i dettagli del server Transfer Family

Quando si utilizza il modello per creare uno AWS CloudFormation stack, viene creato automaticamente un server Transfer Family.

Per visualizzare i dettagli del server Transfer Family

1. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.

2. Scegli lo stack che hai creato.
3. Scegliere la scheda Resources (Risorse).



L'ARN del server viene visualizzato nella colonna ID fisico della TransferServerriga. L'ID del server è contenuto nell'ARN, ad esempio s-11112222333344445.

4. Apri la AWS Transfer Family console all'[indirizzo https://console.aws.amazon.com/transfer/](https://console.aws.amazon.com/transfer/) e nella pagina Server, scegli il nuovo server.

   L'ID del server corrisponde all'ID visualizzato per la TransferServerrisorsa in AWS CloudFormation.

Fase 4: Verifica che l'utente sia in grado di connettersi al server

Per verificare che l'utente sia in grado di connettersi al server, utilizzando la console Transfer Family

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nella pagina Server, scegli il tuo nuovo server, scegli Azioni, quindi scegli Test.
3. Inserisci il testo delle tue credenziali di accesso nel campo Nome utente e nel campo Password. Questi sono i valori che hai impostato quando hai distribuito lo stack. AWS CloudFormation
4. Per Server Protocol, seleziona SFTP e per Source IP, inserisci. **`127.0.0.1`**
5. Scegli Test (Esegui test).

   Se l'autenticazione dell'utente ha esito positivo, il test restituisce una risposta `StatusCode: 200` HTML e un oggetto JSON contenente i dettagli dei ruoli e delle autorizzazioni dell'utente. Per esempio:

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

   Se il test fallisce, aggiungi una delle policy AWS gestite da API Gateway al ruolo che stai utilizzando per la tua API.

Passaggio 5: verifica la connessione SFTP e il trasferimento dei file

Per testare la connessione SFTP

1. Su un dispositivo Linux o macOS, apri un terminale di comando.
2. Inserisci uno dei seguenti comandi, a seconda che tu stia utilizzando una password o una key pair per l'autenticazione.

   - Se stai usando una password, inserisci questo comando:

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

Specifica la password, quando richiesto.

- Se stai usando una key pair, inserisci questo comando:

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

> **Note**
>
> Per questi `sftp` comandi, inserisci il codice relativo al Regione AWS luogo in cui si trova il tuo server Transfer Family. Ad esempio, se il tuo server si trova negli Stati Uniti orientali (Ohio), inserisci**`us-east-2`**.

3. Quando `sftp>` richiesto, assicuratevi di poter caricare (`put`), scaricare (`get`) e visualizzare cartelle e file (pwde). `ls`

Passaggio 6: Limita l'accesso al bucket

Puoi limitare chi può accedere a uno specifico bucket Amazon S3. L'esempio seguente mostra le impostazioni da utilizzare nello CloudFormation stack e nella politica selezionata per l'utente.

In questo esempio, impostiamo i seguenti parametri per lo AWS CloudFormation stack:

- CreateServer: `true`
- UserHomeDirectory: `/myuser-bucket`
- UserName: `myuser`
- UserPassword: `MySuperSecretPassword`

> **Important**
>
> Questa è una password di esempio. Quando configuri il metodo API Gateway, assicurati di inserire una password sicura.

- UserPublicKey1: *`your-public-key`*

- UserRoleArn: `arn:aws:iam::role-id:role/myuser-api-gateway-role`

L'UserPublicKey1 è una chiave pubblica che hai generato come parte di una coppia di chiavi pubblica/privata.

*role-id*È unico per il ruolo utente che crei. La politica allegata a `myuser-api-gateway-role` è la seguente:

```
{
    "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/*"
        }
    ]
}
```

Per connetterti al server tramite SFTP, inserisci uno dei seguenti comandi al prompt.

- Se utilizzate una password per l'autenticazione, eseguite il comando seguente:

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

  Specifica la password, quando richiesto.

- Se stai usando una key pair per l'autenticazione, esegui il seguente comando:

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

> **Note**
>
> Per questi `sftp` comandi, usa l'ID del Regione AWS luogo in cui si trova il tuo server Transfer Family. Ad esempio, se il tuo server si trova negli Stati Uniti orientali (Ohio), usa`us-east-2`.

Al `sftp` prompt, verrete indirizzati alla vostra home directory, che potete visualizzare eseguendo il pwd comando. Per esempio:

```
sftp> pwd
Remote working directory: /myuser-bucket
```

L'utente non può visualizzare alcuna directory al di sopra della home directory. Per esempio:

```
sftp> pwd
Remote working directory: /myuser-bucket
sftp> cd ..
sftp> ls
Couldn't read directory: Permission denied
```

Aggiorna Lambda se usi Amazon EFS

Se hai selezionato Amazon EFS come opzione di storage per il tuo server Transfer Family, devi modificare la funzione lambda per il tuo stack.

Per aggiungere un profilo Posix alla tua funzione Lambda

1. Apri la console Lambda all'indirizzo https://console.aws.amazon.com/lambda/.
2. Seleziona la funzione Lambda che hai creato in precedenza. *La funzione Lambda ha il formato* ***stack-name - GetUserConfigLambda - lambda-identifier, dove stack-name è il nome dello stack e lambda-identifier*** *è l'identificatore della funzione. CloudFormation*

3. Nella scheda Codice, selezionate index.js per visualizzare il codice per la funzione.
4. Nella`response`, aggiungi la seguente riga tra `Policy` e`HomeDirectory`:

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

   Dove *`uid-value e gid-value`* sono numeri interi, 0 o superiori, che rappresentano rispettivamente l'ID utente e l'ID del gruppo.

   Ad esempio, dopo aver aggiunto il profilo Posix, il campo di risposta potrebbe essere simile al seguente:

```
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 '/'
   };
```

Configurazione di una configurazione AS2

Questo tutorial spiega come impostare una configurazione AS2 (Applicability Statement 2) con. AWS Transfer Family Dopo aver completato i passaggi descritti qui, disporrai di un server abilitato per AS2 pronto ad accettare messaggi AS2 da un partner commerciale di esempio. Avrai anche un connettore che può essere utilizzato per inviare messaggi AS2 al partner commerciale campione.

> **Note**
>
> Alcune parti della configurazione di esempio utilizzano AWS Command Line Interface (AWS CLI). Se non avete ancora installato il file AWS CLI, consultate Installazione o aggiornamento della versione più recente di AWS CLI nella Guida per l'AWS Command Line Interface utente.

1. Crea certificati per te e per il tuo partner commerciale. Se disponi di certificati esistenti che puoi utilizzare, puoi saltare questa sezione.

   Questo processo è descritto inFase 1: Creare certificati per AS2.

2. Creare un AWS Transfer Family server che utilizzi il protocollo AS2. Facoltativamente, puoi aggiungere un indirizzo IP elastico al server per renderlo accessibile a Internet.

   Questo processo è descritto in. Fase 2: Creare un server Transfer Family che utilizzi il protocollo AS2

   > **Note**
   >
   > È necessario creare un server Transfer Family solo per i trasferimenti in entrata. Se esegui solo trasferimenti in uscita, non hai bisogno di un server Transfer Family.

3. Importa i certificati che hai creato nel passaggio 1.

   Questo processo è descritto inFase 3: Importazione dei certificati come risorse di certificati Transfer Family.

4. Per configurare i tuoi partner commerciali, crea un profilo locale e un profilo partner.

   Questo processo è descritto inFase 4: Crea profili per te e il tuo partner commerciale.

5. Crea un accordo tra te e il tuo partner commerciale.

   Questo processo è descritto inFase 5: Crea un accordo tra te e il tuo partner.

   > **Note**
   >
   > È necessario creare un accordo solo per i trasferimenti in entrata. Se esegui solo trasferimenti in uscita, non è necessario un accordo.

6. Crea un connettore tra te e il tuo partner commerciale.

   Questo processo è descritto inPassaggio 6: crea un connettore tra te e il tuo partner.

   > **Note**
   >
   > È necessario creare un connettore solo per i trasferimenti in uscita. Se esegui solo trasferimenti in entrata, non hai bisogno di un connettore.

7. Prova uno scambio di file AS2.

Questo processo è descritto in[Passaggio 7: Prova a scambiare file su AS2 utilizzando Transfer Family](#).

Dopo aver completato questi passaggi, puoi effettuare le seguenti operazioni:

- Inviate file a un server partner remoto abilitato per AS2 con il comando Transfer Family `start-file-transfer` AWS Command Line Interface (AWS CLI).
- Ricevi file da un server partner remoto abilitato per AS2 sulla porta 5080 tramite l'endpoint del cloud privato virtuale (VPC).

Fase 1: Creare certificati per AS2

Entrambe le parti in uno scambio AS2 necessitano di certificati X.509. Puoi creare questi certificati nel modo che preferisci. Questo argomento descrive come utilizzare OpenSSL dalla riga di comando per creare un certificato root e quindi firmare certificati subordinati. Entrambe le parti devono generare i propri certificati.

> **Note**
>
> La lunghezza della chiave per i certificati AS2 deve essere di almeno 2048 bit e al massimo di 4096.

Per trasferire file con un partner, prendi nota di quanto segue:

- È possibile allegare certificati ai profili. I certificati contengono chiavi pubbliche o private.
- Il tuo partner commerciale ti invia le sue chiavi pubbliche e tu le invii le tue.
- Il tuo partner commerciale cripta i messaggi con la tua chiave pubblica e li firma con la sua chiave privata. Al contrario, tu crittografi i messaggi con la chiave pubblica del tuo partner e li firmi con la tua chiave privata.

> **Note**
>
> Se preferisci gestire le chiavi con una GUI, Portecleè un'opzione che puoi usare.

Per generare certificati di esempio

> **Important**
>
> Non inviate al vostro partner le vostre chiavi private. In questo esempio, si genera un set di chiavi pubbliche e private autofirmate per una parte. Se intendete agire come entrambi partner commerciali a scopo di test, potete ripetere queste istruzioni per generare due set di chiavi: uno per ogni partner commerciale. In questo caso, non è necessario generare due autorità di certificazione (CA) principali.

1. Esegui il comando seguente per generare una chiave privata RSA con un modulo lungo 2048 bit.

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

2. Esegui il comando seguente per creare un certificato autofirmato con il tuo file. `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
```

L'`-subj`argomento è composto dai seguenti valori.

	Nome	Descrizione
`C`	Codice del paese	Un codice di due lettere per il paese in cui ha sede l'organizzazione.
`ST`	Stato, regione o provincia	Lo stato, la regione o la provincia in cui ha sede l'organizzazione. (In questo caso, la regione non si

	Nome	Descrizione
		riferisce al tuo Regione AWS.)
L	Locality name (Nome località)	La città in cui ha sede l'organizzazione.
O	Nome organizzazione	Il nome legale completo dell'organizzazione, compresi i suffissi, come LLC, Corp e così via.
OU	Nome dell'unità organizzativa	La divisione dell'orga nizzazione che si occupa di questo certificato.
CN	Nome comune o nome di dominio completo (FQDN)	In questo caso, stiamo creando un certificato root, quindi il valore è. `ROOTCA` In questi esempi, lo useremo `CN` per descrivere lo scopo del certificato.

3. Crea una chiave di firma e una chiave di crittografia per il tuo profilo locale.

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

> **Note**
>
> Alcuni server compatibili con AS2, come OpenAS2, richiedono l'utilizzo dello stesso certificato sia per la firma che per la crittografia. In questo caso, puoi importare la stessa chiave privata e lo stesso certificato per entrambi gli scopi. A tale scopo, esegui questo comando anziché i due comandi precedenti:
>
> ```
> /usr/bin/openssl genrsa -out signing-and-encryption-key.pem 2048
> ```

4. Esegui i seguenti comandi per creare richieste di firma dei certificati (CSR) per la firma della chiave principale.

```
/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. Successivamente, è necessario creare un `signing-cert.conf` file e un `encryption-cert.conf` file.

   - Utilizzate un editor di testo per creare il `signing-cert.conf` file con i seguenti contenuti:

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

   - Utilizzate un editor di testo per creare il `encryption-cert.conf` file con i seguenti contenuti:

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

6. Infine, crei i certificati firmati eseguendo i seguenti comandi.

```
/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
```

Fase 2: Creare un server Transfer Family che utilizzi il protocollo AS2

Questa procedura spiega come creare un server compatibile con AS2 utilizzando Transfer Family. AWS CLI

> **Note**
>
> Molti dei passaggi di esempio utilizzano comandi che caricano i parametri da un file. Per maggiori dettagli sull'utilizzo dei file per caricare i parametri, vedete Come caricare i parametri da un file.

Se invece desideri utilizzare la console, consultaCreare un server AS2 utilizzando la console Transfer Family.

Analogamente a come si crea un server SFTP o FTPS, si crea un AWS Transfer Family server abilitato per AS2 utilizzando il `--protocols AS2` parametro del comando. `create-server` AWS CLI Attualmente, Transfer Family supporta solo i tipi di endpoint VPC e lo storage Amazon S3 con il protocollo AS2.

Quando crei il tuo server abilitato per AS2 per Transfer Family utilizzando il `create-server` comando, viene creato automaticamente un endpoint VPC. Questo endpoint espone la porta TCP 5080 in modo da poter accettare messaggi AS2.

Se desideri esporre pubblicamente il tuo endpoint VPC a Internet, puoi associare indirizzi IP elastici al tuo endpoint VPC.

Per utilizzare queste istruzioni, è necessario quanto segue:

- L'ID del tuo VPC (ad esempio, vpc-abcdef01).
- Gli ID delle sottoreti VPC (ad esempio subnet-abcdef01, subnet-subnet-abcdef01, subnet-021345ab).
- Uno o più ID dei gruppi di sicurezza che consentono il traffico in entrata sulla porta TCP 5080 dai partner commerciali (ad esempio, sg-1234567890abcdef0 e sg-abcdef01234567890).
- (Facoltativo) Gli indirizzi IP elastici che desideri associare al tuo endpoint VPC.
- Se il tuo partner commerciale non è connesso al tuo VPC tramite una VPN, hai bisogno di un gateway Internet. Per ulteriori informazioni, consulta Collegamento delle sottoreti a Internet tramite un gateway Internet nella Guida per l'utente di Amazon VPC.

Per creare un server compatibile con AS2

1. Esegui il comando seguente. Sostituisci ogni *`user input placeholder`* con le tue informazioni.

```
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. (Facoltativo) Puoi rendere pubblico l'endpoint VPC. È possibile collegare indirizzi IP elastici a un server Transfer Family solo tramite un'`update-server`operazione. I seguenti comandi arrestano il server, lo aggiornano con indirizzi IP Elastic e quindi lo riavviano.

   ```
   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-abcd012345ccccccc
   ```

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

   Questo `start-server` comando crea automaticamente un record DNS che contiene l'indirizzo IP pubblico del server. Per consentire al tuo partner commerciale di accedere al server, fornisci loro le seguenti informazioni. In questo caso, *`your-region`* si riferisce al tuo Regione AWS.

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

   L'URL completo che fornisci al tuo partner commerciale è il seguente:

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

3. Per verificare se il server abilitato per AS2 è accessibile, usa i seguenti comandi. Assicurati che sia possibile accedere al server tramite l'indirizzo DNS privato dell'endpoint VPC o tramite l'endpoint pubblico (se hai associato un indirizzo IP elastico all'endpoint).

   Se il server è configurato correttamente, la connessione avrà successo. Tuttavia, riceverai una risposta con codice di stato HTTP 400 (Bad Request) perché non stai inviando un messaggio AS2 valido.

   - Per un endpoint pubblico (se hai associato un indirizzo IP elastico nel passaggio precedente), esegui il comando seguente, sostituendo l'ID del server e la regione.

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

- Se ti connetti all'interno del tuo VPC, cerca il nome DNS privato dell'endpoint VPC eseguendo i seguenti comandi.

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

  Questo `describe-server` comando restituisce l'ID dell'endpoint VPC nel parametro. `VpcEndpointId` Utilizzate questo valore per eseguire il comando seguente.

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

  Questo `describe-vpc-endpoints` comando restituisce un `DNSEntries` array con diversi `DnsName` parametri. Utilizzate il nome DNS regionale (quello che non include la zona di disponibilità) nel comando seguente.

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

  Ad esempio, il comando seguente mostra valori di esempio per i segnaposto del comando precedente.

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

4. (Facoltativo) Configura un ruolo di registrazione. Transfer Family registra lo stato dei messaggi inviati e ricevuti in un formato JSON strutturato nei log di Amazon CloudWatch . Per fornire a Transfer Family l'accesso ai CloudWatch registri del tuo account, devi configurare un ruolo di registrazione sul tuo server.

   Crea un ruolo AWS Identity and Access Management (IAM) affidabile e allega `transfer.amazonaws.com` la policy gestita`AWSTransferLoggingAccess`. Per informazioni dettagliate, vedi Crea un ruolo e una policy IAM. Prendi nota dell'Amazon Resource Name (ARN) del ruolo IAM appena creato e associalo al server eseguendo il seguente 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**
>
> Anche se il ruolo di registrazione è facoltativo, consigliamo vivamente di configurarlo in modo da poter visualizzare lo stato dei messaggi e risolvere i problemi di configurazione.

Fase 3: Importazione dei certificati come risorse di certificati Transfer Family

Questa procedura spiega come importare i certificati utilizzando AWS CLI. Se invece desideri utilizzare la console Transfer Family, consultathe section called “Importa certificati AS2”.

Per importare i certificati di firma e crittografia creati nel passaggio 1, esegui i seguenti `import-certificate` comandi. Se utilizzi lo stesso certificato per la crittografia e la firma, importa lo stesso certificato due volte (una volta con l'`SIGNING`utilizzo e un'altra con l'`ENCRYPTION`utilizzo).

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

Questo comando restituisce la tua firma`CertificateId`. Nella sezione successiva, questo ID del certificato viene denominato*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
```

Questo comando restituisce la crittografia`CertificateId`. Nella sezione successiva, questo ID del certificato viene denominato*my-encrypt-cert-id*.

Successivamente, importa i certificati di crittografia e firma del tuo partner eseguendo i seguenti comandi.

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

```
--certificate-chain file://partner-root-ca.pem
```

Questo comando restituisce la crittografia del tuo partner`CertificateId`. Nella sezione successiva, questo ID del certificato viene denominato*partner-encrypt-cert-id*.

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

Questo comando restituisce la firma del partner`CertificateId`. Nella sezione successiva, questo ID del certificato viene denominato*partner-signing-cert-id*.

Fase 4: Crea profili per te e il tuo partner commerciale

Questa procedura spiega come creare profili AS2 utilizzando AWS CLI. Se invece desideri utilizzare la console Transfer Family, consultathe section called “Crea profili AS2”.

Crea il tuo profilo AS2 locale eseguendo il comando seguente. Questo comando fa riferimento ai certificati che contengono le tue chiavi pubbliche e private.

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

Questo comando restituisce l'ID del profilo. Nella sezione successiva, questo ID viene denominato*my-profile-id*.

Ora crea il profilo partner eseguendo il seguente comando. Questo comando utilizza solo i certificati a chiave pubblica del tuo partner. Per utilizzare questo comando, sostituiscilo *user input placeholders* con le tue informazioni, ad esempio il nome AS2 e gli ID del certificato del tuo partner.

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

Questo comando restituisce l'ID del profilo del tuo partner. Nella sezione successiva, questo ID viene denominato*partner-profile-id*.

> **Note**
>
> Nei comandi precedenti, sostituite *MYCORP* con il nome della vostra organizzazione e *PARTNER-COMPANY* con il nome dell'organizzazione del vostro partner commerciale.

Fase 5: Crea un accordo tra te e il tuo partner

Questa procedura spiega come creare accordi AS2 utilizzando. AWS CLI Se invece desideri utilizzare la console Transfer Family, consultathe section called “Crea accordi AS2”.

Gli accordi riuniscono i due profili (locale e partner), i relativi certificati e una configurazione del server che consente i trasferimenti AS2 in entrata tra due parti. Puoi elencare i tuoi articoli eseguendo i seguenti comandi.

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

Questo passaggio richiede un bucket Amazon S3 e un ruolo IAM con accesso in lettura/scrittura da e verso il bucket. Le istruzioni per creare questo ruolo sono le stesse dei protocolli SFTP, FTP e FTPS di Transfer Family e sono disponibili in. Crea un ruolo e una policy IAM

Per creare un accordo, sono necessari i seguenti elementi:

- Il nome del bucket Amazon S3 (e il prefisso dell'oggetto, se specificato)
- L'ARN del ruolo IAM con accesso al bucket
- L'ID del tuo server Transfer Family
- L'ID del tuo profilo e l'ID del profilo del tuo partner

Crea l'accordo eseguendo il comando seguente.

```
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
```

In caso di successo, questo comando restituisce l'ID dell'accordo. È quindi possibile visualizzare i dettagli dell'accordo con il seguente comando.

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

Passaggio 6: crea un connettore tra te e il tuo partner

Questa procedura spiega come creare connettori AS2 utilizzando il AWS CLI. Se invece desideri utilizzare la console Transfer Family, consultathe section called “Configura i connettori AS2”.

Puoi utilizzare l'operazione `StartFileTransfer` API per inviare file archiviati in Amazon S3 all'endpoint AS2 del tuo partner commerciale utilizzando un connettore. Puoi trovare i profili che hai creato in precedenza eseguendo il comando seguente.

```
aws transfer list-profiles
```

Quando crei il connettore, devi fornire l'URL del server AS2 del tuo partner. Copia il testo seguente in un file denominato`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**
>
> Infatti`EncryptionAlgorithm`, non specificate l'`DES_EDE3_CBC`algoritmo a meno che non dobbiate supportare un client legacy che lo richiede, poiché si tratta di un algoritmo di crittografia debole.

Quindi esegui il comando seguente per creare il connettore.

```
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
```

Passaggio 7: Prova a scambiare file su AS2 utilizzando Transfer Family

Ricevi un file dal tuo partner commerciale

Se hai associato un indirizzo IP elastico pubblico al tuo endpoint VPC, Transfer Family ha creato automaticamente un nome DNS che contiene il tuo indirizzo IP pubblico. Il sottodominio è l'ID AWS Transfer Family del tuo server (del formato). `s-1234567890abcdef0` Fornisci l'URL del tuo server al tuo partner commerciale nel seguente formato.

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

Se non hai associato un indirizzo IP elastico pubblico al tuo endpoint VPC, cerca il nome host dell'endpoint VPC in grado di accettare messaggi AS2 su HTTP POST dai tuoi partner commerciali sulla porta 5080. Per recuperare i dettagli dell'endpoint VPC, usa il seguente comando.

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

Ad esempio, supponiamo che il comando precedente restituisca un ID endpoint VPC di. `vpce-1234abcd5678efghi` Quindi, è necessario utilizzare il comando seguente per recuperare i nomi DNS.

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

Questo comando restituisce tutti i dettagli per l'endpoint VPC necessari per eseguire il comando seguente.

Il nome DNS è elencato nell'array. `DnsEntries` Il tuo partner commerciale deve trovarsi all'interno del tuo VPC per accedere al tuo endpoint VPC (ad esempio tramite AWS PrivateLink una VPN). Fornisci l'URL dell'endpoint VPC al tuo partner nel seguente formato.

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

Ad esempio, l'URL seguente mostra valori di esempio per i segnaposto dei comandi precedenti.

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

In questo esempio, i trasferimenti riusciti vengono archiviati nella posizione specificata nel `base-directory` parametro specificato in. Fase 5: Crea un accordo tra te e il tuo partner Se riceviamo correttamente i file denominati `myfile1.txt` and`myfile2.txt`, i file vengono archiviati come/*`path-defined-in-the-agreement`*/`processed/`*`original_filename.messageId.original_extension`*. Qui, i file vengono archiviati come `/DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox/processed/myfile1.`*`messageId`*`.txt` e`/DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox/processed/myfile2.`*`messageId`*`.txt`.

Se hai configurato un ruolo di registrazione quando hai creato il server Transfer Family, puoi anche controllare CloudWatch i log per verificare lo stato dei messaggi AS2.

Invia un file al tuo partner commerciale

È possibile utilizzare Transfer Family per inviare messaggi AS2 facendo riferimento all'ID del connettore e ai percorsi dei file, come illustrato nel seguente 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"
```

Per ottenere i dettagli dei connettori, esegui il seguente comando:

```
aws transfer list-connectors
```

Il `list-connectors` comando restituisce gli ID dei connettori, gli URL e gli Amazon Resource Names (ARN) per i connettori.

Per restituire le proprietà di un particolare connettore, esegui il comando seguente con l'ID che desideri utilizzare:

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

Il `describe-connector` comando restituisce tutte le proprietà del connettore, inclusi l'URL, i ruoli, i profili, gli mDNS (Message Disposition Notices), i tag e le metriche di monitoraggio.

È possibile confermare che il partner ha ricevuto correttamente i file visualizzando i file JSON e MDN. Questi file sono denominati in base alle convenzioni descritte in. Nomi e posizioni dei file
Se hai configurato un ruolo di registrazione quando hai creato il connettore, puoi anche controllare CloudWatch nei log lo stato dei messaggi AS2.

Configurazione di un endpoint server SFTP, FTPS o FTP

Questo argomento fornisce dettagli sulla creazione e l'utilizzo di endpoint AWS Transfer Family server che utilizzano uno o più protocolli SFTP, FTPS e FTP.

Argomenti

Opzioni del provider di identità

AWS Transfer Family fornisce diversi metodi per l'autenticazione e la gestione degli utenti. La tabella seguente confronta i provider di identità disponibili che puoi utilizzare con Transfer Family.

Azione	AWS Transfer Family servizio gestito	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
Protocolli supportati	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
Autenticazione basata su chiavi	Sì	No	Sì	Sì
Autenticazione password	No	Sì	Sì	Sì
AWS Identity and Access Management (IAM) e POSIX	Sì	Sì	Sì	Sì

Azione	AWS Transfer Family servizio gestito	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
cartella home logica	Sì	Sì	Sì	Sì
Accesso parametrizzato (basato sul nome utente)	Sì	Sì	Sì	Sì
Struttura di accesso ad hoc	Sì	No	Sì	Sì
AWS WAF	No	No	Sì	No

Note:

- IAM viene utilizzato per controllare l'accesso per lo storage di backup di Amazon S3 e POSIX viene utilizzato per Amazon EFS.
- Ad hoc si riferisce alla possibilità di inviare il profilo utente in fase di esecuzione. Ad esempio, puoi indirizzare gli utenti nelle loro home directory passando il nome utente come variabile.
- Per ulteriori informazioni su AWS WAF, vedereAggiungi un firewall per applicazioni Web.
- C'è un post sul blog che descrive l'utilizzo di una funzione Lambda integrata con Microsoft Azure AD come provider di identità Transfer Family. Per i dettagli, vedere Autenticazione AWS Transfer Family con Azure Active Directory e. AWS Lambda
- Forniamo diversi AWS CloudFormation modelli per aiutarti a implementare rapidamente un server Transfer Family che utilizza un provider di identità personalizzato. Per informazioni dettagliate, vedi Modelli di funzioni Lambda.

Nelle seguenti procedure, è possibile creare un server abilitato per SFTP, un server abilitato per FTPS, un server abilitato per FTP o un server abilitato per AS2.

Approfondimenti

- Crea un server compatibile con SFTP

- Creare un server compatibile con FTPS
- Crea un server abilitato all'FTP
- Configurazione di AS2

AWS Transfer Family matrice del tipo di endpoint

Quando crei un server Transfer Family, scegli il tipo di endpoint da utilizzare. La tabella seguente descrive le caratteristiche per ogni tipo di endpoint.

Matrice del tipo di endpoint

Caratteristica	Pubblica	VPC - Internet	VPC - Interno	VPC_Endpoint (obsoleto)
Protocolli supportati	SFTP	SFTP, FTPS, AS2	SFTP, FTP, FTPS, AS2	SFTP
Accesso	Da Internet. Questo tipo di endpoint non richiede alcuna configurazione speciale nel tuo VPC.	Tramite Internet e dall'interno di ambienti VPC e connessi a VPC, come un data center locale o una VPN. AWS Direct Connect	Dall'interno di ambienti VPC e connessi a VPC, come un data center locale o una VPN. AWS Direct Connect	Dall'interno di ambienti VPC e connessi a VPC, come un data center locale o una VPN. AWS Direct Connect
Indirizzo IP statico	Non è possibile allegare un indirizzo IP statico. AWS fornisce indirizzi IP soggetti a modifiche.	È possibile collegare indirizzi IP elastici all'endpoint. Questi possono essere indirizzi AWS IP di proprietà o indirizzi IP personali (Bring your own IP	Gli indirizzi IP privati collegati all'endpoint non cambiano.	Gli indirizzi IP privati collegati all'endpoint non cambiano.

Caratteristica	Pubblica	VPC - Internet	VPC - Interno	VPC_Endpoint (obsoleto)
		address). Gli indirizzi IP elastici collegati all'endpoint non cambiano. Inoltre, gli indirizzi IP privati collegati al server non vengono modificati.		

Caratteristica	Pubblica	VPC - Internet	VPC - Interno	VPC_Endpoint (obsoleto)
Elenco degli IP consentiti di origine	Questo tipo di endpoint non supporta gli elenchi consentiti per indirizzi IP di origine. L'endpoint è accessibile al pubblico e ascolta il traffico sulla porta 22. **Note** Per gli endpoint ospitati su VPC, i server SFTP Transfer Family possono funzionare sulla porta 22 (impostazione predefinita), la porta 2222 o	Per consentire l'accesso tramite l'indirizzo IP di origine, è possibile utilizzare i gruppi di sicurezza collegati agli endpoint del server e gli ACL di rete collegati alla sottorete in cui si trova l'endpoint.	Per consentire l'accesso tramite indirizzo IP di origine, è possibile utilizzare i gruppi di sicurezza collegati agli endpoint del server e le liste di controllo dell'accesso alla rete (ACL di rete) collegate alla sottorete in cui si trova l'endpoint.	Per consentire l'accesso tramite indirizzo IP di origine, è possibile utilizzare i gruppi di sicurezza collegati agli endpoint del server e gli ACL di rete collegati alla sottorete in cui si trova l'endpoint.

Caratteristica	Pubblica	VPC - Internet	VPC - Interno	VPC_Endpoint (obsoleto)
	la porta 22000.			
Elenco degli indirizzi consentiti dal firewall del client	È necessario consentire il nome DNS del server. Poiché gli indirizzi IP sono soggetti a modifiche, evita di utilizzare gli indirizzi IP per l'elenco consentito del firewall del client.	È possibile consentire il nome DNS del server o gli indirizzi IP elastici collegati al server.	È possibile consentire gli indirizzi IP privati o il nome DNS degli endpoint.	È possibile consentire gli indirizzi IP privati o il nome DNS degli endpoint.

> **Note**
>
> Il tipo di `VPC_ENDPOINT` endpoint è ora obsoleto e non può essere utilizzato per creare nuovi server. Invece di utilizzare`EndpointType=VPC_ENDPOINT`, utilizza il nuovo tipo di endpoint VPC (`EndpointType=VPC`), che puoi usare come interfaccia interna o Internet, come descritto nella tabella precedente. Per informazioni dettagliate, vedi Interruzione dell'uso di VPC_ENDPOINT.

Considerate le seguenti opzioni per aumentare il livello di sicurezza del vostro server: AWS Transfer Family

- Utilizza un endpoint VPC con accesso interno, in modo che il server sia accessibile solo ai client all'interno del tuo VPC o agli ambienti connessi a VPC, come un data center locale o una VPN. AWS Direct Connect

- Per consentire ai client di accedere all'endpoint tramite Internet e proteggere il server, utilizza un endpoint VPC con accesso a Internet. Quindi, modifica i gruppi di sicurezza del VPC per consentire il traffico solo da determinati indirizzi IP che ospitano i client degli utenti.
- Se richiedi l'autenticazione basata su password e utilizzi un provider di identità personalizzato con il tuo server, è buona norma che la politica in materia di password impedisca agli utenti di creare password deboli e limiti il numero di tentativi di accesso non riusciti.
- AWS Transfer Family è un servizio gestito e quindi non fornisce l'accesso alla shell. Non è possibile accedere direttamente al server SFTP sottostante per eseguire comandi nativi del sistema operativo sui server Transfer Family.
- Usa un Network Load Balancer davanti a un endpoint VPC con accesso interno. Cambia la porta del listener sul load balancer dalla porta 22 a una porta diversa. Ciò può ridurre, ma non eliminare, il rischio che scanner di porte e bot controllino il server, poiché la porta 22 è la più comunemente utilizzata per la scansione. Per maggiori dettagli, consulta il post sul blog Network Load Balancer now support Security groups.

> **Note**
>
> Se si utilizza un Network Load Balancer, AWS Transfer Family CloudWatch i log mostrano l'indirizzo IP dell'NLB, anziché l'indirizzo IP effettivo del client.

Configurazione di un endpoint server SFTP, FTPS o FTP

È possibile creare un server di trasferimento file utilizzando il servizio. AWS Transfer Family Sono disponibili i seguenti protocolli di trasferimento file:

- Secure Shell (SSH) File Transfer Protocol (SFTP): trasferimento di file tramite SSH. Per informazioni dettagliate, vedi the section called “Creare un server compatibile con SFTP”.

> **Note**
>
> Forniamo un AWS CDK esempio per la creazione di un server SFTP Transfer Family. L'esempio utilizza TypeScript ed è disponibile GitHub qui.

- File Transfer Protocol Secure (FTPS): trasferimento di file con crittografia TLS. Per informazioni dettagliate, vedi the section called “Crea un server abilitato per FTPS”.

- File Transfer Protocol (FTP): trasferimento di file non crittografato. Per informazioni dettagliate, vedi the section called “Crea un server abilitato per FTP”.
- Dichiarazione di applicabilità 2 (AS2) — Trasferimento di file per il trasporto di dati strutturati. business-to-business Per informazioni dettagliate, vedi the section called “Configurare AS2”. Per AS2, puoi creare rapidamente uno AWS CloudFormation stack a scopo dimostrativo. Questa procedura è descritta in. Usa un modello per creare uno stack demo Transfer Family AS2

È possibile creare un server con più protocolli.

> **Note**
>
> Se hai più protocolli abilitati per lo stesso endpoint server e desideri fornire l'accesso utilizzando lo stesso nome utente su più protocolli, puoi farlo purché le credenziali specifiche del protocollo siano state configurate nel tuo provider di identità. Per FTP, consigliamo di mantenere credenziali separate da SFTP e FTPS. Questo perché, a differenza di SFTP e FTPS, FTP trasmette le credenziali in testo non crittografato. Isolando le credenziali FTP da SFTP o FTPS, se le credenziali FTP sono condivise o esposte, i carichi di lavoro che utilizzano SFTP o FTPS rimangono sicuri.

Quando create un server, ne scegliete uno specifico Regione AWS per eseguire le richieste di gestione dei file degli utenti assegnati a quel server. Oltre ad assegnare al server uno o più protocolli, si assegna anche uno dei seguenti tipi di provider di identità:

- Servizio gestito tramite chiavi SSH. Per informazioni dettagliate, vedi Lavorare con utenti gestiti dal servizio.
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Questo metodo consente di integrare i gruppi Microsoft Active Directory per fornire l'accesso ai server Transfer Family. Per informazioni dettagliate, vedi Utilizzo del provider di identità AWS Directory Service.
- Un metodo personalizzato. Il metodo del provider di identità personalizzato utilizza AWS Lambda Amazon API Gateway e consente di integrare il servizio di directory per autenticare e autorizzare gli utenti. Il servizio assegna automaticamente un identificatore che identifica in modo univoco il server. Per informazioni dettagliate, vedi Lavorare con provider di identità personalizzati. Transfer Family fornisce AWS CloudFormation modelli che è possibile utilizzare per distribuire rapidamente server che utilizzano un provider di identità personalizzato.

- Funzioni Lambda per l'autenticazionedescrive CloudFormation i modelli che utilizzano una funzione Lambda per l'autenticazione.
- Autenticazione tramite un metodo API Gatewaydescrive CloudFormation i modelli che utilizzano un metodo Amazon API Gateway per l'autenticazione.

Puoi anche assegnare al server un tipo di endpoint (accessibile pubblicamente o ospitato su VPC) e un nome host utilizzando l'endpoint server predefinito o un nome host personalizzato utilizzando il servizio Amazon Route 53 o utilizzando un servizio DNS (Domain Name System) a tua scelta. Il nome host del server deve essere univoco nel luogo in cui è stato creato. Regione AWS

Inoltre, puoi CloudWatch assegnare un ruolo di registrazione di Amazon per inviare eventi ai tuoi CloudWatch log, scegliere una politica di sicurezza che contenga gli algoritmi crittografici abilitati all'uso dal tuo server e aggiungere metadati al server sotto forma di tag che sono coppie chiave-valore.

> **Important**
>
> Sono a tuo carico i costi per i server istanziati e per il trasferimento dei dati. Per informazioni sui prezzi e da utilizzare per AWS Pricing Calculator ottenere una stima del costo di utilizzo di Transfer Family, consulta AWS Transfer Family i prezzi.

Crea un server compatibile con SFTP

Secure Shell (SSH) File Transfer Protocol (SFTP) è un protocollo di rete utilizzato per il trasferimento sicuro di dati su Internet. Il protocollo supporta tutte le funzionalità di sicurezza e autenticazione di SSH. È ampiamente utilizzato per lo scambio di dati, comprese informazioni sensibili tra partner commerciali in una varietà di settori come i servizi finanziari, la sanità, la vendita al dettaglio e la pubblicità.

> **Note**
>
> I server SFTP per Transfer Family funzionano sulla porta 22. Per gli endpoint ospitati su VPC, i server SFTP Transfer Family possono funzionare anche sulla porta 2222 o sulla porta 22000. Per informazioni dettagliate, vedi Crea un server in un cloud privato virtuale.

Consulta anche

- Forniamo un AWS CDK esempio per la creazione di un server SFTP Transfer Family. L'esempio utilizza TypeScript ed è disponibile GitHub qui.
- Per una procedura dettagliata su come implementare un server Transfer Family all'interno di un VPC, consulta Usa l'elenco degli IP consentiti per proteggere i tuoi server. AWS Transfer Family

Per creare un server compatibile con SFTP

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/ e seleziona Server dal pannello di navigazione, quindi scegli Crea server.
2. In Scegli i protocolli, seleziona SFTP, quindi scegli Avanti.
3. In Scegli un provider di identità, scegli il provider di identità che desideri utilizzare per gestire l'accesso degli utenti. Sono disponibili le seguenti opzioni:

   - Servizio gestito: memorizzi le identità e le chiavi degli utenti. AWS Transfer Family
   - AWS Directory Service for Microsoft Active Directory— Fornisci una AWS Directory Service directory per accedere all'endpoint. In questo modo, è possibile utilizzare le credenziali archiviate in Active Directory per autenticare gli utenti. Per ulteriori informazioni sull'utilizzo dei provider di AWS Managed Microsoft AD identità, consulta. Utilizzo del provider di identità AWS Directory Service

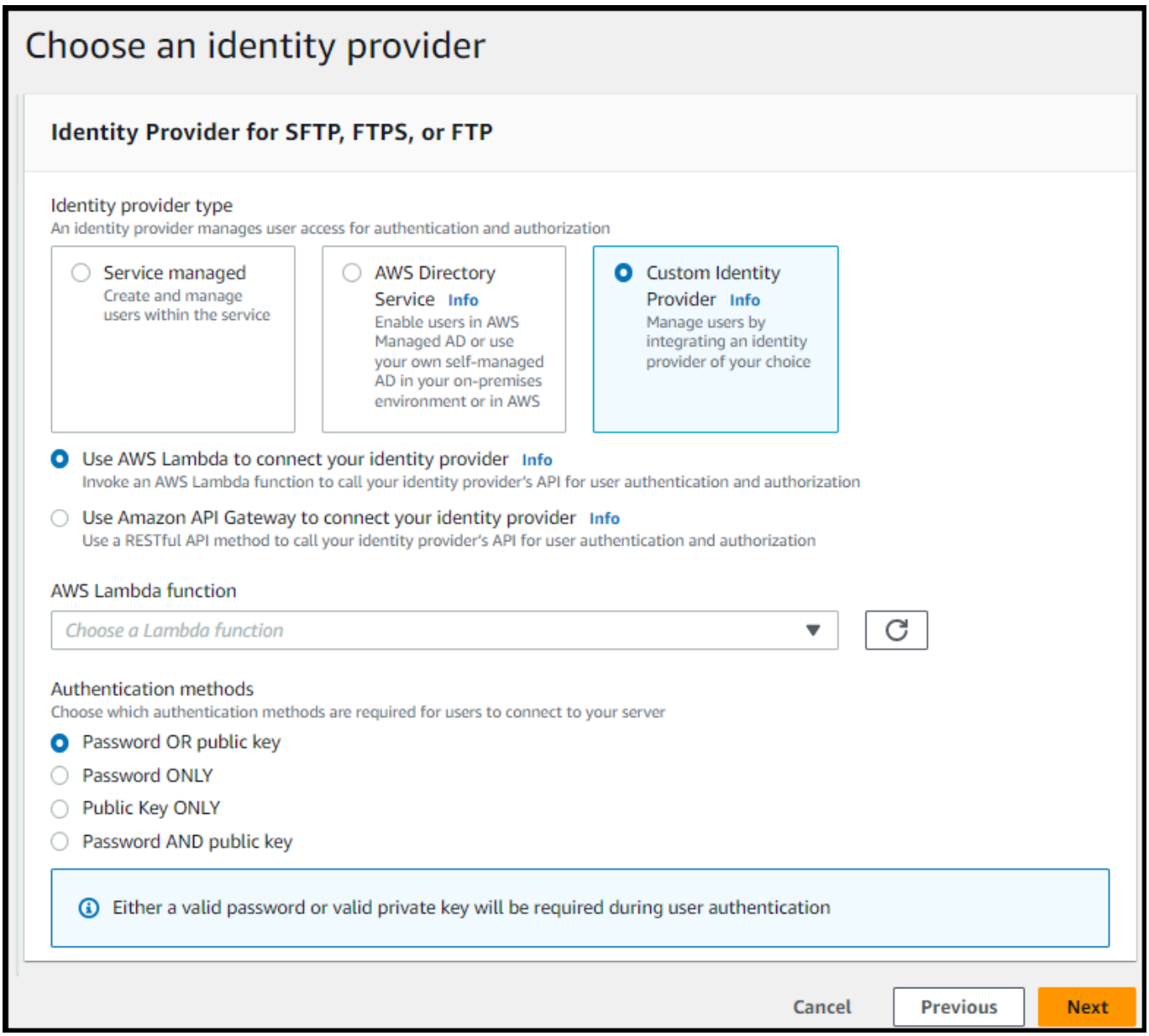
     > **Note**
     >
     > - Le directory Cross-Account e Shared non sono supportate per. AWS Managed Microsoft AD
     > - Per configurare un server con Directory Service come provider di identità, è necessario aggiungere alcune AWS Directory Service autorizzazioni. Per informazioni dettagliate, vedi Prima di iniziare a utilizzare AWS Directory Service for Microsoft Active Directory.

   - Provider di identità personalizzato: scegli una delle seguenti opzioni:
     - AWS Lambda Utilizzalo per connettere il tuo provider di identità: puoi utilizzare un provider di identità esistente, supportato da una funzione Lambda. Fornisci il nome della funzione Lambda. Per ulteriori informazioni, consulta Utilizzo AWS Lambda per integrare il proprio provider di identità.
     - Usa Amazon API Gateway per connettere il tuo provider di identità: puoi creare un metodo API Gateway supportato da una funzione Lambda da utilizzare come provider di identità.

Fornisci un URL di Amazon API Gateway e un ruolo di chiamata. Per ulteriori informazioni, consulta Utilizzo di Amazon API Gateway per integrare il tuo provider di identità.

Per entrambe le opzioni, puoi anche specificare come effettuare l'autenticazione.

- Password O chiave: gli utenti possono autenticarsi con la propria password o la propria chiave. Si tratta del valore di default.
- SOLO password: gli utenti devono fornire la propria password per connettersi.
- SOLO chiave: gli utenti devono fornire la propria chiave privata per connettersi.
- Password E chiave: gli utenti devono fornire sia la chiave privata che la password per connettersi. Il server controlla prima la chiave e poi, se la chiave è valida, il sistema richiede una password. Se la chiave privata fornita non corrisponde alla chiave pubblica archiviata, l'autenticazione fallisce.



4. Seleziona Successivo.
5. In Scegli un endpoint, procedi come segue:

   a. Per Tipo di endpoint, scegli il tipo di endpoint accessibile pubblicamente. Per un endpoint ospitato in un VPC, vedi. Crea un server in un cloud privato virtuale

   b. (Facoltativo) Per Nome host personalizzato, scegli Nessuno.

      Ottieni un nome host del server fornito da. AWS Transfer Family Il nome host del server ha il formato `serverId.server.transfer.regionId.amazonaws.com`.

Per un nome host personalizzato, è necessario specificare un alias personalizzato per l'endpoint del server. Per ulteriori informazioni sull'utilizzo di nomi host personalizzati, consulta. Lavorare con nomi host personalizzati

c. (Facoltativo) Per FIPS Enabled, selezionate la casella di controllo FIPS Enabled Endpoint per assicurarvi che l'endpoint sia conforme ai Federal Information Processing Standards (FIPS).

> **Note**
>
> Gli endpoint compatibili con FIPS sono disponibili solo nelle regioni del Nord America. AWS Per le regioni disponibili, consulta gli AWS Transfer Family endpoint e le quote nel. Riferimenti generali di AWS Per ulteriori informazioni su FIPS, vedere Federal Information Processing Standard (FIPS) 140-2.

d. Seleziona Successivo.

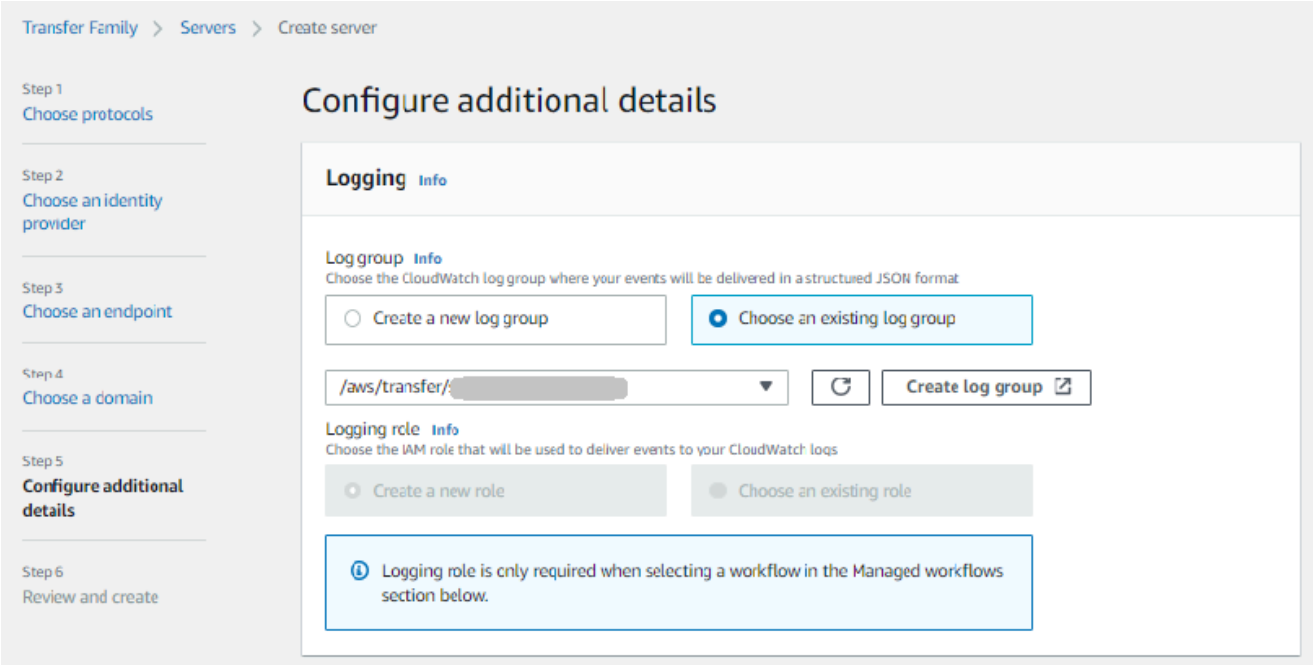
6. Nella pagina Scegli il dominio, scegli il servizio AWS di archiviazione che desideri utilizzare per archiviare e accedere ai tuoi dati tramite il protocollo selezionato:

   - Scegli Amazon S3 per archiviare e accedere ai tuoi file come oggetti tramite il protocollo selezionato.
   - Scegli Amazon EFS per archiviare e accedere ai tuoi file nel tuo file system Amazon EFS tramite il protocollo selezionato.

   Seleziona Successivo.

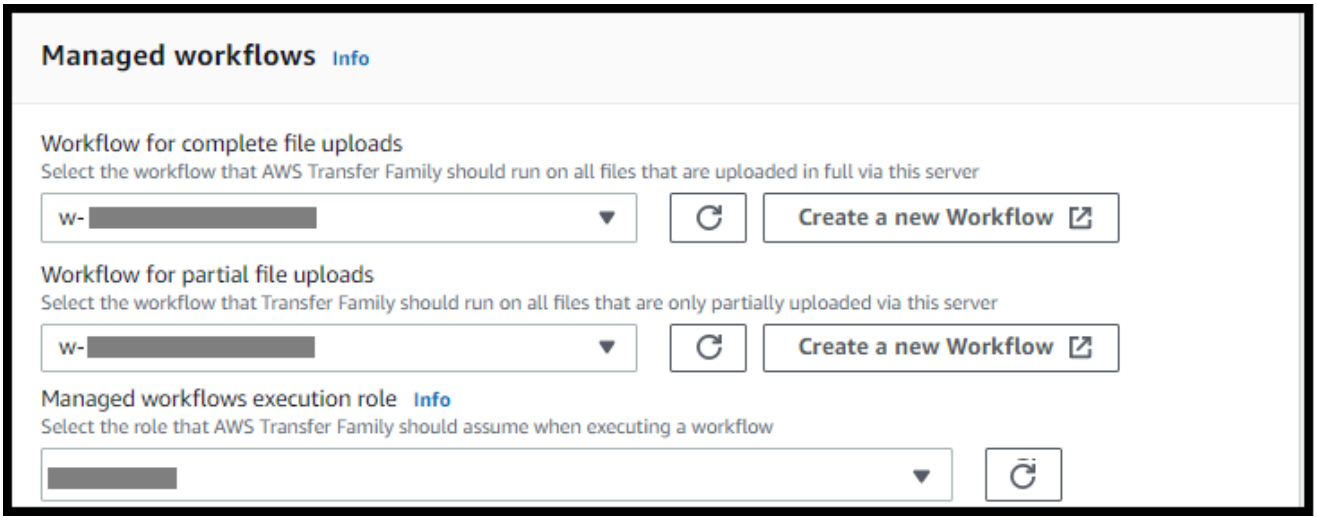
7. In Configura dettagli aggiuntivi, procedi come segue:

   a. Per la registrazione, specifica un gruppo di log esistente o creane uno nuovo (opzione predefinita). Se scegli un gruppo di log esistente, devi selezionarne uno associato al tuo Account AWS.



Se scegli Crea gruppo di log, la CloudWatch console (https://console.aws.amazon.com/cloudwatch/) apre la pagina Crea gruppo di log. Per i dettagli, consulta Creare un gruppo di log in CloudWatch Logs.

b. (Facoltativo) Per i flussi di lavoro gestiti, scegliete gli ID del flusso di lavoro (e un ruolo corrispondente) che Transfer Family deve assumere durante l'esecuzione del flusso di lavoro. È possibile scegliere un flusso di lavoro da eseguire dopo un caricamento completo e un altro da eseguire dopo un caricamento parziale. Per ulteriori informazioni sull'elaborazione dei file utilizzando flussi di lavoro gestiti, consultaAWS Transfer Family flussi di lavoro gestiti.



c. Per le opzioni relative agli algoritmi crittografici, scegli una politica di sicurezza che contenga gli algoritmi crittografici abilitati per l'uso dal tuo server. La nostra politica di sicurezza più recente è quella predefinita: per i dettagli, consulta. Politiche di sicurezza per AWS Transfer Family i server

d. (Facoltativo) Per Server Host Key, inserisci una chiave privata RSA, ED25519 o ECDSA che verrà utilizzata per identificare il server quando i client si connettono ad esso tramite SFTP. Puoi anche aggiungere una descrizione per distinguere tra più chiavi host.

   Dopo aver creato il server, puoi aggiungere chiavi host aggiuntive. Avere più chiavi host è utile se si desidera ruotare le chiavi o se si desidera disporre di diversi tipi di chiavi, ad esempio una chiave RSA e anche una chiave ECDSA.

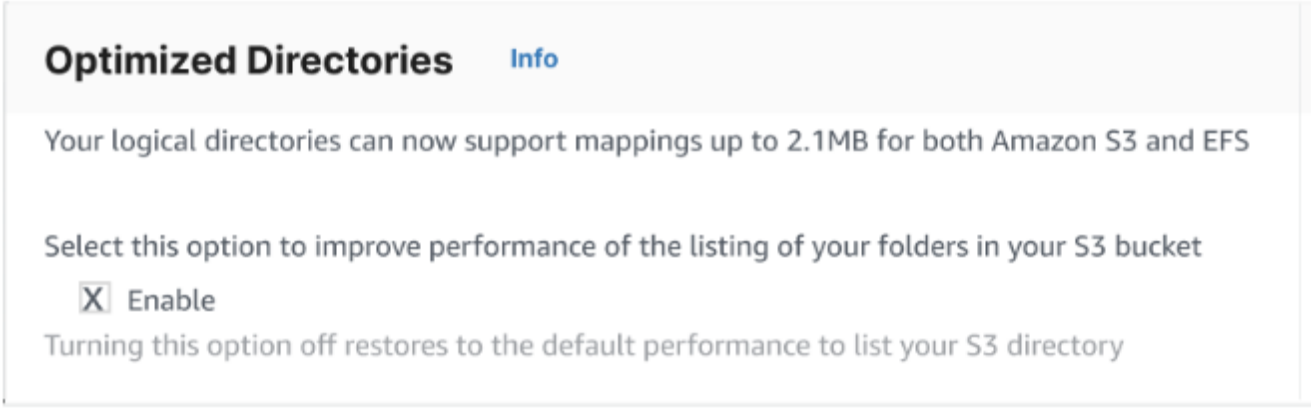
   > **Note**
   >
   > La sezione Server Host Key viene utilizzata solo per la migrazione degli utenti da un server esistente compatibile con SFTP.

e. (Facoltativo) Per Tag, per Chiave e Valore, inserite uno o più tag come coppie chiave-valore, quindi scegliete Aggiungi tag.

f. Seleziona Successivo.

g. Puoi ottimizzare le prestazioni per le tue directory Amazon S3. Ad esempio, supponiamo di accedere alla directory home e di avere 10.000 sottodirectory. In altre parole, il tuo bucket Amazon S3 ha 10.000 cartelle. In questo scenario, se si esegue il comando `ls` (list), l'operazione list richiede dai sei agli otto minuti. Tuttavia, se si ottimizzano le directory, questa operazione richiede solo pochi secondi.

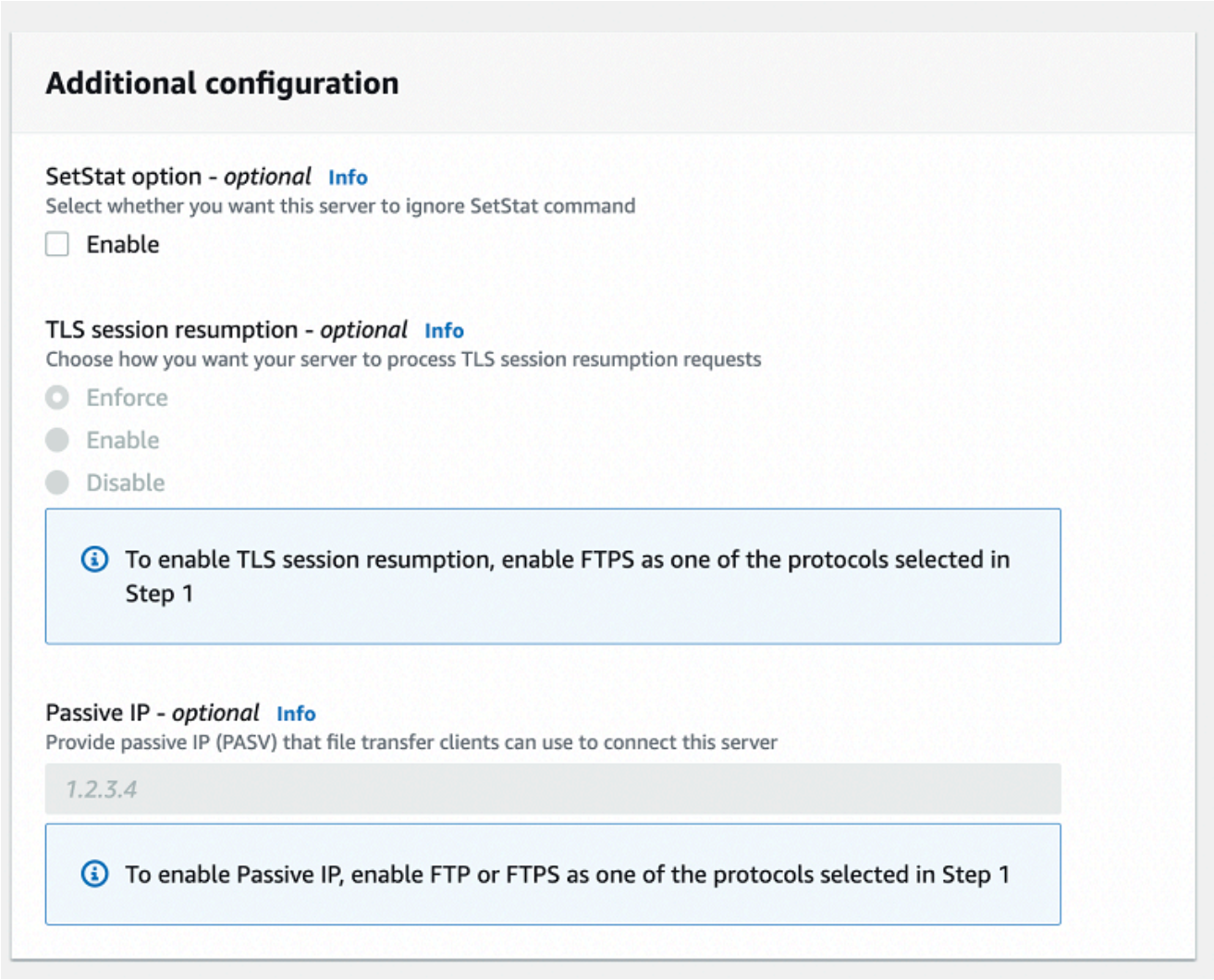
   Quando si crea il server utilizzando la console, le directory ottimizzate sono abilitate per impostazione predefinita. Se crei il server utilizzando l'API, questo comportamento non è abilitato per impostazione predefinita.



h. (Facoltativo) Configura AWS Transfer Family i server per visualizzare messaggi personalizzati come politiche organizzative o termini e condizioni agli utenti finali. Per Visualizza banner, nella casella di testo Pre-autenticazione visualizza banner, inserisci il messaggio di testo che desideri mostrare agli utenti prima che si autentichino.

i. (Facoltativo) È possibile configurare le seguenti opzioni aggiuntive.

- SetStat opzione: abilita questa opzione per ignorare l'errore generato quando un client tenta di utilizzarlo `SETSTAT` su un file che stai caricando su un bucket Amazon S3. Per ulteriori dettagli, consulta la `SetStatOption` documentazione contenuta in. ProtocolDetails
- Ripresa della sessione TLS: questa opzione è disponibile solo se hai abilitato FTPS come uno dei protocolli per questo server.
- IP passivo: questa opzione è disponibile solo se hai abilitato FTPS o FTP come uno dei protocolli per questo server.



8. In Rivedi e crea, esamina le tue scelte.

   - Se desideri modificarne una, scegli Modifica accanto al passaggio.

     > **Note**
     >
     > Devi rivedere ogni passaggio dopo quello che hai scelto di modificare.

   - Se non hai apportato modifiche, scegli Crea server per creare il tuo server. Viene visualizzata la pagina Servers (Server), mostrata di seguito, in cui è elencato il nuovo server.

Possono essere necessari un paio di minuti prima che lo stato del nuovo server passi a Online. A quel punto, il server sarà in grado di eseguire operazioni sui file, ma dovrai prima creare un utente.

Per informazioni dettagliate sulla creazione di utenti, consultaGestione degli utenti per gli endpoint del server.

Creare un server compatibile con FTPS

File Transfer Protocol over SSL (FTPS) è un'estensione di FTP. Utilizza i protocolli crittografici Transport Layer Security (TLS) e Secure Sockets Layer (SSL) per crittografare il traffico. FTPS consente la crittografia delle connessioni dei canali di controllo e dati in modo simultaneo o indipendente.

Per creare un server compatibile con FTPS

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/ e seleziona Server dal pannello di navigazione, quindi scegli Crea server.
2. In Scegli i protocolli, seleziona FTPS.

   Per Certificato server, scegli un certificato archiviato in AWS Certificate Manager (ACM) che verrà utilizzato per identificare il server quando i client si connettono ad esso tramite FTPS, quindi scegli Avanti.

   Per richiedere un nuovo certificato pubblico, consulta Richiedere un certificato pubblico nella Guida per l'AWS Certificate Manager utente.

   Per importare un certificato esistente in ACM, consulta Importazione di certificati in ACM nella Guida per l'AWS Certificate Manager utente.

   Per richiedere un certificato privato per utilizzare FTPS tramite indirizzi IP privati, consulta Richiesta di un certificato privato nella Guida per l'utente.AWS Certificate Manager

   Sono supportati i certificati con gli algoritmi di crittografia e le dimensioni delle chiavi seguenti:

   - RSA a 2048 bit (RSA_2048)
   - RSA a 4096 bit (RSA_4096)
   - Elliptic Prime Curve a 256 bit (EC_prime256v1)
   - Elliptic Prime Curve a 384 bit (EC_secp384r1)
   - Elliptic Prime Curve a 521 bit (EC_secp521r1)

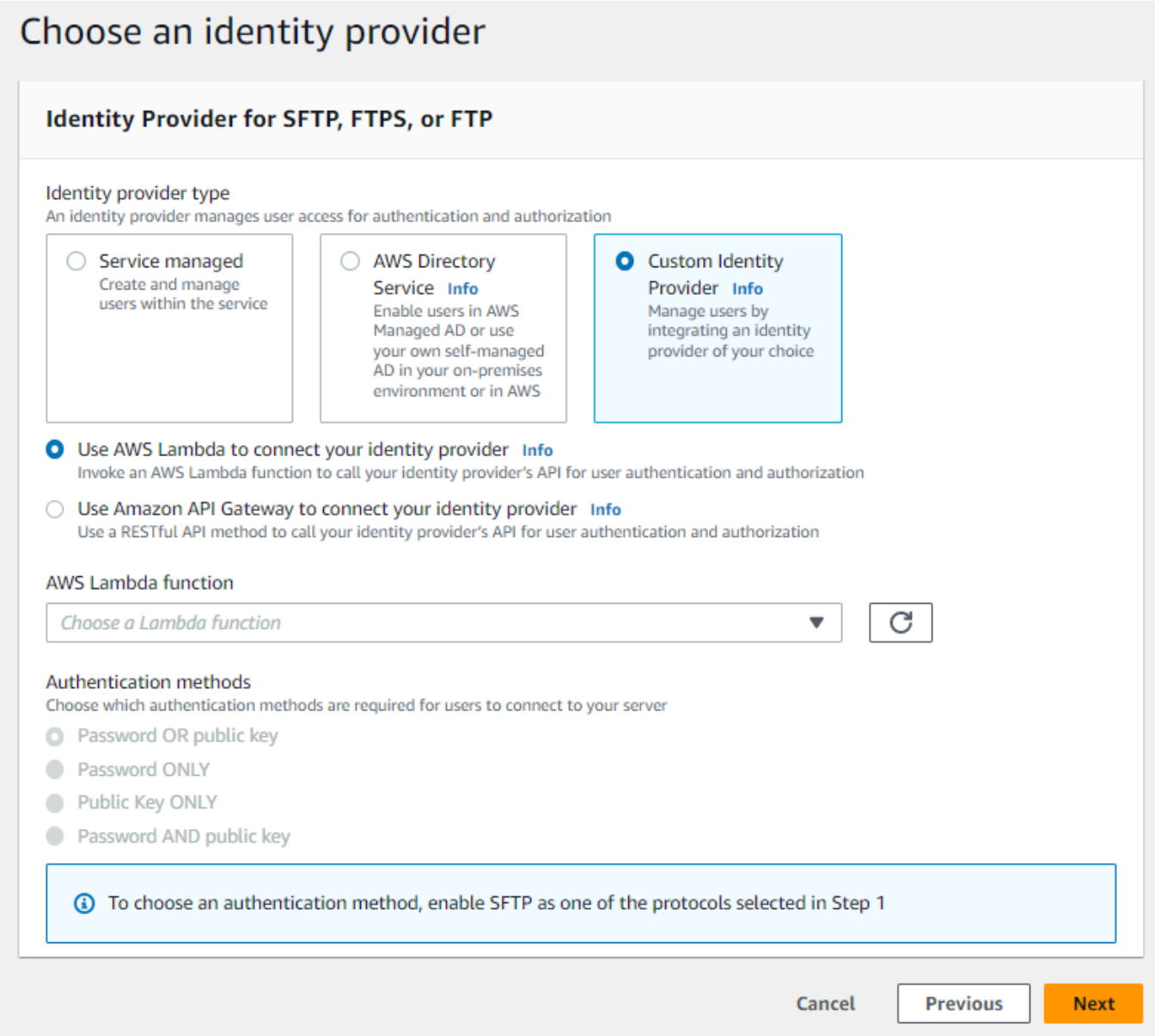
> **Note**
>
> Il certificato deve essere un certificato SSL/TLS X.509 versione 3 valido con FQDN o indirizzo IP specificato e contenere informazioni sull'emittente.

3. In Scegli un provider di identità, scegli il provider di identità che desideri utilizzare per gestire l'accesso degli utenti. Sono disponibili le seguenti opzioni:

   - AWS Directory Service for Microsoft Active Directory— Fornisci una AWS Directory Service directory per accedere all'endpoint. In questo modo, è possibile utilizzare le credenziali archiviate in Active Directory per autenticare gli utenti. Per ulteriori informazioni sull'utilizzo dei provider di AWS Managed Microsoft AD identità, consulta. Utilizzo del provider di identità AWS Directory Service

     > **Note**
     >
     > - Le directory Cross-Account e Shared non sono supportate per. AWS Managed Microsoft AD
     > - Per configurare un server con Directory Service come provider di identità, è necessario aggiungere alcune AWS Directory Service autorizzazioni. Per informazioni dettagliate, vedi Prima di iniziare a utilizzare AWS Directory Service for Microsoft Active Directory.

   - Provider di identità personalizzato: scegli una delle seguenti opzioni:
     - AWS Lambda Utilizzalo per connettere il tuo provider di identità: puoi utilizzare un provider di identità esistente, supportato da una funzione Lambda. Fornisci il nome della funzione Lambda. Per ulteriori informazioni, consulta Utilizzo AWS Lambda per integrare il proprio provider di identità.
     - Usa Amazon API Gateway per connettere il tuo provider di identità: puoi creare un metodo API Gateway supportato da una funzione Lambda da utilizzare come provider di identità. Fornisci un URL di Amazon API Gateway e un ruolo di chiamata. Per ulteriori informazioni, consulta Utilizzo di Amazon API Gateway per integrare il tuo provider di identità.



4. Seleziona Successivo.
5. In Scegli un endpoint, procedi come segue:

> **Note**
>
> I server FTPS per Transfer Family funzionano su Port 21 (Control Channel) e Port Range 8192—8200 (Data Channel).

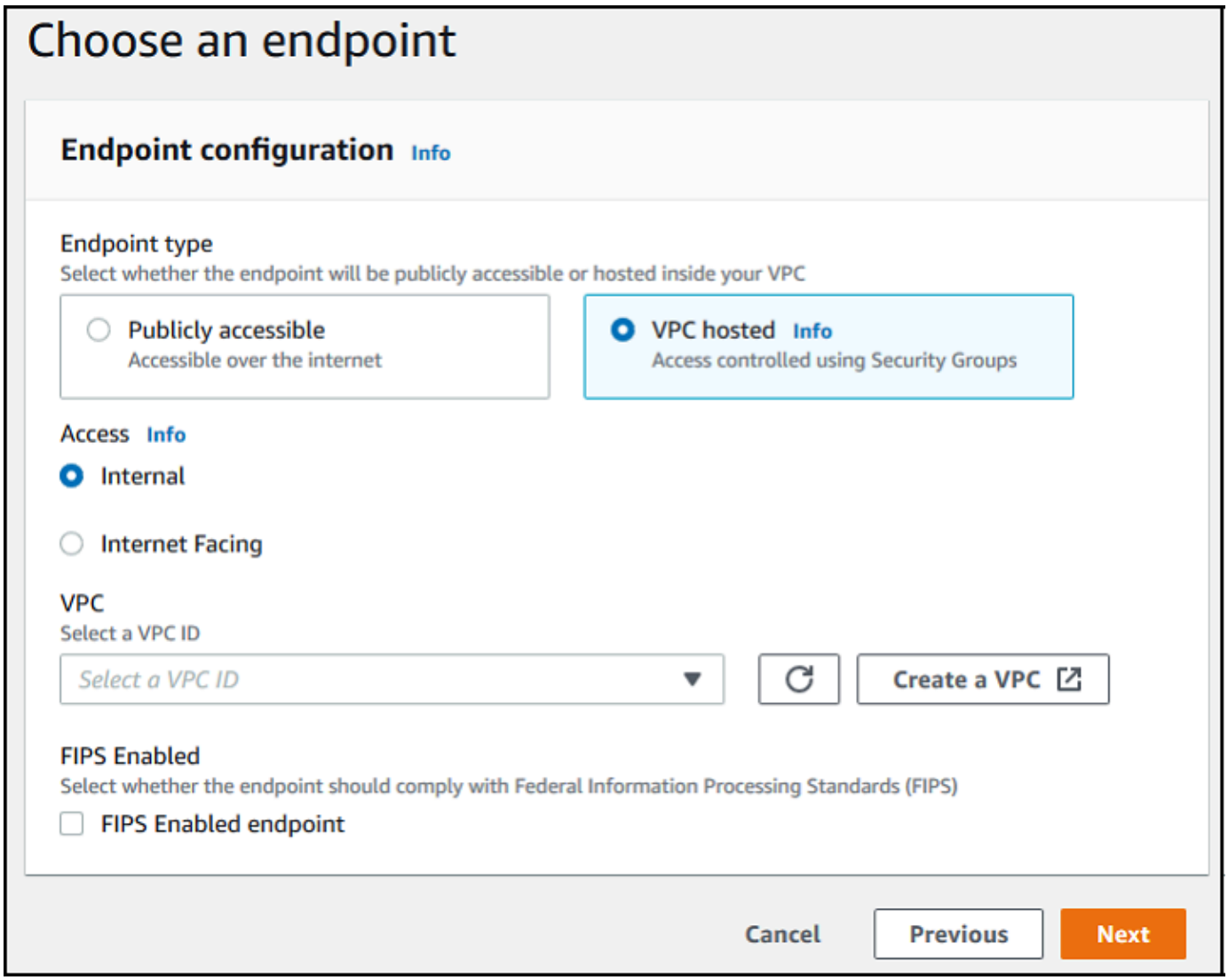
a. Per Tipo di endpoint, scegli il tipo di endpoint ospitato da VPC per ospitare l'endpoint del tuo server. Per informazioni sulla configurazione dell'endpoint ospitato da VPC, consulta. Crea un server in un cloud privato virtuale

> **Note**
>
> Gli endpoint accessibili pubblicamente non sono supportati.

b. (Facoltativo) Per FIPS Enabled, selezionate la casella di controllo FIPS Enabled Endpoint per assicurarvi che l'endpoint sia conforme ai Federal Information Processing Standards (FIPS).

> **Note**
>
> Gli endpoint compatibili con FIPS sono disponibili solo nelle regioni del Nord America. AWS Per le regioni disponibili, consulta gli AWS Transfer Family endpoint e le quote nel. Riferimenti generali di AWS Per ulteriori informazioni su FIPS, vedere Federal Information Processing Standard (FIPS) 140-2.

c. Seleziona Successivo.



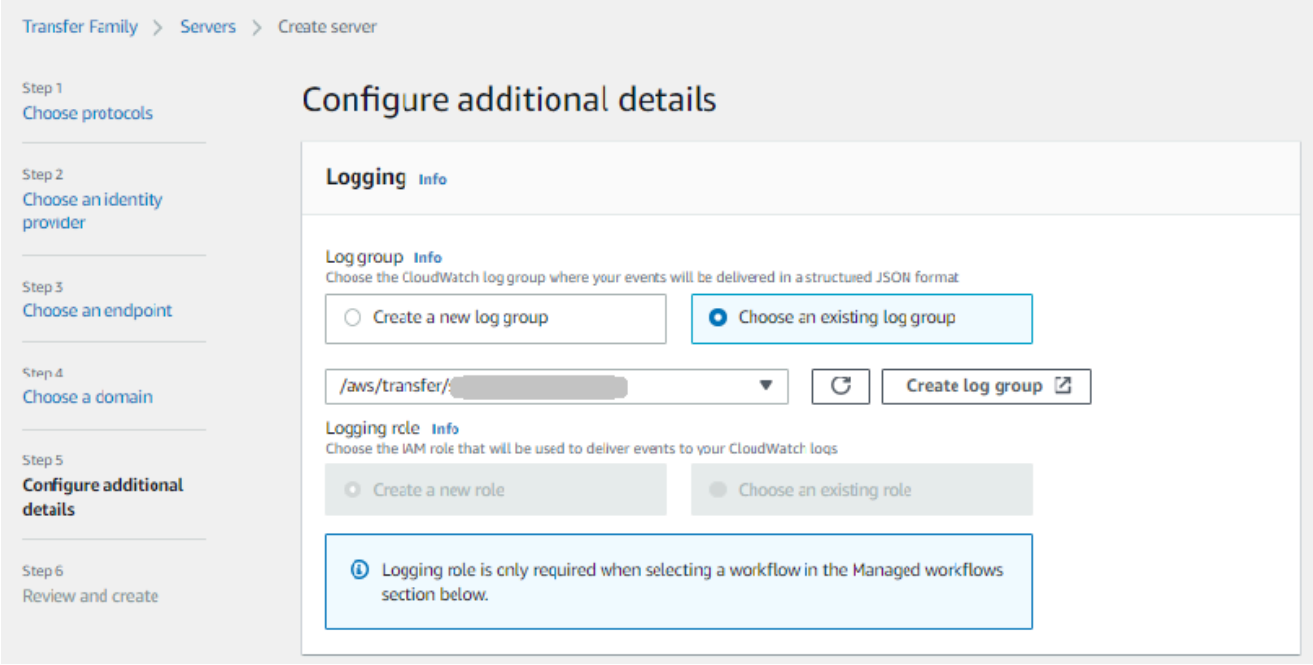
6. Nella pagina Scegli il dominio, scegli il servizio AWS di archiviazione che desideri utilizzare per archiviare e accedere ai tuoi dati tramite il protocollo selezionato:

   - Scegli Amazon S3 per archiviare e accedere ai tuoi file come oggetti tramite il protocollo selezionato.
   - Scegli Amazon EFS per archiviare e accedere ai tuoi file nel tuo file system Amazon EFS tramite il protocollo selezionato.

   Seleziona Successivo.

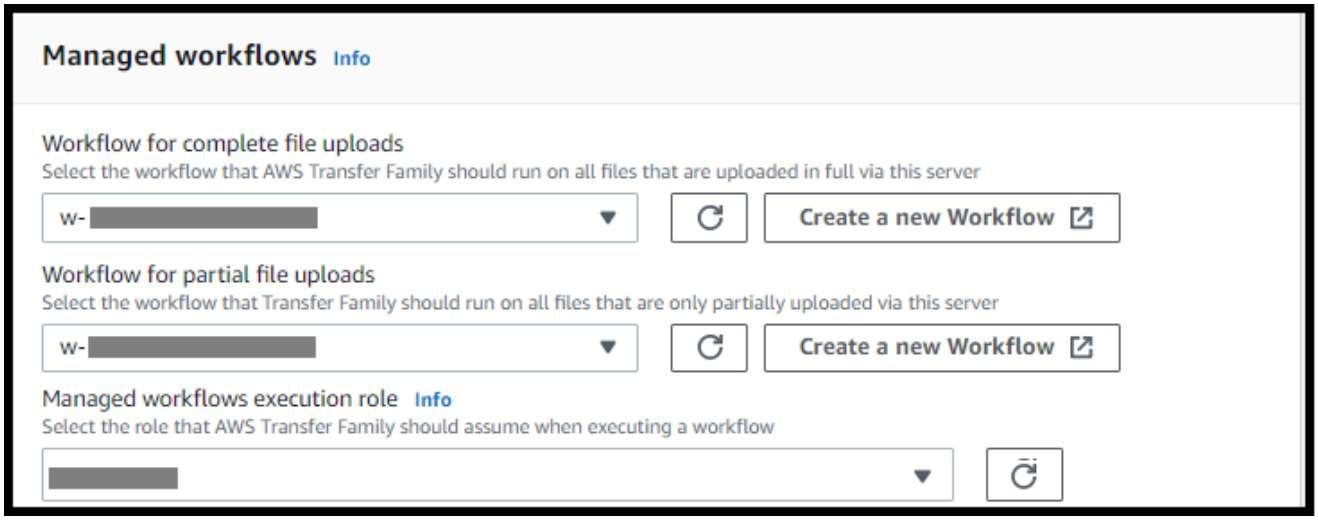
7. In Configura dettagli aggiuntivi, procedi come segue:

a. Per la registrazione, specifica un gruppo di log esistente o creane uno nuovo (opzione predefinita).



Se scegli Crea gruppo di log, la CloudWatch console (https://console.aws.amazon.com/cloudwatch/) apre la pagina Crea gruppo di log. Per i dettagli, consulta Creare un gruppo di log in CloudWatch Logs.

b. (Facoltativo) Per i flussi di lavoro gestiti, scegliete gli ID del flusso di lavoro (e un ruolo corrispondente) che Transfer Family deve assumere durante l'esecuzione del flusso di lavoro. È possibile scegliere un flusso di lavoro da eseguire dopo un caricamento completo e un altro da eseguire dopo un caricamento parziale. Per ulteriori informazioni sull'elaborazione dei file utilizzando flussi di lavoro gestiti, consultaAWS Transfer Family flussi di lavoro gestiti.



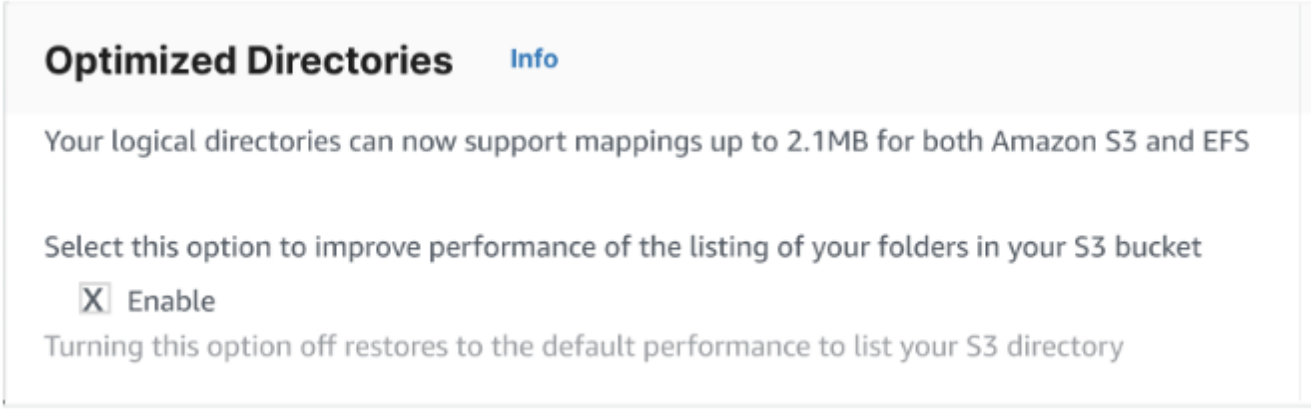
c. Per le opzioni relative agli algoritmi crittografici, scegli una politica di sicurezza che contenga gli algoritmi crittografici abilitati per l'uso dal tuo server. La nostra politica di sicurezza più recente è quella predefinita: per i dettagli, consulta. Politiche di sicurezza per AWS Transfer Family i server

d. Per Server Host Key, lascia vuoto il campo.

e. (Facoltativo) Per Tag, per Chiave e Valore, inserisci uno o più tag come coppie chiave-valore, quindi scegli Aggiungi tag.

f. Puoi ottimizzare le prestazioni per le tue directory Amazon S3. Ad esempio, supponiamo di accedere alla directory home e di avere 10.000 sottodirectory. In altre parole, il tuo bucket Amazon S3 ha 10.000 cartelle. In questo scenario, se si esegue il comando `ls` (list), l'operazione list richiede dai sei agli otto minuti. Tuttavia, se si ottimizzano le directory, questa operazione richiede solo pochi secondi.

   Quando si crea il server utilizzando la console, le directory ottimizzate sono abilitate per impostazione predefinita. Se crei il server utilizzando l'API, questo comportamento non è abilitato per impostazione predefinita.



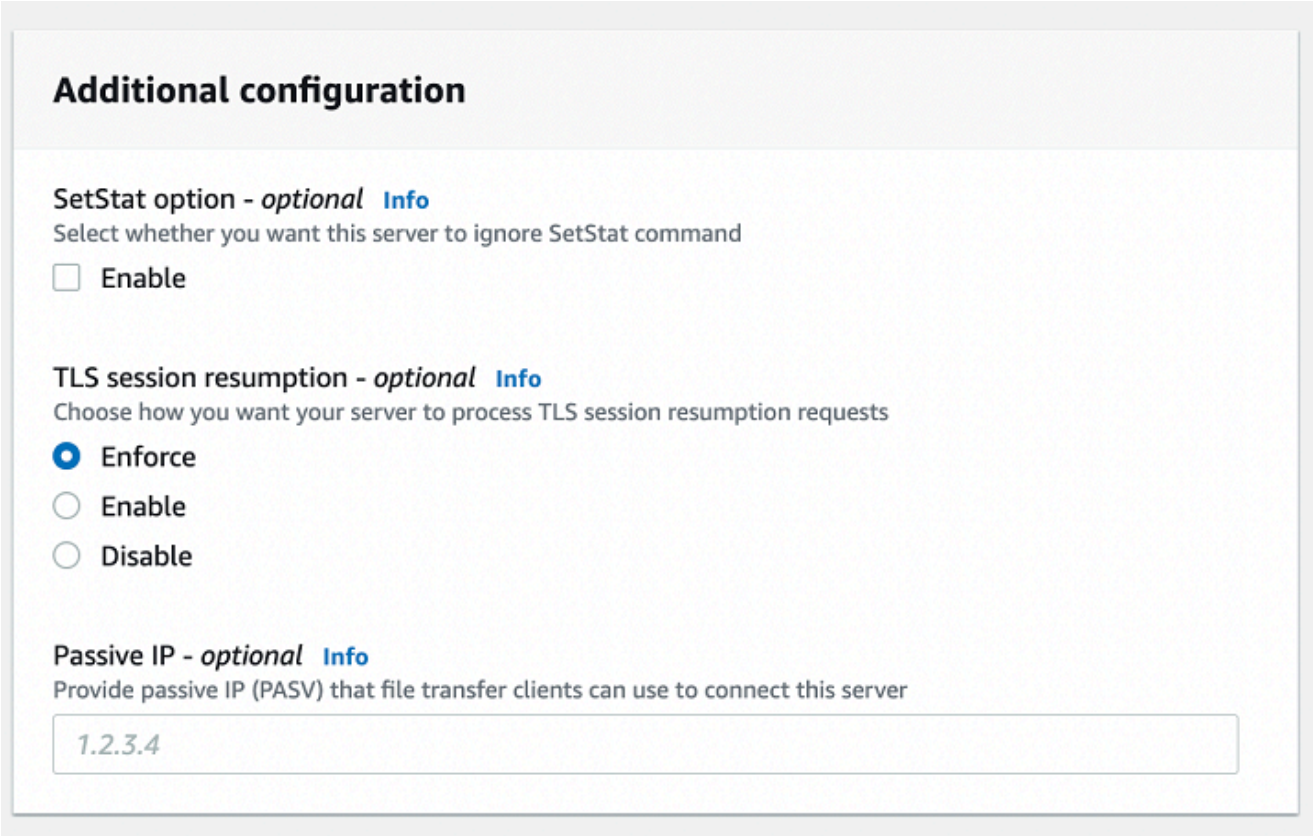
g. Seleziona Successivo.

h. (Facoltativo) È possibile configurare AWS Transfer Family i server per visualizzare messaggi personalizzati, ad esempio politiche organizzative o termini e condizioni, agli utenti finali. È inoltre possibile visualizzare il messaggio del giorno (MOTD) personalizzato agli utenti che si sono autenticati correttamente.

   Per Visualizza banner, nella casella di testo Banner di visualizzazione pre-autenticazione, inserisci il messaggio di testo che desideri mostrare agli utenti prima che si autentichino e nella casella di testo Banner di visualizzazione post-autenticazione, inserisci il testo che desideri mostrare agli utenti dopo che si sono autenticati con successo.

i. (Facoltativo) È possibile configurare le seguenti opzioni aggiuntive.

   - SetStat opzione: abilita questa opzione per ignorare l'errore generato quando un client tenta di utilizzarlo `SETSTAT` su un file che stai caricando su un bucket Amazon S3. Per ulteriori dettagli, consulta la `SetStatOption` documentazione nell'argomento. ProtocolDetails
   - Ripresa della sessione TLS: fornisce un meccanismo per riprendere o condividere una chiave segreta negoziata tra il controllo e la connessione dati per una sessione FTPS. Per ulteriori dettagli, consultate la documentazione nell'argomento. `TlsSessionResumptionMode` ProtocolDetails
   - IP passivo: indica la modalità passiva, per i protocolli FTP e FTPS. Inserisci un singolo indirizzo IPv4, ad esempio l'indirizzo IP pubblico di un firewall, router o load balancer. Per ulteriori dettagli, consultate la `PassiveIp` documentazione nell'ProtocolDetailsargomento.



8. In Rivedi e crea, esamina le tue scelte.

   - Se desideri modificarne una, scegli Modifica accanto al passaggio.

     > **Note**
     >
     > Devi rivedere ogni passaggio dopo quello che hai scelto di modificare.

   - Se non hai apportato modifiche, scegli Crea server per creare il tuo server. Viene visualizzata la pagina Servers (Server), mostrata di seguito, in cui è elencato il nuovo server.

Possono essere necessari un paio di minuti prima che lo stato del nuovo server passi a Online. A questo punto, il server può eseguire operazioni sui file per gli utenti.

Passaggi successivi: per il passaggio successivo, continua con Lavorare con provider di identità personalizzati la configurazione degli utenti.

Crea un server abilitato all'FTP

File Transfer Protocol (FTP) è un protocollo di rete utilizzato per il trasferimento di dati. FTP utilizza un canale separato per il controllo e il trasferimento dei dati. Il canale di controllo è aperto fino al termine o al timeout di inattività. Il canale dati è attivo per tutta la durata del trasferimento. FTP utilizza testo non crittografato e non supporta la crittografia del traffico.

> **Note**
>
> Quando abiliti FTP, devi scegliere l'opzione di accesso interno per l'endpoint ospitato da VPC. Se è necessario che il server trasmetta i dati alla rete pubblica, è necessario utilizzare protocolli sicuri, come SFTP o FTPS.

Per creare un server compatibile con FTP

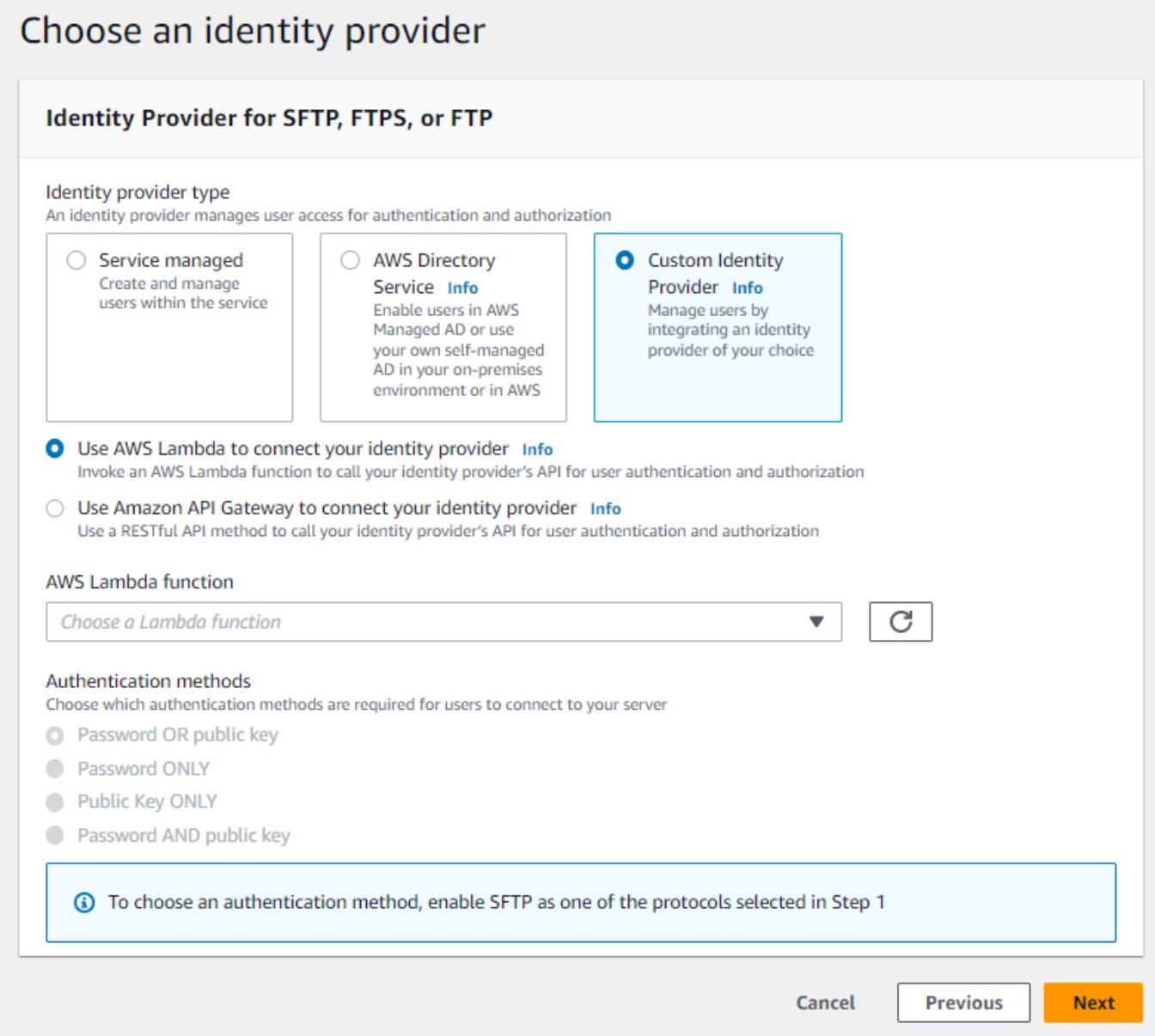
1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/ e seleziona Server dal pannello di navigazione, quindi scegli Crea server.
2. In Scegli i protocolli, seleziona FTP, quindi scegli Avanti.
3. In Scegli un provider di identità, scegli il provider di identità che desideri utilizzare per gestire l'accesso degli utenti. Sono disponibili le seguenti opzioni:

   - AWS Directory Service for Microsoft Active Directory— Fornisci una AWS Directory Service directory per accedere all'endpoint. In questo modo, è possibile utilizzare le credenziali archiviate in Active Directory per autenticare gli utenti. Per ulteriori informazioni sull'utilizzo dei provider di AWS Managed Microsoft AD identità, consulta. Utilizzo del provider di identità AWS Directory Service

     > **Note**
     >
     > - Le directory Cross-Account e Shared non sono supportate per. AWS Managed Microsoft AD
     > - Per configurare un server con Directory Service come provider di identità, è necessario aggiungere alcune AWS Directory Service autorizzazioni. Per informazioni dettagliate, vedi Prima di iniziare a utilizzare AWS Directory Service for Microsoft Active Directory.

   - Provider di identità personalizzato: scegli una delle seguenti opzioni:

- AWS Lambda Utilizzalo per connettere il tuo provider di identità: puoi utilizzare un provider di identità esistente, supportato da una funzione Lambda. Fornisci il nome della funzione Lambda. Per ulteriori informazioni, consulta Utilizzo AWS Lambda per integrare il proprio provider di identità.
- Usa Amazon API Gateway per connettere il tuo provider di identità: puoi creare un metodo API Gateway supportato da una funzione Lambda da utilizzare come provider di identità. Fornisci un URL di Amazon API Gateway e un ruolo di chiamata. Per ulteriori informazioni, consulta Utilizzo di Amazon API Gateway per integrare il tuo provider di identità.



4. Seleziona Successivo.
5. In Scegli un endpoint, procedi come segue:

> **Note**
>
> I server FTP per Transfer Family funzionano su Port 21 (Control Channel) e Port Range 8192—8200 (Data Channel).

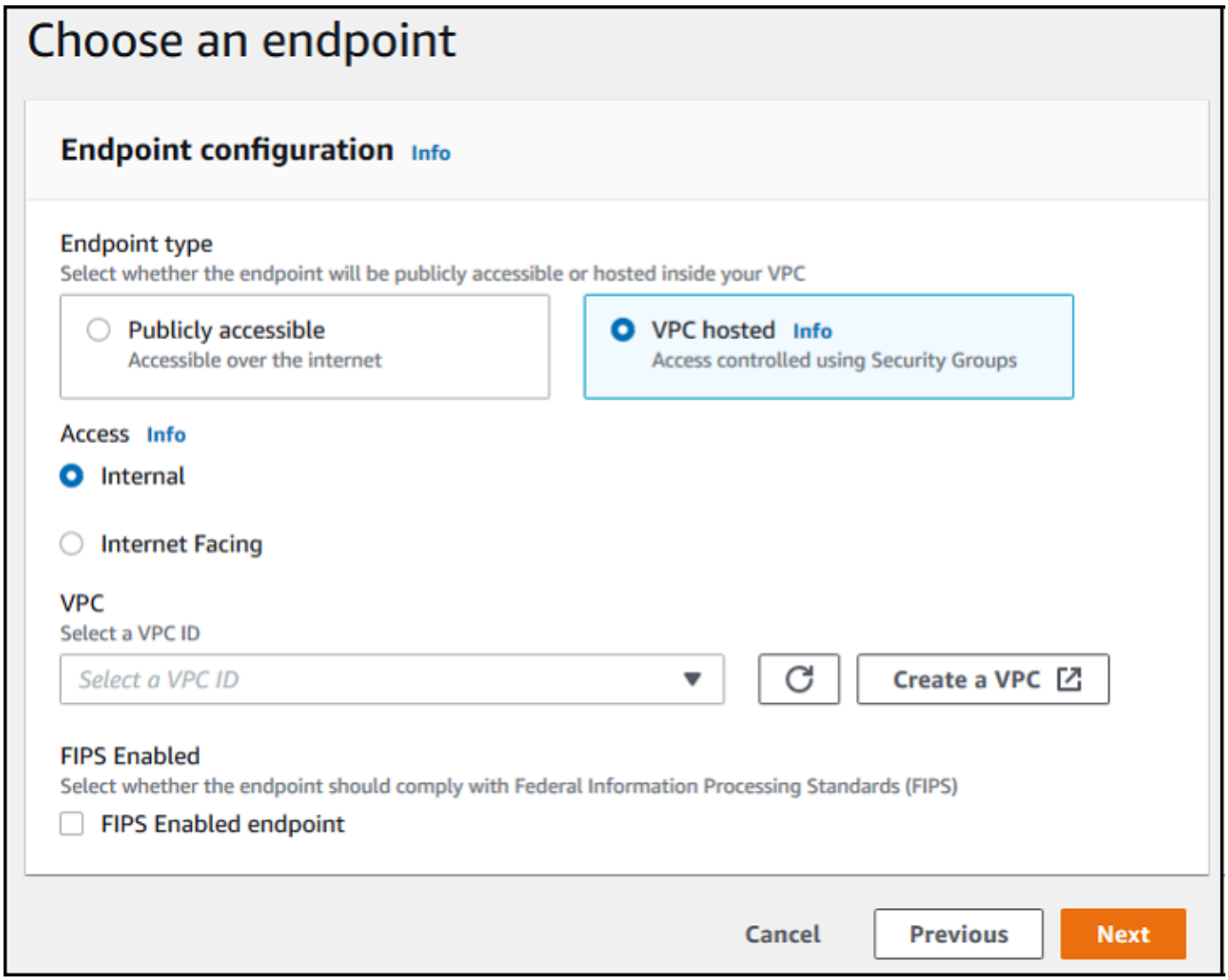
a. Per il tipo di endpoint, scegli VPC ospitato per ospitare l'endpoint del tuo server. Per informazioni sulla configurazione dell'endpoint ospitato da VPC, consulta. Crea un server in un cloud privato virtuale

   > **Note**
   >
   > Gli endpoint accessibili pubblicamente non sono supportati.

b. Per FIPS Enabled, mantieni deselezionata la casella di controllo FIPS Enabled endpoint.

   > **Note**
   >
   > Gli endpoint compatibili con FIPS non sono supportati per i server FTP.

c. Seleziona Successivo.



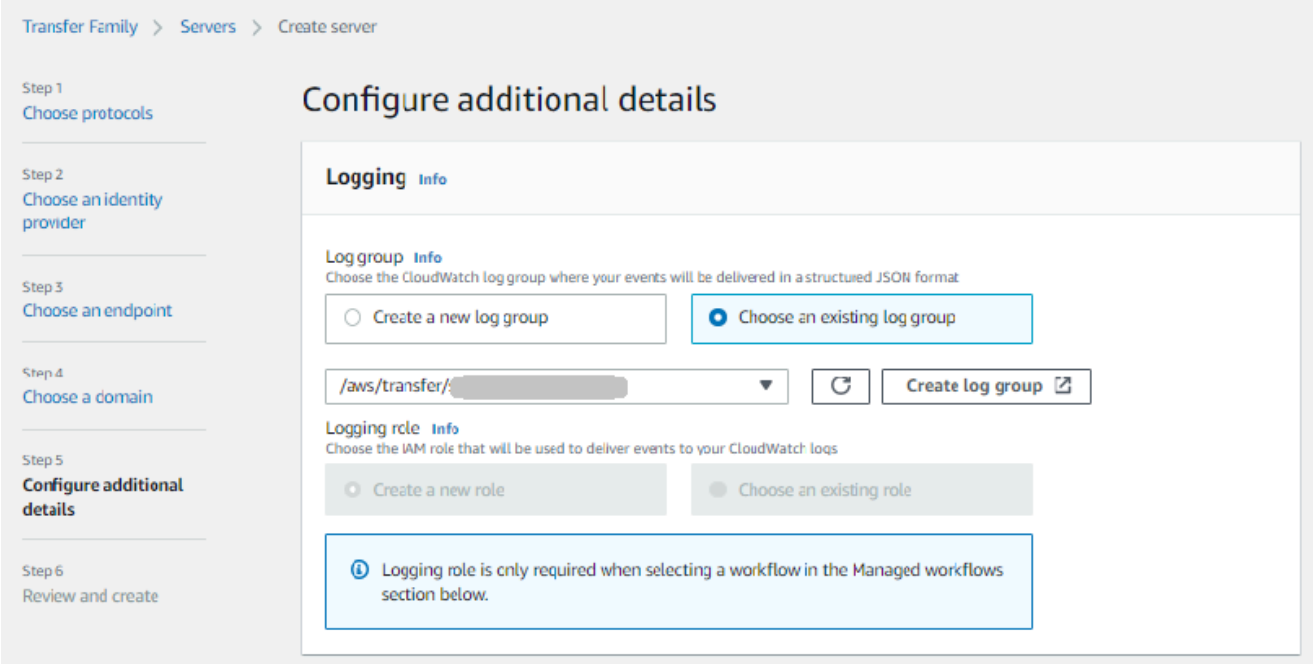
6. Nella pagina Scegli il dominio, scegli il servizio AWS di archiviazione che desideri utilizzare per archiviare e accedere ai tuoi dati tramite il protocollo selezionato.

   - Scegli Amazon S3 per archiviare e accedere ai tuoi file come oggetti tramite il protocollo selezionato.
   - Scegli Amazon EFS per archiviare e accedere ai tuoi file nel tuo file system Amazon EFS tramite il protocollo selezionato.

   Seleziona Successivo.

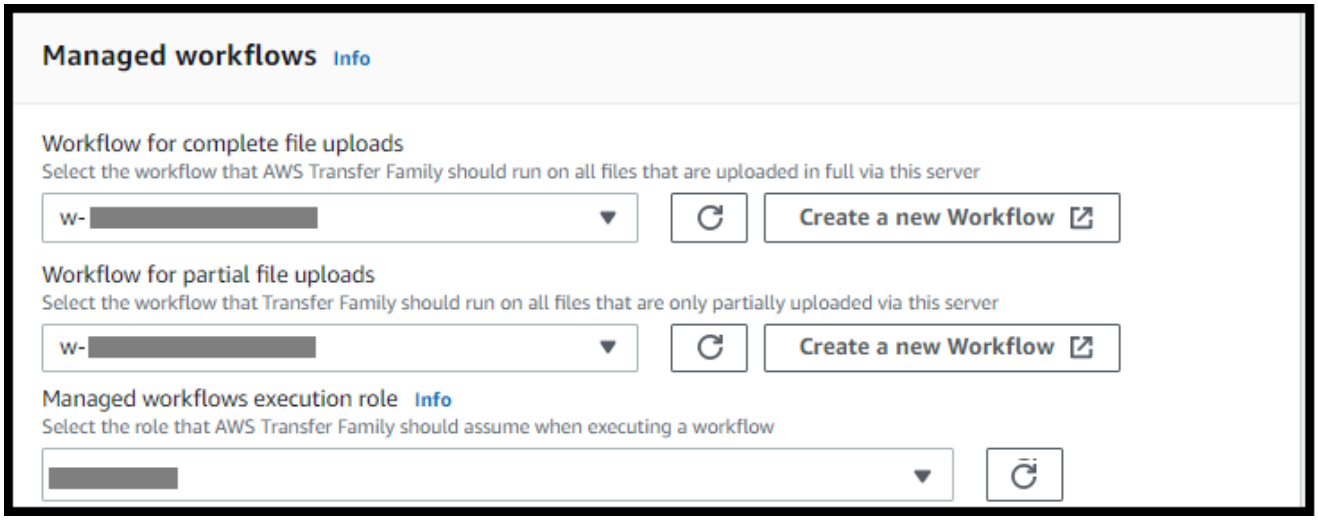
7. In Configura dettagli aggiuntivi, procedi come segue:

a. Per la registrazione, specifica un gruppo di log esistente o creane uno nuovo (opzione predefinita).



Se scegli Crea gruppo di log, la CloudWatch console (https://console.aws.amazon.com/cloudwatch/) apre la pagina Crea gruppo di log. Per i dettagli, consulta Creare un gruppo di log in CloudWatch Logs.

b. (Facoltativo) Per i flussi di lavoro gestiti, scegliete gli ID del flusso di lavoro (e un ruolo corrispondente) che Transfer Family deve assumere durante l'esecuzione del flusso di lavoro. È possibile scegliere un flusso di lavoro da eseguire dopo un caricamento completo e un altro da eseguire dopo un caricamento parziale. Per ulteriori informazioni sull'elaborazione dei file utilizzando flussi di lavoro gestiti, consultaAWS Transfer Family flussi di lavoro gestiti.



c. Per le opzioni relative agli algoritmi crittografici, scegli una politica di sicurezza che contenga gli algoritmi crittografici abilitati per l'uso dal tuo server.

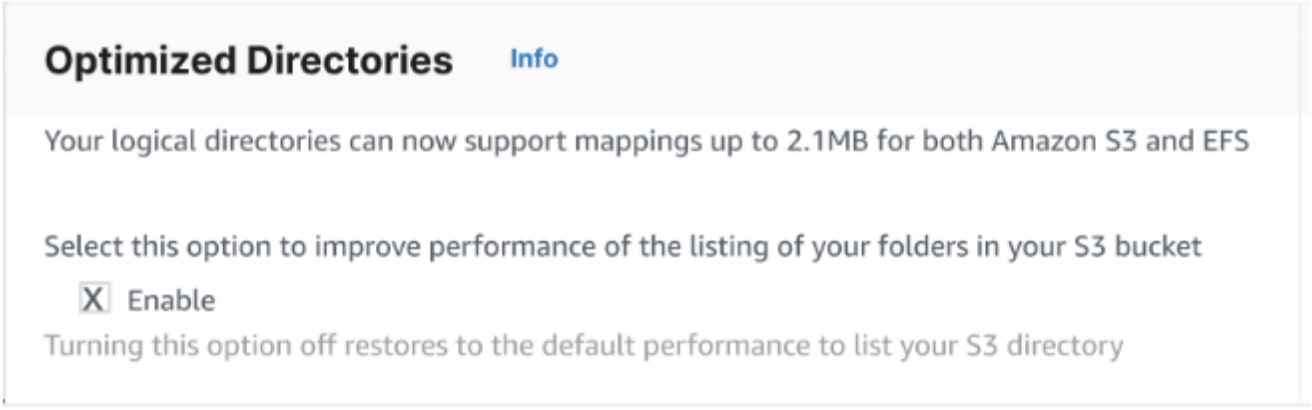
> **Note**
>
> Transfer Family assegna la politica di sicurezza più recente al tuo server FTP. Tuttavia, poiché il protocollo FTP non utilizza alcuna crittografia, i server FTP non utilizzano nessuno degli algoritmi delle politiche di sicurezza. A meno che il server non utilizzi anche il protocollo FTPS o SFTP, la politica di sicurezza rimane inutilizzata.

d. Per Server Host Key, lascialo vuoto.

e. (Facoltativo) Per Tag, per Chiave e Valore, inserisci uno o più tag come coppie chiave-valore, quindi scegli Aggiungi tag.

f. Puoi ottimizzare le prestazioni per le tue directory Amazon S3. Ad esempio, supponiamo di accedere alla directory home e di avere 10.000 sottodirectory. In altre parole, il tuo bucket Amazon S3 ha 10.000 cartelle. In questo scenario, se si esegue il comando `ls` (list), l'operazione list richiede dai sei agli otto minuti. Tuttavia, se si ottimizzano le directory, questa operazione richiede solo pochi secondi.

   Quando si crea il server utilizzando la console, le directory ottimizzate sono abilitate per impostazione predefinita. Se crei il server utilizzando l'API, questo comportamento non è abilitato per impostazione predefinita.



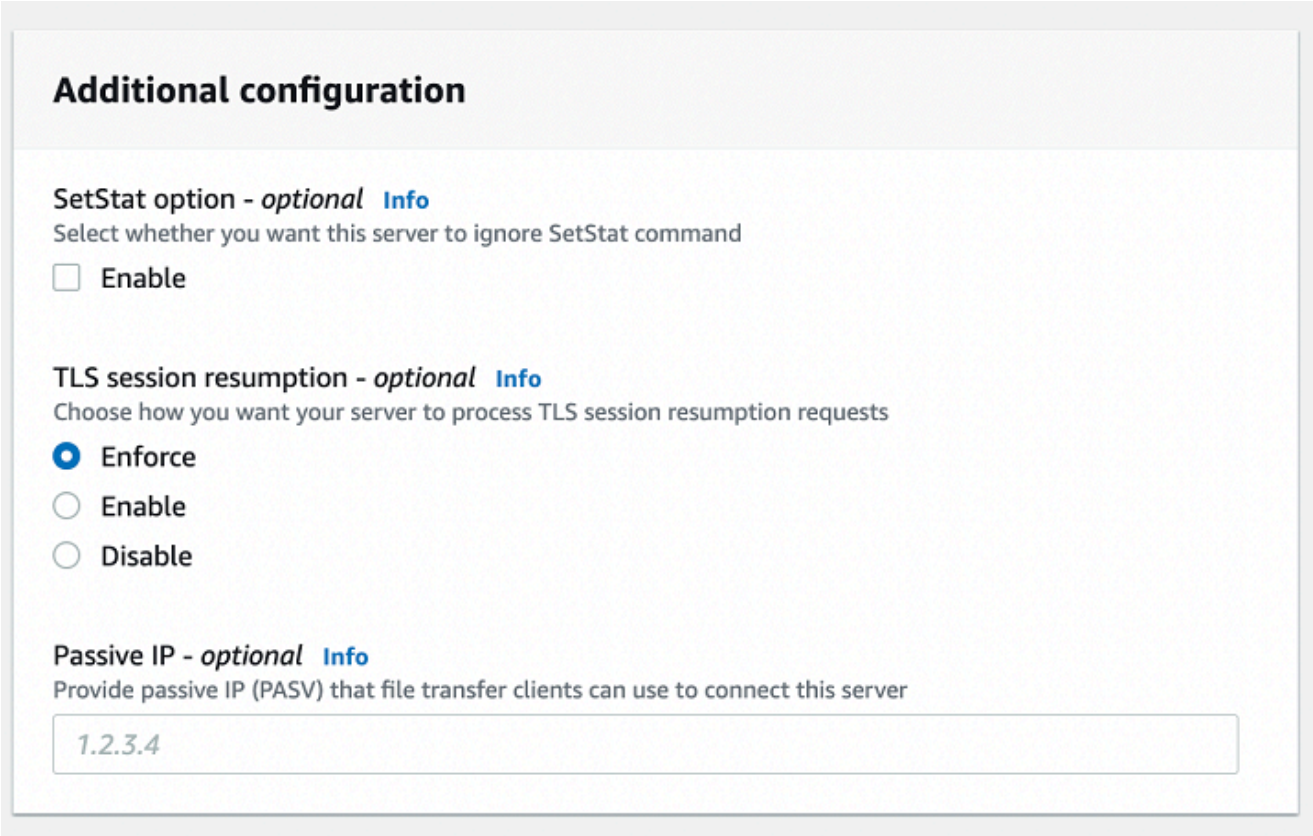
g. Seleziona Successivo.

h. (Facoltativo) È possibile configurare AWS Transfer Family i server per visualizzare messaggi personalizzati, ad esempio politiche organizzative o termini e condizioni, agli utenti finali. È inoltre possibile visualizzare il messaggio del giorno (MOTD) personalizzato agli utenti che si sono autenticati correttamente.

   Per Visualizza banner, nella casella di testo Banner di visualizzazione pre-autenticazione, inserisci il messaggio di testo che desideri mostrare agli utenti prima che si autentichino e nella casella di testo Banner di visualizzazione post-autenticazione, inserisci il testo che desideri mostrare agli utenti dopo che si sono autenticati con successo.

i. (Facoltativo) È possibile configurare le seguenti opzioni aggiuntive.

   - SetStat opzione: abilita questa opzione per ignorare l'errore generato quando un client tenta di utilizzarlo `SETSTAT` su un file che stai caricando su un bucket Amazon S3. Per ulteriori dettagli, consulta la `SetStatOption` documentazione nell'argomento. ProtocolDetails
   - Ripresa della sessione TLS: fornisce un meccanismo per riprendere o condividere una chiave segreta negoziata tra il controllo e la connessione dati per una sessione FTPS. Per ulteriori dettagli, consultate la documentazione nell'argomento. `TlsSessionResumptionMode` ProtocolDetails
   - IP passivo: indica la modalità passiva, per i protocolli FTP e FTPS. Inserisci un singolo indirizzo IPv4, ad esempio l'indirizzo IP pubblico di un firewall, router o load balancer. Per ulteriori dettagli, consultate la `PassiveIp` documentazione nell'ProtocolDetailsargomento.



8. In Rivedi e crea, esamina le tue scelte.

   - Se desideri modificarne una, scegli Modifica accanto al passaggio.

     > **Note**
     >
     > Devi rivedere ogni passaggio dopo quello che hai scelto di modificare.

   - Se non hai apportato modifiche, scegli Crea server per creare il tuo server. Viene visualizzata la pagina Servers (Server), mostrata di seguito, in cui è elencato il nuovo server.

Possono essere necessari un paio di minuti prima che lo stato del nuovo server passi a Online. A questo punto, il server può eseguire operazioni sui file per gli utenti.

Passaggi successivi: per il passaggio successivo, continua con Lavorare con provider di identità personalizzati la configurazione degli utenti.

Crea un server in un cloud privato virtuale

Puoi ospitare l'endpoint del tuo server all'interno di un cloud privato virtuale (VPC) da utilizzare per il trasferimento di dati da e verso un bucket Amazon S3 o un file system Amazon EFS senza passare dalla rete Internet pubblica.

> **Note**
>
> Dopo il 19 maggio 2021, non potrai creare un server utilizzando il tuo AWS account se quest'`EndpointType=VPC_ENDPOINT`ultimo non l'ha già fatto prima del 19 maggio 2021. Se hai già creato dei server con `EndpointType=VPC_ENDPOINT` il tuo AWS account entro il 21 febbraio 2021, non subirai alcuna modifica. Dopo questa data, usa `EndpointType=VPC`. Per ulteriori informazioni, consulta the section called “Interruzione dell'uso di VPC_ENDPOINT”.

Se utilizzi Amazon Virtual Private Cloud (Amazon VPC) per ospitare AWS le tue risorse, puoi stabilire una connessione privata tra il tuo VPC e un server. È quindi possibile utilizzare questo server per trasferire dati tramite client da e verso il bucket Amazon S3 senza utilizzare indirizzi IP pubblici o richiedere un gateway Internet.

Utilizzando Amazon VPC, puoi avviare AWS risorse in una rete virtuale personalizzata. Puoi utilizzare un VPC per controllare le impostazioni di rete, come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Per ulteriori informazioni sui VPC, consulta What Is Amazon VPC? nella Guida per l'utente di Amazon VPC.

Nelle sezioni successive, trova le istruzioni su come creare e connettere il tuo VPC a un server. In sintesi, procedi come segue:

1. Configura un server utilizzando un endpoint VPC.
2. Connettiti al tuo server utilizzando un client che si trova all'interno del tuo VPC tramite l'endpoint VPC. In questo modo puoi trasferire i dati archiviati nel tuo bucket Amazon S3 tramite il tuo client utilizzando. AWS Transfer Family Puoi eseguire questo trasferimento anche se la rete è disconnessa dalla rete Internet pubblica.
3. Inoltre, se scegli di rendere l'endpoint del tuo server rivolto a Internet, puoi associare indirizzi IP elastici all'endpoint. In questo modo i client esterni al tuo VPC si connettono al tuo server. Puoi utilizzare i gruppi di sicurezza VPC per controllare l'accesso agli utenti autenticati le cui richieste provengono solo da indirizzi consentiti.

Argomenti

Crea un endpoint server a cui è possibile accedere solo all'interno del tuo VPC

Nella procedura seguente, crei un endpoint server accessibile solo alle risorse all'interno del tuo VPC.

Per creare un endpoint server all'interno di un VPC

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Dal pannello di navigazione, seleziona Server, quindi scegli Crea server.
3. In Scegli i protocolli, seleziona uno o più protocolli, quindi scegli Avanti. Per ulteriori informazioni sui protocolli, consultaFase 2: Creare un server compatibile con SFTP.
4. In Scegli un provider di identità, scegli Servizio gestito per archiviare le identità e le chiavi degli utenti AWS Transfer Family, quindi scegli Avanti.

   > **Note**
   >
   > Questa procedura utilizza l'opzione gestita dal servizio. Se scegli Custom, fornisci un endpoint Amazon API Gateway e un ruolo AWS Identity and Access Management (IAM) per accedere all'endpoint. In questo modo, puoi integrare il tuo servizio di directory per autenticare e autorizzare i tuoi utenti. Per ulteriori informazioni sull'utilizzo di provider di identità personalizzati, consulta Lavorare con provider di identità personalizzati.

5. In Scegli un endpoint, procedi come segue:

   > **Note**
   >
   > I server FTP e FTPS per Transfer Family funzionano su Port 21 (Control Channel) e Port Range 8192-8200 (Data Channel).

a. Per Tipo di endpoint, scegli il tipo di endpoint ospitato da VPC per ospitare l'endpoint del tuo server.

b. Per Access, scegli Interno per rendere l'endpoint accessibile solo ai client che utilizzano gli indirizzi IP privati dell'endpoint.

> **Note**
>
> Per i dettagli sull'opzione Connessione Internet, consulta. Crea un endpoint con accesso a Internet per il tuo server Un server creato in un VPC solo per l'accesso interno non supporta nomi host personalizzati.

c. Per VPC, scegli un ID VPC esistente o scegli Crea un VPC per creare un nuovo VPC.

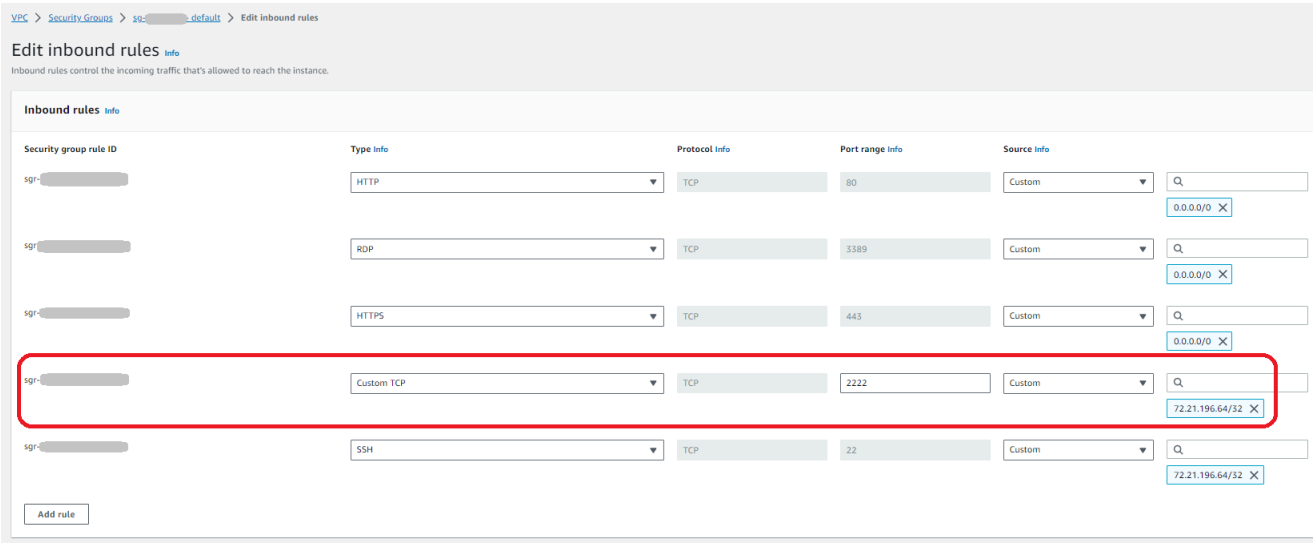
d. Nella sezione Zone di disponibilità, scegli fino a tre zone di disponibilità e sottoreti associate.

e. Nella sezione Gruppi di sicurezza, scegli uno o più ID del gruppo di sicurezza esistente o scegli Crea un gruppo di sicurezza per creare un nuovo gruppo di sicurezza. Per ulteriori informazioni sui gruppi di sicurezza, consulta la sezione Gruppi di sicurezza per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud. Per creare un gruppo di sicurezza, consulta Creazione di un gruppo di sicurezza nella Amazon Virtual Private Cloud User Guide.

> **Note**
>
> Il tuo VPC include automaticamente un gruppo di sicurezza predefinito. Se non specifichi uno o più gruppi di sicurezza diversi all'avvio del server, associamo il gruppo di sicurezza predefinito al tuo server.

Per le regole in entrata per il gruppo di sicurezza, puoi configurare il traffico SSH per utilizzare le porte 22, 2222, 22000 o qualsiasi combinazione. La porta 22 è configurata per impostazione predefinita. Per utilizzare la porta 2222 o la porta 22000, aggiungi una regola in entrata al tuo gruppo di sicurezza. Per il tipo, scegli TCP personalizzato, quindi inserisci uno **`2222`** o **`22000`** per Intervallo di porte e, per l'origine, inserisci lo stesso intervallo CIDR che hai utilizzato per la regola della porta SSH 22.

> **Note**
>
> Puoi anche utilizzare la porta 2223 per i client che richiedono ACK «piggy-back» TCP o la possibilità che il pack finale dell'handshake TCP a 3 vie contenga anche dati.
>
> Alcuni software client potrebbero essere incompatibili con la porta 2223, ad esempio un client che richiede al server di inviare la stringa di identificazione SFTP prima che il client lo faccia.



f. (Facoltativo) Per FIPS Enabled, selezionate la casella di controllo FIPS Enabled Endpoint per assicurarvi che l'endpoint sia conforme ai Federal Information Processing Standards (FIPS).

> **Note**
>
> Gli endpoint compatibili con FIPS sono disponibili solo nelle regioni del Nord America. AWS Per le regioni disponibili, consulta gli AWS Transfer Family endpoint e le quote nel. Riferimenti generali di AWS Per ulteriori informazioni su FIPS, vedere Federal Information Processing Standard (FIPS) 140-2.

g. Seleziona Successivo.

6. In Configura dettagli aggiuntivi, procedi come segue:

a. Per la CloudWatch registrazione, scegli una delle seguenti opzioni per abilitare la CloudWatch registrazione Amazon dell'attività dell'utente:

   - Crea un nuovo ruolo per consentire a Transfer Family di creare automaticamente il ruolo IAM, purché tu disponga delle autorizzazioni giuste per creare un nuovo ruolo. Viene chiamato `AWSTransferLoggingAccess` il ruolo IAM creato.
   - Scegli un ruolo esistente per scegliere un ruolo IAM esistente dal tuo account. In Ruolo di registrazione, scegli il ruolo. Questo ruolo IAM dovrebbe includere una politica di fiducia con Service impostato `transfer.amazonaws.com` su.

     Per ulteriori informazioni sulla CloudWatch registrazione, vedereConfigura il CloudWatch ruolo di registrazione.

   > **Note**
   >
   > - Non è possibile visualizzare l'attività dell'utente finale CloudWatch se non si specifica un ruolo di registrazione.
   > - Se non desideri impostare un ruolo di CloudWatch registrazione, seleziona Scegli un ruolo esistente, ma non selezionare un ruolo di registrazione.

b. Per le opzioni relative agli algoritmi crittografici, scegli una politica di sicurezza che contenga gli algoritmi crittografici abilitati per l'uso da parte del tuo server.

   > **Note**
   >
   > Per impostazione predefinita, la politica `TransferSecurityPolicy-2020-06` di sicurezza è collegata al server a meno che non ne scelga una diversa.

   Per ulteriori informazioni sulle policy di sicurezza, consulta Politiche di sicurezza per AWS Transfer Family i server.

c. (Facoltativo: questa sezione riguarda solo la migrazione degli utenti da un server compatibile con SFTP esistente.) Per Server Host Key, inserite una chiave privata RSA, ED25519 o ECDSA che verrà utilizzata per identificare il server quando i client si connettono ad esso tramite SFTP.

d. (Facoltativo) Per Tag, per Chiave e Valore, inserite uno o più tag come coppie chiave-valore, quindi scegliete Aggiungi tag.

e. Seleziona Successivo.

7. In Rivedi e crea, rivedi le tue scelte. Se:

- Se desideri modificarne una, scegli Modifica accanto al passaggio.

> **Note**
>
> Dovrai rivedere ogni passaggio dopo il passaggio che hai scelto di modificare.

- Non apporti modifiche, scegli Crea server per creare il tuo server. Viene visualizzata la pagina Servers (Server), mostrata di seguito, in cui è elencato il nuovo server.

Possono essere necessari un paio di minuti prima che lo stato del nuovo server passi a Online. A quel punto, il server sarà in grado di eseguire operazioni sui file, ma dovrai prima creare un utente. Per informazioni dettagliate sulla creazione di utenti, consultaGestione degli utenti per gli endpoint del server.

Crea un endpoint con accesso a Internet per il tuo server

Nella procedura seguente, si crea un endpoint server. Questo endpoint è accessibile via Internet solo ai client i cui indirizzi IP di origine sono consentiti nel gruppo di sicurezza predefinito del VPC. Inoltre, utilizzando indirizzi IP elastici per rendere l'endpoint rivolto a Internet, i clienti possono utilizzare l'indirizzo IP elastico per consentire l'accesso all'endpoint tramite i loro firewall.

> **Note**
>
> È possibile utilizzare solo SFTP e FTPS su un endpoint ospitato in VPC con accesso a Internet.

Per creare un endpoint con accesso a Internet

1. Apri la console all'indirizzo https://console.aws.amazon.com/transfer/ AWS Transfer Family .
2. Dal pannello di navigazione, seleziona Server, quindi scegli Crea server.
3. In Scegli i protocolli, seleziona uno o più protocolli, quindi scegli Avanti. Per ulteriori informazioni sui protocolli, consultaFase 2: Creare un server compatibile con SFTP.

4. In Scegli un provider di identità, scegli Servizio gestito per archiviare le identità e le chiavi degli utenti AWS Transfer Family, quindi scegli Avanti.

> **Note**
>
> Questa procedura utilizza l'opzione gestita dal servizio. Se scegli Custom, fornisci un endpoint Amazon API Gateway e un ruolo AWS Identity and Access Management (IAM) per accedere all'endpoint. In questo modo, puoi integrare il tuo servizio di directory per autenticare e autorizzare i tuoi utenti. Per ulteriori informazioni sull'utilizzo di provider di identità personalizzati, consulta Lavorare con provider di identità personalizzati.

5. In Scegli un endpoint, procedi come segue:

   a. Per Tipo di endpoint, scegli il tipo di endpoint ospitato da VPC per ospitare l'endpoint del tuo server.

   b. Per Access, scegli Internet Facing per rendere il tuo endpoint accessibile ai client su Internet.

   > **Note**
   >
   > Quando scegli Internet Facing, puoi scegliere un indirizzo IP elastico esistente in ogni sottorete o sottoreti. Oppure puoi andare alla console VPC (https://console.aws.amazon.com/vpc/) per allocare uno o più nuovi indirizzi IP elastici. Questi indirizzi possono essere di proprietà dell'utente AWS o dell'utente. Non puoi associare indirizzi IP elastici già in uso al tuo endpoint.

   c. (Facoltativo) Per Nome host personalizzato, scegli una delle seguenti opzioni:

   > **Note**
   >
   > I clienti AWS GovCloud (US) devono connettersi direttamente tramite l'indirizzo IP elastico o creare un record di nome host all'interno di Commercial Route 53 che punti al proprio EIP. Per ulteriori informazioni sull'uso di Route 53 per gli GovCloud endpoint, consulta Configurare Amazon Route 53 con AWS GovCloud (US) le tue risorse nella Guida per l'AWS GovCloud (US) utente.

- Alias DNS Amazon Route 53: se il nome host che desideri utilizzare è registrato con Route 53. Puoi quindi inserire il nome host.
- Altro DNS: se il nome host che desideri utilizzare è registrato con un altro provider DNS. È quindi possibile inserire il nome host.
- Nessuno: per utilizzare l'endpoint del server e non utilizzare un nome host personalizzato. Il nome host del server ha il formato *server-id*.server.transfer.*region*.amazonaws.com.

> **Note**
>
> Per i clienti che utilizzano AWS GovCloud (US), selezionando Nessuno non viene creato un nome host in questo formato.

Per ulteriori informazioni sull'utilizzo di nomi host personalizzati, consulta. Lavorare con nomi host personalizzati

d. Per VPC, scegli un ID VPC esistente o scegli Crea un VPC per creare un nuovo VPC.

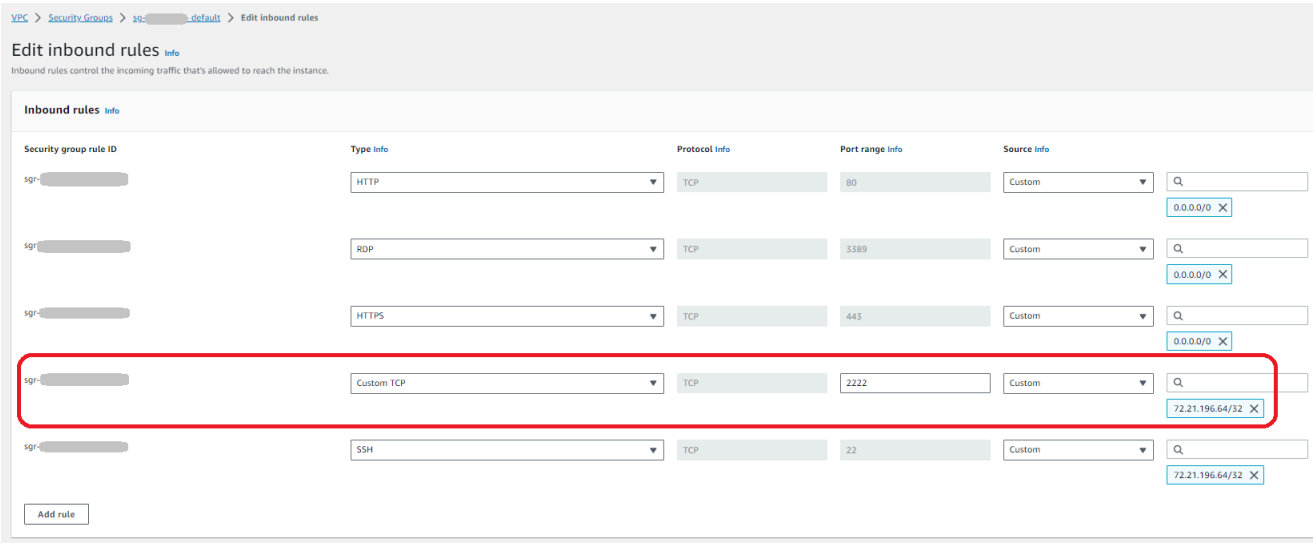
e. Nella sezione Zone di disponibilità, scegli fino a tre zone di disponibilità e sottoreti associate. Per gli indirizzi IPv4, scegli un indirizzo IP elastico per ogni sottorete. Questo è l'indirizzo IP che i tuoi clienti possono utilizzare per consentire l'accesso all'endpoint nei loro firewall.

f. Nella sezione Gruppi di sicurezza, scegli uno o più ID del gruppo di sicurezza esistenti o scegli Crea un gruppo di sicurezza per creare un nuovo gruppo di sicurezza. Per ulteriori informazioni sui gruppi di sicurezza, consulta la sezione Gruppi di sicurezza per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud. Per creare un gruppo di sicurezza, consulta Creazione di un gruppo di sicurezza nella Amazon Virtual Private Cloud User Guide.

> **Note**
>
> Il tuo VPC include automaticamente un gruppo di sicurezza predefinito. Se non specifichi uno o più gruppi di sicurezza diversi all'avvio del server, associamo il gruppo di sicurezza predefinito al tuo server.

Per le regole in entrata per il gruppo di sicurezza, puoi configurare il traffico SSH per utilizzare le porte 22, 2222, 22000 o qualsiasi combinazione. La porta 22 è configurata per impostazione predefinita. Per utilizzare la porta 2222 o la porta 22000, aggiungi una regola in entrata al tuo gruppo di sicurezza. Per il tipo, scegli TCP personalizzato, quindi inserisci uno **`2222`** o **`22000`** per Intervallo di porte e, per l'origine, inserisci lo stesso intervallo CIDR che hai utilizzato per la regola della porta SSH 22.

> **Note**
>
> Puoi anche utilizzare la porta 2223 per i client che richiedono ACK «piggy-back» TCP o la possibilità che il pack finale dell'handshake TCP a 3 vie contenga anche dati.
>
> Alcuni software client potrebbero essere incompatibili con la porta 2223, ad esempio un client che richiede al server di inviare la stringa di identificazione SFTP prima che il client lo faccia.



g. (Facoltativo) Per FIPS Enabled, selezionate la casella di controllo FIPS Enabled Endpoint per assicurarvi che l'endpoint sia conforme ai Federal Information Processing Standards (FIPS).

> **Note**
>
> Gli endpoint compatibili con FIPS sono disponibili solo nelle regioni del Nord America. AWS Per le regioni disponibili, consulta gli AWS Transfer Family endpoint e le quote nel. Riferimenti generali di AWS Per ulteriori informazioni su FIPS, vedere Federal Information Processing Standard (FIPS) 140-2.

h. Seleziona Successivo.

6. In Configura dettagli aggiuntivi, procedi come segue:

   a. Per la CloudWatch registrazione, scegli una delle seguenti opzioni per abilitare la CloudWatch registrazione Amazon dell'attività dell'utente:

      - Crea un nuovo ruolo per consentire a Transfer Family di creare automaticamente il ruolo IAM, purché tu disponga delle autorizzazioni giuste per creare un nuovo ruolo. Viene chiamato `AWSTransferLoggingAccess` il ruolo IAM creato.
      - Scegli un ruolo esistente per scegliere un ruolo IAM esistente dal tuo account. In Ruolo di registrazione, scegli il ruolo. Questo ruolo IAM dovrebbe includere una politica di fiducia con Service impostato `transfer.amazonaws.com` su.

      Per ulteriori informazioni sulla CloudWatch registrazione, vedereConfigura il CloudWatch ruolo di registrazione.

> **Note**
>
> - Non è possibile visualizzare l'attività dell'utente finale CloudWatch se non si specifica un ruolo di registrazione.
> - Se non desideri impostare un ruolo di CloudWatch registrazione, seleziona Scegli un ruolo esistente, ma non selezionare un ruolo di registrazione.

   b. Per le opzioni relative agli algoritmi crittografici, scegli una politica di sicurezza che contenga gli algoritmi crittografici abilitati per l'uso da parte del tuo server.

> **Note**
>
> Per impostazione predefinita, la politica `TransferSecurityPolicy-2020-06` di sicurezza è collegata al server a meno che non ne scelga una diversa.

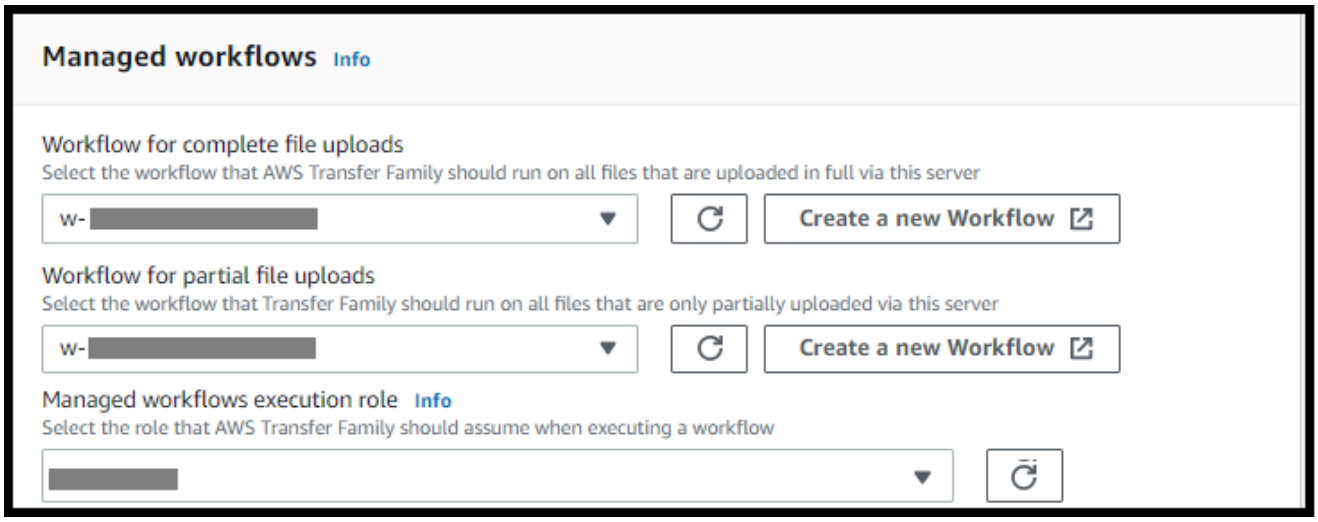
Per ulteriori informazioni sulle policy di sicurezza, consulta Politiche di sicurezza per AWS Transfer Family i server.

c. (Facoltativo: questa sezione riguarda solo la migrazione degli utenti da un server compatibile con SFTP esistente.) Per Server Host Key, inserite una chiave privata RSA, ED25519 o ECDSA che verrà utilizzata per identificare il server quando i client si connettono ad esso tramite SFTP.

d. (Facoltativo) Per Tag, per Chiave e Valore, inserite uno o più tag come coppie chiave-valore, quindi scegliete Aggiungi tag.

e. Seleziona Successivo.

f. (Facoltativo) Per i flussi di lavoro gestiti, scegliete gli ID del flusso di lavoro (e un ruolo corrispondente) che Transfer Family deve assumere durante l'esecuzione del flusso di lavoro. È possibile scegliere un flusso di lavoro da eseguire dopo un caricamento completo e un altro da eseguire dopo un caricamento parziale. Per ulteriori informazioni sull'elaborazione dei file utilizzando flussi di lavoro gestiti, consultaAWS Transfer Family flussi di lavoro gestiti.



7. In Rivedi e crea, esamina le tue scelte. Se:

   - Se desideri modificarne una, scegli Modifica accanto al passaggio.

> **Note**
>
> Dovrai rivedere ogni passaggio dopo il passaggio che hai scelto di modificare.

- Non apporti modifiche, scegli Crea server per creare il tuo server. Viene visualizzata la pagina Servers (Server), mostrata di seguito, in cui è elencato il nuovo server.

Puoi scegliere l'ID del server per vedere le impostazioni dettagliate del server che hai appena creato. Dopo aver compilato la colonna Indirizzo IPv4 pubblico, gli indirizzi IP elastici forniti vengono associati correttamente all'endpoint del server.

> **Note**
>
> Quando il server in un VPC è online, solo le sottoreti possono essere modificate e solo tramite l'API. UpdateServer È necessario interrompere il server per aggiungere o modificare gli indirizzi IP elastici dell'endpoint del server.

Cambia il tipo di endpoint per il tuo server

Se disponi di un server esistente accessibile tramite Internet (ovvero con un tipo di endpoint pubblico), puoi cambiarne l'endpoint in un endpoint VPC.

> **Note**
>
> Se hai un server esistente in un VPC visualizzato come`VPC_ENDPOINT`, ti consigliamo di modificarlo con il nuovo tipo di endpoint VPC. Con questo nuovo tipo di endpoint, non è più necessario utilizzare un Network Load Balancer (NLB) per associare gli indirizzi IP elastici all'endpoint del server. Inoltre, puoi utilizzare i gruppi di sicurezza VPC per limitare l'accesso all'endpoint del tuo server. Tuttavia, puoi continuare a utilizzare il tipo di `VPC_ENDPOINT` endpoint secondo necessità.

La procedura seguente presuppone che si disponga di un server che utilizza il tipo di endpoint pubblico corrente o il tipo precedente. `VPC_ENDPOINT`

Per modificare il tipo di endpoint per il server

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione, selezionare Servers (Server).
3. Seleziona la casella di controllo del server di cui desideri modificare il tipo di endpoint.

   > **Important**
   >
   > È necessario arrestare il server prima di poter modificare l'endpoint.

4. In Actions (Operazioni), scegliere Stop (Arresta).
5. Nella finestra di dialogo di conferma che appare, scegli Stop per confermare che desideri arrestare il server.

   > **Note**
   >
   > Prima di procedere al passaggio successivo, nella sezione Dettagli dell'endpoint, attendi che lo stato del server passi a Offline; l'operazione può richiedere un paio di minuti. Potrebbe essere necessario scegliere Aggiorna nella pagina Server per visualizzare la modifica dello stato.
   > Non potrai apportare modifiche finché il server non sarà offline.

6. Nei dettagli dell'endpoint, scegli Modifica.
7. In Modifica configurazione dell'endpoint, procedi come segue:

   a. Per Modifica tipo di endpoint, scegli VPC ospitato.

   b. Per Access, scegli una delle seguenti opzioni:

      - Interno per rendere l'endpoint accessibile solo ai client che utilizzano gli indirizzi IP privati dell'endpoint.
      - Internet Facing per rendere l'endpoint accessibile ai clienti sulla rete Internet pubblica.

        > **Note**
        >
        > Quando scegli Internet Facing, puoi scegliere un indirizzo IP elastico esistente in ogni sottorete o sottoreti. In alternativa, puoi accedere alla console VPC (https://console.aws.amazon.com/vpc/) per allocare uno o più nuovi indirizzi IP elastici.

Questi indirizzi possono essere di proprietà dell'utente AWS o dell'utente. Non puoi associare indirizzi IP elastici già in uso al tuo endpoint.

c. (Facoltativo solo per l'accesso tramite Internet) Per Nome host personalizzato, scegli una delle seguenti opzioni:

- Alias DNS Amazon Route 53: se il nome host che desideri utilizzare è registrato con Route 53. Puoi quindi inserire il nome host.
- Altro DNS: se il nome host che desideri utilizzare è registrato con un altro provider DNS. È quindi possibile inserire il nome host.
- Nessuno: per utilizzare l'endpoint del server e non utilizzare un nome host personalizzato. Il nome host del server ha il formato *serverId*`.server.transfer.`*regionId*`.amazonaws.com`.

  Per ulteriori informazioni sull'utilizzo di nomi host personalizzati, consulta. Lavorare con nomi host personalizzati

d. Per VPC, scegli un ID VPC esistente oppure scegli Crea un VPC per creare un nuovo VPC.

e. Nella sezione Zone di disponibilità, seleziona fino a tre zone di disponibilità e le sottoreti associate. Se scegli Internet Facing, scegli anche un indirizzo IP elastico per ogni sottorete.

> **Note**
>
> Se desideri il massimo di tre zone di disponibilità, ma non ce ne sono abbastanza, creale nella console VPC (https://console.aws.amazon.com/vpc/).
> Se modifichi le sottoreti o gli indirizzi IP elastici, l'aggiornamento del server impiega alcuni minuti. Non è possibile salvare le modifiche fino al completamento dell'aggiornamento del server.

f. Selezionare Salva.

8. Per Azioni, scegli Avvia e attendi che lo stato del server passi a Online; l'operazione può richiedere un paio di minuti.

> **Note**
>
> Se hai cambiato un tipo di endpoint pubblico in un tipo di endpoint VPC, nota che il tipo di endpoint per il tuo server è cambiato in VPC.

Il gruppo di sicurezza predefinito è collegato all'endpoint. Per modificare o aggiungere gruppi di sicurezza aggiuntivi, vedere Creazione di gruppi di sicurezza.

Interruzione dell'uso di VPC_ENDPOINT

AWS Transfer Family sta interrompendo la possibilità di creare server con nuovi account. `EndpointType=VPC_ENDPOINT` AWS A partire dal 19 maggio 2021, AWS gli account che non possiedono AWS Transfer Family server con un tipo di endpoint di non `VPC_ENDPOINT` saranno in grado di creare nuovi server con. `EndpointType=VPC_ENDPOINT` Se possiedi già server che utilizzano il tipo di `VPC_ENDPOINT` endpoint, ti consigliamo di iniziare a utilizzarli `EndpointType=VPC` il prima possibile. Per i dettagli, consulta Aggiornare il tipo di endpoint AWS Transfer Family del server da VPC_ENDPOINT a VPC.

Abbiamo lanciato il nuovo tipo di endpoint all'inizio del 2020`VPC`. Per ulteriori informazioni, vedere AWS Transfer Family perché SFTP supporta i gruppi di sicurezza VPC e gli indirizzi IP elastici. Questo nuovo endpoint è più ricco di funzionalità e conveniente e non prevede costi. PrivateLink Per ulteriori informazioni, consulta la pagina AWS PrivateLink dei prezzi.

Questo tipo di endpoint è funzionalmente equivalente al tipo di endpoint precedente (). `VPC_ENDPOINT` È possibile collegare gli indirizzi IP elastici direttamente all'endpoint per renderlo accessibile a Internet e utilizzare i gruppi di sicurezza per il filtraggio degli IP di origine. Per ulteriori informazioni, consulta il post sul blog Use IP allow to secure your AWS Transfer Family for SFTP servers.

Puoi anche ospitare questo endpoint in un ambiente VPC condiviso. Per ulteriori informazioni, vedi AWS Transfer Family ora supporta gli ambienti VPC con servizi condivisi.

Oltre a SFTP, puoi utilizzare il `EndpointType` VPC per abilitare FTPS e FTP. Non abbiamo intenzione di aggiungere queste funzionalità e il supporto FTPS/FTP a. `EndpointType=VPC_ENDPOINT` Abbiamo anche rimosso questo tipo di endpoint come opzione dalla console. AWS Transfer Family

Puoi modificare il tipo di endpoint per il tuo server utilizzando la console Transfer Family, l'API AWS CLI, gli SDK o. AWS CloudFormation Per modificare il tipo di endpoint del server, consulta. Aggiornamento del tipo di endpoint AWS Transfer Family del server da VPC_ENDPOINT a VPC

In caso di domande, contatta AWS Support o contatta il team addetto AWS all'account.

> **Note**
>
> Non abbiamo intenzione di aggiungere queste funzionalità e il supporto FTPS o FTP a =VPC_ENDPOINT. EndpointType Non lo offriamo più come opzione sulla console. AWS Transfer Family

Se hai altre domande, puoi contattarci tramite AWS Support il team del tuo account.

Aggiornamento del tipo di endpoint AWS Transfer Family del server da VPC_ENDPOINT a VPC

Puoi utilizzare AWS Management Console AWS CloudFormation, o l'API Transfer Family per aggiornare un server `EndpointType` da `VPC_ENDPOINT` a`VPC`. Nelle sezioni seguenti sono disponibili procedure ed esempi dettagliati per l'utilizzo di ciascuno di questi metodi per aggiornare un tipo di endpoint del server. Se disponi di server in più AWS regioni e in più AWS account, puoi utilizzare lo script di esempio fornito nella sezione seguente, con le modifiche, per identificare i server utilizzando il `VPC_ENDPOINT` tipo che dovrai aggiornare.

Argomenti

Identificazione dei server utilizzando il tipo di **`VPC_ENDPOINT`** endpoint

È possibile identificare quali server `VPC_ENDPOINT` utilizzano il AWS Management Console.

Per identificare i server utilizzando il tipo di **`VPC_ENDPOINT`** endpoint utilizzando la console

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Scegli Server nel riquadro di navigazione per visualizzare l'elenco dei server del tuo account in quella regione.
3. Ordina l'elenco dei server in base al tipo di endpoint per visualizzare tutti i server utilizzati`VPC_ENDPOINT`.

Per identificare i server che utilizzano più **VPC_ENDPOINT**AWS regioni e account

Se disponi di server in più AWS regioni e in più AWS account, puoi utilizzare il seguente script di esempio, con modifiche, per identificare i server che utilizzano il tipo di `VPC_ENDPOINT` endpoint. Lo script di esempio utilizza le chiamate ListServers API Amazon EC2 DescribeRegionse Transfer Family per ottenere un elenco degli ID server e delle regioni di tutti i server utilizzati. `VPC_ENDPOINT` Se disponi di molti AWS account, puoi passare in rassegna gli account utilizzando un ruolo IAM con accesso da revisore in sola lettura se esegui l'autenticazione utilizzando i profili di sessione presso il tuo provider di identità.

1. Di seguito è riportato un semplice esempio.

```
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. Dopo aver ottenuto l'elenco dei server da aggiornare, è possibile utilizzare uno dei metodi descritti nelle sezioni seguenti per `EndpointType` aggiornare il fileVPC.

Aggiornamento del tipo di endpoint del server utilizzando il AWS Management Console

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione, selezionare Servers (Server).
3. Seleziona la casella di controllo del server di cui desideri modificare il tipo di endpoint.

> **Important**
>
> È necessario arrestare il server prima di poter modificare l'endpoint.

4. In Actions (Operazioni), scegliere Stop (Arresta).
5. Nella finestra di dialogo di conferma che appare, scegli Stop per confermare che desideri arrestare il server.

> **Note**
>
> Prima di procedere al passaggio successivo, attendi che lo stato del server passi a Offline; l'operazione può richiedere un paio di minuti. Potrebbe essere necessario scegliere Aggiorna nella pagina Server per vedere la modifica dello stato.

6. Dopo che lo stato è passato a Offline, scegli il server per visualizzare la pagina dei dettagli del server.
7. Nella sezione Dettagli dell'endpoint, scegli Modifica.
8. Scegli VPC ospitato per il tipo di endpoint.
9. Seleziona Salva
10. Per Azioni, scegli Avvia e attendi che lo stato del server passi a Online; l'operazione può richiedere un paio di minuti.

Aggiornamento del tipo di endpoint del server tramite AWS CloudFormation

Questa sezione descrive come utilizzare AWS CloudFormation per aggiornare un server `EndpointType` aVPC. Usa questa procedura per i server Transfer Family che hai distribuito utilizzando AWS CloudFormation. In questo esempio, il AWS CloudFormation modello originale utilizzato per distribuire il server Transfer Family è illustrato come segue:

```
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
```

Il modello viene aggiornato con le seguenti modifiche:

- `EndpointType`È stato modificato in`VPC`.
- La `AWS::EC2::VPCEndpoint` risorsa viene rimossa.
- I `SecurityGroupIdSubnetIds`, e `VpcId` sono stati spostati nella `EndpointDetails` sezione della `AWS::Transfer::Server` risorsa,
- La `VpcEndpointId` proprietà di `EndpointDetails` è stata rimossa.

Il modello aggiornato ha il seguente aspetto:

```
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
```

Per aggiornare il tipo di endpoint dei server Transfer Family distribuiti utilizzando AWS CloudFormation

1. Arresta il server che desideri aggiornare utilizzando i seguenti passaggi.

   a. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.

   b. Nel riquadro di navigazione, selezionare Servers (Server).

   c. Seleziona la casella di controllo del server di cui desideri modificare il tipo di endpoint.

   > **Important**
   >
   > È necessario arrestare il server prima di poter modificare l'endpoint.

   d. In Actions (Operazioni), scegliere Stop (Arresta).

   e. Nella finestra di dialogo di conferma che appare, scegli Stop per confermare che desideri arrestare il server.

> **Note**
>
> Prima di procedere al passaggio successivo, attendi che lo stato del server passi a Offline; l'operazione può richiedere un paio di minuti. Potrebbe essere necessario scegliere Aggiorna nella pagina Server per vedere la modifica dello stato.

2. Aggiorna lo stack CloudFormation

   a. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.

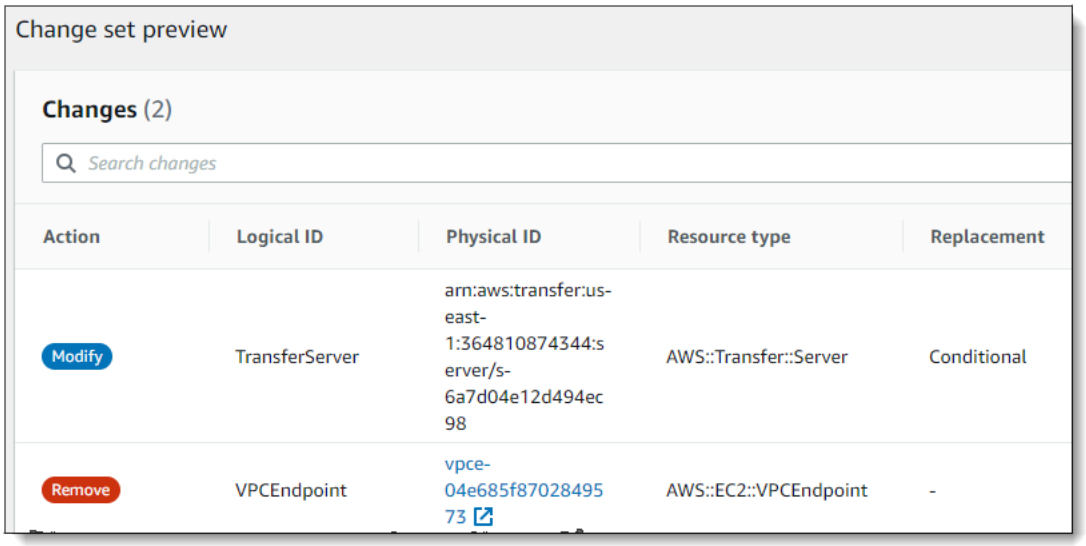
   b. Scegli lo stack utilizzato per creare il server Transfer Family.

   c. Scegli Aggiorna.

   d. Scegli Sostituisci il modello corrente

   e. Carica il nuovo modello. CloudFormation I set di modifiche ti aiutano a capire in che modo le modifiche ai modelli influiranno sulle risorse in esecuzione prima di implementarle. In questo esempio, la risorsa Transfer server verrà modificata e la risorsa VPCEndpoint verrà rimossa. Il server di tipo endpoint VPC crea un endpoint VPC per tuo conto, sostituendo la risorsa originale. `VPCEndpoint`

      Dopo aver caricato il nuovo modello, il set di modifiche sarà simile al seguente:



   f. Aggiornare lo stack.

3. Una volta completato l'aggiornamento dello stack, accedi alla console di gestione Transfer Family all'indirizzo https://console.aws.amazon.com/transfer/.

4. Riavvia il server. Scegli il server in cui hai eseguito l'aggiornamento AWS CloudFormation, quindi scegli Avvia dal menu Azioni.

Aggiornamento del server EndpointType tramite l'API

È possibile utilizzare il comando describe-server o AWS CLI il UpdateServer comando API. Lo script di esempio seguente arresta il server Transfer Family, aggiorna EndpointType, rimuove VPC_ENDPOINT e avvia il server.

```
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])
```

Lavorare con nomi host personalizzati

Il nome host del server è il nome host che gli utenti inseriscono nei loro client quando si connettono al server. Quando lavori, puoi utilizzare un dominio personalizzato che hai registrato come nome host del server. AWS Transfer Family Ad esempio, potresti usare un hostname personalizzato come. `mysftpserver.mysubdomain.domain.com`

Per reindirizzare il traffico dal tuo dominio personalizzato registrato all'endpoint del server, puoi utilizzare Amazon Route 53 o qualsiasi provider DNS (Domain Name System). Route 53 è il servizio DNS che supporta nativamente. AWS Transfer Family

Argomenti

- Usa Amazon Route 53 come provider DNS
- Usa altri provider DNS
- Nomi host personalizzati per server non creati da console

Sulla console, puoi scegliere una di queste opzioni per configurare un nome host personalizzato:

- Alias DNS Amazon Route 53: se il nome host che desideri utilizzare è registrato con Route 53. Puoi quindi inserire il nome host.
- Altro DNS: se il nome host che desideri utilizzare è registrato con un altro provider DNS. È quindi possibile inserire il nome host.
- Nessuno: per utilizzare l'endpoint del server e non utilizzare un nome host personalizzato.

Questa opzione viene impostata quando si crea un nuovo server o si modifica la configurazione di un server esistente. Per ulteriori informazioni sulla creazione di un nuovo server, vedereFase 2: Creare un server compatibile con SFTP. Per ulteriori informazioni sulla modifica della configurazione di un server esistente, vedereModifica i dettagli del server.

Per ulteriori dettagli sull'utilizzo del proprio dominio per il nome host del server e sull' AWS Transfer Family utilizzo di Route 53, consulta le seguenti sezioni.

Usa Amazon Route 53 come provider DNS

Quando crei un server, puoi utilizzare Amazon Route 53 come provider DNS. Prima di utilizzare un dominio con Route 53, devi registrare il dominio. Per ulteriori informazioni, consulta Come funziona la registrazione del dominio nella Amazon Route 53 Developer Guide.

Quando utilizzi Route 53 per fornire il routing DNS al tuo server, AWS Transfer Family utilizza il nome host personalizzato che hai inserito per estrarre la zona ospitata. Quando si AWS Transfer Family estrae una zona ospitata, possono succedere tre cose:

1. Se non conosci Route 53 e non hai una zona ospitata, AWS Transfer Family aggiunge una nuova zona ospitata e un `CNAME` record. Il valore di questo `CNAME` record è il nome host dell'endpoint per il tuo server. Un CNAME è un nome di dominio alternativo.
2. Se hai una zona ospitata in Route 53 senza `CNAME` record, AWS Transfer Family aggiunge un `CNAME` record alla zona ospitata.
3. Se il servizio rileva che un record `CNAME` esiste già nella zona ospitata, viene visualizzato un errore che indica che un record `CNAME` esiste già. In questo caso, modifica il valore del `CNAME` record con il nome host del server.

Per ulteriori informazioni sulle zone ospitate in Route 53, consulta Hosted zone nella Amazon Route 53 Developer Guide.

Usa altri provider DNS

Quando crei un server, puoi utilizzare anche provider DNS diversi da Amazon Route 53. Se utilizzi un provider DNS alternativo, devi accertarti che il traffico dal tuo dominio sia indirizzato all'endpoint del server .

A tale scopo, imposta il dominio sull'hostname dell'endpoint del server. Il nome host di un endpoint ha il seguente aspetto nella console:

```
serverid.server.transfer.region.amazonaws.com
```

> **Note**
>
> Se il server dispone di un endpoint VPC, il formato del nome host è diverso da quello descritto sopra. Per trovare il tuo endpoint VPC, seleziona il VPC nella pagina dei dettagli del

server, quindi seleziona l'ID dell'endpoint VPC nella dashboard VPC. L'endpoint è il primo nome DNS tra quelli elencati.

Nomi host personalizzati per server non creati da console

Quando si crea un server utilizzando AWS Cloud Development Kit (AWS CDK) o tramite la CLI, è necessario aggiungere un tag se si desidera che il server abbia un nome host personalizzato. AWS CloudFormation Quando si crea un server Transfer Family utilizzando la console, l'etichettatura viene eseguita automaticamente.

> **Note**
>
> È inoltre necessario creare un record DNS per reindirizzare il traffico dal dominio all'endpoint del server. Per i dettagli, consulta Lavorare con i record nella Amazon Route 53 Developer Guide.

Usa le seguenti chiavi per il tuo nome host personalizzato:

- Aggiungi `transfer:customHostname` per visualizzare il nome host personalizzato nella console.
- Se utilizzi Route 53 come provider DNS, aggiungi. `transfer:route53HostedZoneId` Questo tag collega il nome host personalizzato all'ID della zona ospitata della Route 53.

Per aggiungere il nome host personalizzato, emettete il seguente comando CLI.

```
aws transfer tag-resource --arn arn:aws:transfer:region:Account AWS:server/server-ID --
tags Key=transfer:customHostname,Value="custom-host-name"
```

Per esempio:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:customHostname,Value="abc.example.com"
```

Se utilizzi Route 53, esegui il seguente comando per collegare il tuo hostname personalizzato al tuo ID della zona ospitata di Route 53.

```
aws transfer tag-resource --arn server-ARN:server/server-ID --tags
 Key=transfer:route53HostedZoneId,Value=HOSTED-ZONE-ID
```

Per esempio:

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:route53HostedZoneId,Value=ABCDE1111222233334444
```

Supponendo i valori di esempio del comando precedente, esegui il comando seguente per visualizzare i tag:

```
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**
>
> Le tue zone pubbliche ospitate e i relativi ID sono disponibili su Amazon Route 53. Accedi AWS Management Console e apri la console Route 53 all'indirizzo https://console.aws.amazon.com/route53/.

Trasferimento di file su un endpoint server utilizzando un client

I file vengono trasferiti tramite il AWS Transfer Family servizio specificando l'operazione di trasferimento in un client. AWS Transfer Family supporta i seguenti client:

- Supportiamo la versione 3 del protocollo SFTP.
- OpenSSH (macOS e Linux)

> **Note**
>
> Questo client funziona solo con server abilitati per Secure Shell (SSH) File Transfer Protocol (SFTP).

- WinSCP (solo Microsoft Windows)
- Cyberduck (Windows, macOS e Linux)
- FileZilla (Windows, macOS e Linux)

Le seguenti limitazioni si applicano a tutti i client:

- Il numero massimo di sessioni SFTP simultanee e multiplex per connessione è 10.
- Esistono due valori di timeout per le connessioni SFTP/FTP/FTPS. Per le connessioni inattive, il valore di timeout è 1800 secondi (30 minuti). Se non vi è alcuna attività dopo lo scadere del periodo, il client potrebbe essere disconnesso. C'è anche un timeout di 300 secondi (5 minuti) quando un client non risponde completamente.
- Amazon S3 e Amazon EFS (a causa del protocollo NFSv4) richiedono che i nomi dei file abbiano la codifica UTF-8. L'utilizzo di codifiche diverse può portare a risultati imprevisti. Per Amazon S3, consulta le linee guida per la denominazione delle chiavi degli oggetti.
- Per File Transfer Protocol over SSL (FTPS), è supportata solo la modalità Explicit. La modalità implicita non è supportata.
- Per File Transfer Protocol (FTP) e FTPS, è supportata solo la modalità Passiva.
- Per FTP e FTPS, è supportata solo la modalità STREAM.
- Per FTP e FTPS, è supportata solo la modalità Image/Binary.
- Per FTP e FTPS, TLS - PROT C (non protetto) TLS per la connessione dati è l'impostazione predefinita, ma PROT C non è supportato nel protocollo FTPS. AWS Transfer Family Quindi, per FTPS, è necessario emettere PROT P affinché le operazioni relative ai dati vengano accettate.
- Se utilizzi Amazon S3 per lo storage del tuo server e se il tuo client contiene un'opzione per utilizzare più connessioni per un singolo trasferimento, assicurati di disabilitare l'opzione. Altrimenti, i caricamenti di file di grandi dimensioni possono fallire in modi imprevedibili. Tieni presente che se utilizzi Amazon EFS come backend di storage, EFS supporta più connessioni per un singolo trasferimento.

Di seguito è riportato un elenco di comandi disponibili per FTP e FTPS:

Comandi disponibili					
- LAVORARE	PRODEZZA	LA MAGGIOR PARTE	PASSARE	RETR	STORMO
AUTENTICAZIONE	LANG	MOD	PASV	RMD	STOU
COPPA	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NST	PORTO	AFFITTARE	CISTI
DELE	MFMT	NOOP	PWD	SIZE	TYPE
EPSV	MLSD	OPTA	QUIT	SUBITO	UTENTE

> **Note**
>
> APPE non è supportato.

Per SFTP, le seguenti operazioni non sono attualmente supportate per gli utenti che utilizzano la home directory logica su server che utilizzano Amazon Elastic File System (Amazon EFS).

Comandi SFTP non supportati			
LINK SSH_FXP_READ	SSH_FXP_LINK	SSH_FXP_STAT quando il file richiesto è un collegamento simbolico	SSH_FXP_REALPATH quando il percorso richiesto contiene componenti di symlink

Genera una coppia di chiavi pubblica-privata

Prima di poter trasferire un file, è necessario disporre di una coppia di chiavi pubblica-privata. Se non hai mai generato una key pair in precedenza, vediGenera chiavi SSH per gli utenti gestiti dal servizio.

Argomenti

Comandi SFTP/FTPS/FTP disponibili

La tabella seguente descrive i comandi disponibili per AWS Transfer Family, per i protocolli SFTP, FTPS e FTP.

> **Note**
>
> La tabella menziona file e directory per Amazon S3, che supporta solo bucket e oggetti: non esiste una gerarchia. Tuttavia, puoi utilizzare prefissi nei nomi delle chiavi degli oggetti per implicare una gerarchia e organizzare i dati in modo simile alle cartelle. Questo comportamento è descritto in Utilizzo dei metadati degli oggetti nella Guida per l'utente di Amazon Simple Storage Service.

Comandi SFTP/FTPS/FTP

Comando	Amazon S3	Amazon EFS
`cd`	Supportato	Supportato
`chgrp`	Non supportato	Supportato (o solo) `root` `owner`
`chmod`	Non supportato	Supportato (`root`solo)

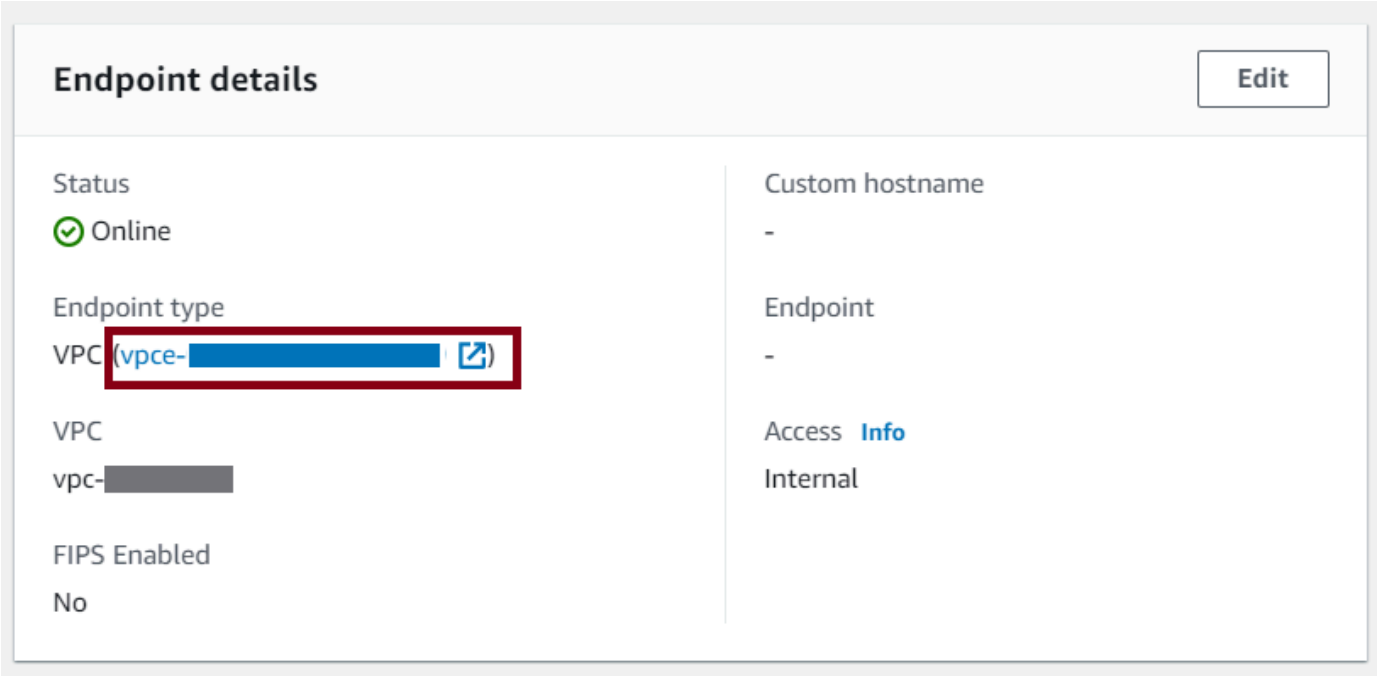
Comando	Amazon S3	Amazon EFS
`chmtime`	Non supportato	Supportata
`chown`	Non supportato	Supportato (`root`solo)
`get`	Supportato	Supportato (inclusa la risoluzione di collegamenti simbolici)
`ln -s`	Non supportato	Supportato
`ls/dir`	Supportato	Supportato
`mkdir`	Supportato	Supportato
`put`	Supportato	Supportato
`pwd`	Supportato	Supportato
`rename`	Supportato solo per i file	Supportato **Note** La ridenominazione che sovrascriverebbe un file o una directory esistente non è supportata.
`rm`	Supportato	Supportato
`rmdir`	Supportato (solo cartelle vuote)	Supportato
`version`	Supportato	Supportato

Trova il tuo endpoint Amazon VPC

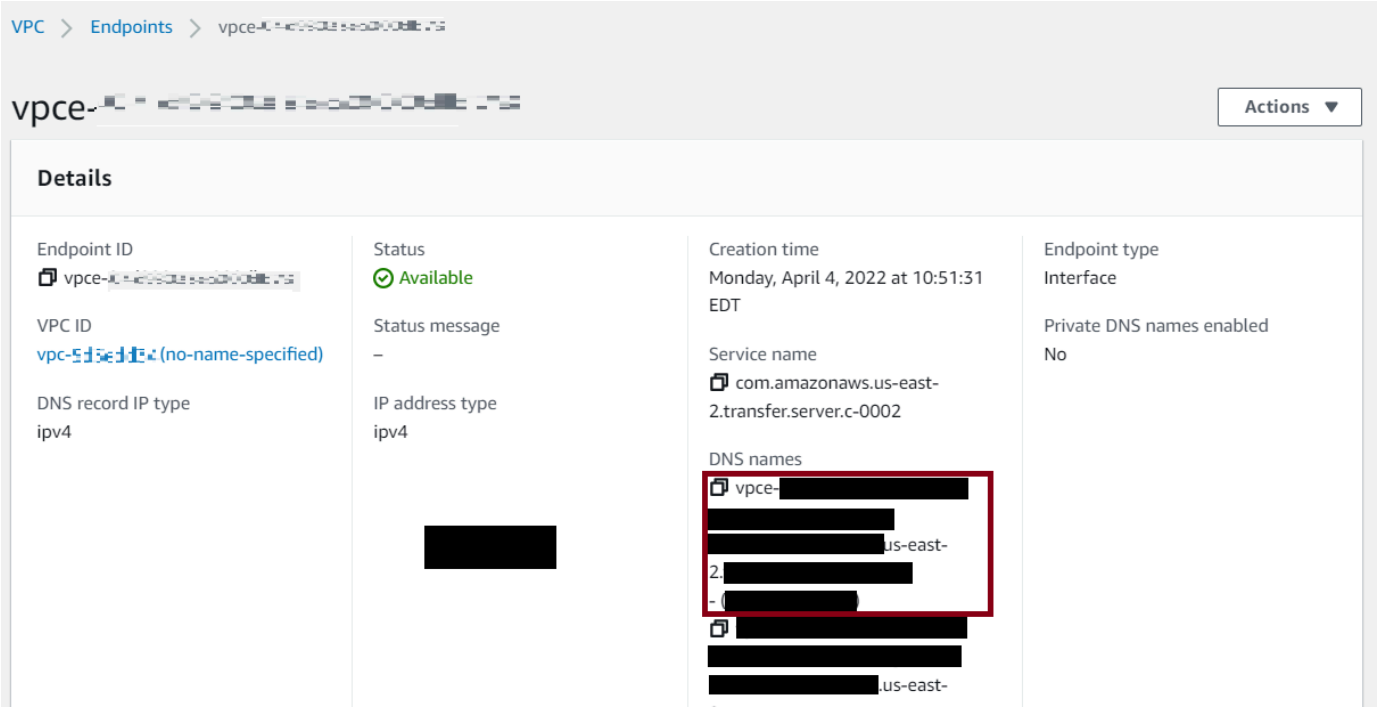
Se il tipo di endpoint per il server Transfer Family è VPC, identificare l'endpoint da utilizzare per il trasferimento dei file non è semplice. In questo caso, usa la seguente procedura per trovare il tuo endpoint Amazon VPC.

Trova il tuo endpoint Amazon VPC

1. Vai alla pagina dei dettagli del tuo server.
2. Nel riquadro dei dettagli dell'endpoint, seleziona il VPC.



3. Nella dashboard di Amazon VPC, seleziona l'ID dell'endpoint VPC.
4. Nell'elenco dei nomi DNS, l'endpoint del server è il primo elencato.



`setstat`Evita gli errori

Alcuni client di trasferimento di file SFTP possono tentare di modificare gli attributi dei file remoti, inclusi timestamp e autorizzazioni, utilizzando comandi come SETSTAT durante il caricamento del file. Tuttavia, questi comandi non sono compatibili con i sistemi di archiviazione degli oggetti, come Amazon S3. A causa di questa incompatibilità, i caricamenti di file da questi client possono causare errori anche quando il file viene caricato correttamente.

- Quando chiami l'`UpdateServer`API `CreateServer` o, utilizza l'`ProtocolDetails`opzione `SetStatOption` per ignorare l'errore generato quando il client tenta di utilizzare SETSTAT su un file che stai caricando in un bucket S3.
- Impostare il valore su `ENABLE_NO_OP` per fare in modo che il server Transfer Family ignori il comando SETSTAT e carichi i file senza che sia necessario modificare il client SFTP.
- Tieni presente che, sebbene l'*`SetStatOption`**`ENABLE_NO_OP`*impostazione ignori l'errore, genera una voce di registro in CloudWatch Logs, in modo da poter determinare quando il client sta effettuando una chiamata SETSTAT.

Per i dettagli dell'API per questa opzione, consulta. ProtocolDetails

Usa OpenSSH

Utilizza le istruzioni che seguono per trasferire i file dalla riga di comando tramite OpenSSH.

> **Note**
>
> Questo client funziona solo con un server compatibile con SFTP.

Per trasferire file AWS Transfer Family utilizzando l'utilità da riga di comando OpenSSH

1. Su Linux, macOS o Windows, apri un terminale di comando.
2. Al prompt, inserisci il seguente comando:

   ```
   sftp -i transfer-key sftp_user@service_endpoint
   ```

   Nel comando precedente, *sftp_user* è il nome utente e la chiave *transfer-key* privata SSH. Qui *service_endpoint* è l'endpoint del server come mostrato nella AWS Transfer Family console per il server selezionato.

   > **Note**
   >
   > Questo comando utilizza le impostazioni presenti nel `ssh_config` file predefinito. A meno che non abbiate precedentemente modificato questo file, SFTP utilizza la porta 22. È possibile specificare una porta diversa (ad esempio 2222) aggiungendo un **`-P`** flag al comando, come segue.
   >
   > ```
   > sftp -P 2222 -i transfer-key sftp_user@service_endpoint
   > ```
   >
   > In alternativa, se desideri utilizzare sempre la porta 2222 o la porta 22000, puoi aggiornare la porta predefinita nel `ssh_config` file.

   Viene visualizzato un prompt `sftp`.
3. (Facoltativo) Per visualizzare la home directory dell'utente, immettete il seguente comando al `sftp` prompt:

   ```
   pwd
   ```

4. Per caricare un file dal tuo file system al server Transfer Family, usa il `put` comando. Ad esempio, per caricare `hello.txt` (supponendo che il file si trovi nella directory corrente del file system), esegui il comando seguente al `sftp` prompt:

   ```
   put hello.txt
   ```

   Viene visualizzato un messaggio simile al seguente, che indica che il trasferimento del file è in corso o completato.

   ```
   Uploading hello.txt to /my-bucket/home/sftp_user/hello.txt

   hello.txt 100% 127 0.1KB/s 00:00
   ```

> **Note**
>
> Dopo la creazione del server, possono essere necessari alcuni minuti prima che il nome host dell'endpoint del server sia risolvibile dal servizio DNS dell'ambiente in uso.

Usa WinSCP

Utilizza le istruzioni che seguono per trasferire i file dalla riga di comando tramite WinSCP.

> **Note**
>
> Se utilizzi WinSCP 5.19, puoi connetterti direttamente ad Amazon S3 utilizzando le tue credenziali e caricare/scaricare file. AWS Per ulteriori dettagli, consulta Connessione al servizio Amazon S3.

Per trasferire file AWS Transfer Family tramite WinSCP

1. Aprire il client WinSCP.
2. Nella finestra di dialogo di accesso, per File protocol, scegli un protocollo: SFTP o FTP.

   Se avete scelto FTP, per la crittografia scegliete una delle seguenti opzioni:

   - Nessuna crittografia per FTP
   - TLS/SSL Crittografia esplicita per FTPS

3. Per Host name (Nome host), immettere l'endpoint del server. L'endpoint del server si trova nella pagina dei dettagli del server. Per ulteriori informazioni, consulta Visualizza i dettagli dei server SFTP, FTPS e FTP.

   > **Note**
   >
   > Se il tuo server utilizza un endpoint VPC, vedi. Trova il tuo endpoint Amazon VPC

4. Per Numero di porta, inserisci quanto segue:

   - **22**per SFTP
   - **21**per FTP/FTPS

5. Per Nome utente, inserisci il nome dell'utente che hai creato per il tuo provider di identità specifico.

   > **Note**
   >
   > Il nome utente deve essere uno degli utenti che hai creato o configurato per il tuo provider di identità. AWS Transfer Family fornisce i seguenti provider di identità:
   >
   > - Lavorare con utenti gestiti dal servizio
   > - Utilizzo del provider di identità AWS Directory Service
   > - Lavorare con provider di identità personalizzati

6. Scegliete Avanzate per aprire la finestra di dialogo Impostazioni avanzate del sito. Nella sezione SSH, scegli Autenticazione.

7. Per il file della chiave privata, cerca e scegli il file della chiave privata SSH dal tuo file system.

   > **Note**
   >
   > Se WinSCP offre la possibilità di convertire la chiave privata SSH nel formato PPK, scegliete OK.

8. Scegliere OK per tornare alla finestra di dialogo Login (Accesso), quindi selezionare Save (Salva).

9. Nella finestra di dialogo Salva sessione come sito, scegliete OK per completare la configurazione della connessione.

10. Nella finestra di dialogo di accesso, scegliete Strumenti, quindi scegliete Preferenze.
11. Nella finestra di dialogo Preferenze, per Trasferimento, scegliete Resistenza.

    Per l'opzione Abilita trasferimento resume/trasferimento a nome file temporaneo per, scegliete Disabilita.

    > **Note**
    >
    > Se lasci questa opzione abilitata, aumenta i costi di caricamento, diminuendo notevolmente le prestazioni di caricamento. Inoltre, può causare errori nel caricamento di file di grandi dimensioni.

12. Per Trasferimento, scegliete Sfondo e deselezionate la casella di controllo Usa più connessioni per un singolo trasferimento.

    > **Note**
    >
    > Se lasci selezionata questa opzione, i caricamenti di file di grandi dimensioni possono fallire in modi imprevedibili. Ad esempio, è possibile creare caricamenti multiparte orfani che prevedono costi per Amazon S3. Può verificarsi anche un danneggiamento silenzioso dei dati.

13. Esegui il trasferimento dei file.

    È possibile utilizzare drag-and-drop metodi per copiare i file tra la finestra di destinazione e quella di origine. È possibile utilizzare le icone della barra degli strumenti per caricare, scaricare, eliminare, modificare o modificare le proprietà dei file in WinSCP.

> **Note**
>
> Questa nota non si applica se utilizzi Amazon EFS per lo storage.
> I comandi che tentano di modificare gli attributi dei file remoti, inclusi i timestamp, non sono compatibili con i sistemi di storage di oggetti come Amazon S3. Pertanto, se utilizzi Amazon S3 per lo storage, assicurati di disabilitare le impostazioni del timestamp WinSCP (o di utilizzarle `SetStatOption` come descritto in) prima di eseguire i trasferimenti di file. `setstat`Evita gli errori A tale scopo, nella finestra di dialogo delle impostazioni di WinSCP

Transfer, disabilitate l'opzione di caricamento Set permissions e l'opzione comune Preserve timestamp.

Usa Cyberduck

Utilizza le istruzioni che seguono per trasferire i file dalla riga di comando tramite Cyberduck.

Per trasferire file tramite Cyberduck AWS Transfer Family

1. Apri il client Cyberduck.
2. Scegli Apri connessione.
3. Nella finestra di dialogo Apri connessione, scegliete un protocollo: SFTP (SSH File Transfer Protocol), FTP-SSL (Explicit AUTH TLS) o FTP (File Transfer Protocol).
4. Per Server, inserite l'endpoint del server. L'endpoint del server si trova nella pagina dei dettagli del server. Per ulteriori informazioni, consulta Visualizza i dettagli dei server SFTP, FTPS e FTP.

   > **Note**
   >
   > Se il tuo server utilizza un endpoint VPC, vedi. Trova il tuo endpoint Amazon VPC

5. Per Numero di porta, inserisci quanto segue:

   - **22**per SFTP
   - **21**per FTP/FTPS
6. Per Username (Nome utente), immettere il nome per l'utente creato in Gestione degli utenti per gli endpoint del server.
7. Se è selezionato SFTP, per Chiave privata SSH, scegli o inserisci la chiave privata SSH.
8. Scegli Connetti.
9. Esegui il trasferimento dei file.

   In base alla posizione dei file, eseguire una delle seguenti operazioni:

   - Nella tua directory locale (l'origine), scegli i file che desideri trasferire e trascinali nella directory Amazon S3 (la destinazione).
   - Nella directory Amazon S3 (l'origine), scegli i file che desideri trasferire e trascinali nella tua directory locale (la destinazione).

Usa FileZilla

Usa le istruzioni che seguono per trasferire file utilizzando FileZilla.

FileZilla Per configurare un trasferimento di file

1. Apri il FileZilla client.
2. Scegli File, quindi scegli Site Manager.
3. Nella finestra di dialogo Gestione siti, scegliete Nuovo sito.
4. Nella scheda Generale, per Protocollo, scegliete un protocollo: SFTP o FTP.

   Se avete scelto FTP, per Crittografia, scegliete una delle seguenti opzioni:

   - Usa solo FTP semplice (non sicuro), per FTP
   - Utilizzate l'FTP esplicito su TLS, se disponibile, per FTPS
5. Come nome host, inserisci il protocollo che stai utilizzando, seguito dall'endpoint del server. L'endpoint del server si trova nella pagina dei dettagli del server. Per ulteriori informazioni, consulta Visualizza i dettagli dei server SFTP, FTPS e FTP.

   > **Note**
   >
   > Se il tuo server utilizza un endpoint VPC, vedi. Trova il tuo endpoint Amazon VPC

   - Se stai usando SFTP, inserisci: `sftp://`*`hostname`*
   - Se stai usando FTPS, inserisci: `ftps://`*`hostname`*

   Assicuratevi di sostituire l'*`hostname`* con l'endpoint effettivo del server.
6. Per Numero di porta, inserisci quanto segue:

   - **22**per SFTP
   - **21**per FTP/FTPS
7. Se è selezionato SFTP, per Tipo di accesso, scegliete File chiave.

   Per File chiave, scegli o inserisci la chiave privata SSH.
8. Per Utente, inserisci il nome dell'utente in Gestione degli utenti per gli endpoint del server cui hai creato.

9. Scegli Connetti.
10. Esegui il trasferimento del file.

> **Note**
>
> Se interrompi un trasferimento di file in corso, AWS Transfer Family potresti scrivere un oggetto parziale nel tuo bucket Amazon S3. Se interrompi un caricamento, verifica che la dimensione del file nel bucket Amazon S3 corrisponda alla dimensione del file dell'oggetto sorgente prima di continuare.

Usa un client Perl

Se si utilizza il client NET::SFTP::Foreign perl, è necessario impostare su. `queue_size` 1 Per esempio:

```
my $sftp = Net::SFTP::Foreign->new('user@s-12345.server.transfer.us-east-2.amazonaws.com', queue_size => 1);
```

> **Note**
>
> Questa soluzione alternativa è necessaria per le revisioni `Net::SFTP::Foreign` precedenti alla 1.92.02.

Elaborazione successiva al caricamento

Puoi visualizzare le informazioni di elaborazione post-caricamento, inclusi i metadati degli oggetti Amazon S3 e le notifiche degli eventi.

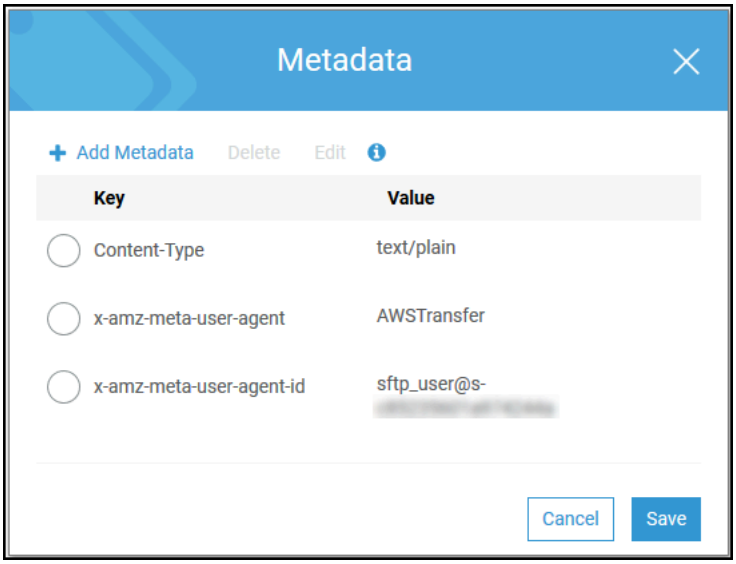
Argomenti

- Metadati degli oggetti Amazon S3
- Notifiche di eventi Amazon S3

Metadati degli oggetti Amazon S3

Come parte dei metadati del tuo oggetto, vedi una chiave chiamata `x-amz-meta-user-agent` il cui valore è `AWSTransfer` e `x-amz-meta-user-agent-id` il cui valore è. `username@server-`

`id` `username`È l'utente Transfer Family che ha caricato il file ed `server-id` è il server utilizzato per il caricamento. È possibile accedere a queste informazioni utilizzando l'HeadObjectoperazione sull'oggetto S3 all'interno della funzione Lambda.



Notifiche di eventi Amazon S3

Quando un oggetto viene caricato nel tuo bucket S3 utilizzando Transfer Family, `RoleSessionName` è contenuto nel campo Requester nella struttura di notifica degli eventi S3 come. `[AWS:Role Unique Identifier]/username.sessionid@server-id` Ad esempio, di seguito sono riportati i contenuti di un campo Requester di esempio da un log di accesso S3 per un file che è stato copiato nel bucket S3.

`arn:aws:sts::AWS-Account-ID:assumed-role/`*`IamRoleName`*`/username.sessionid@server-id`

Nel campo Requester riportato sopra, mostra il ruolo IAM chiamato. `IamRoleName` Per ulteriori informazioni sulla configurazione delle notifiche degli eventi S3, consulta la sezione Configurazione delle notifiche degli eventi di Amazon S3 nella Amazon Simple Storage Service Developer Guide. Per ulteriori informazioni sugli identificatori univoci dei ruoli AWS Identity and Access Management (IAM), consulta Identificatori univoci nella Guida per l'utente.AWS Identity and Access Management

Gestione degli utenti per gli endpoint del server

Nelle sezioni seguenti, puoi trovare informazioni su come aggiungere utenti utilizzando AWS Transfer Family AWS Directory Service for Microsoft Active Directory o un provider di identità personalizzato.

Se si utilizza un tipo di identità gestito dal servizio, si aggiungono utenti al server abilitato al protocollo di trasferimento file. In tal caso, ogni nome utente deve essere univoco sul server.

Come parte delle proprietà di ogni utente, puoi anche archiviare la chiave pubblica SSH (Secure Shell) dell'utente. Questa operazione è necessaria per l'autenticazione basata su chiavi, utilizzata da questa procedura. La chiave privata viene archiviata localmente sul computer dell'utente. Quando l'utente invia una richiesta di autenticazione al server utilizzando un client, il server conferma innanzitutto che l'utente ha accesso alla chiave privata SSH associata. Il server quindi autentica correttamente l'utente.

Inoltre, si specifica la home directory o la directory di destinazione di un utente e si assegna un ruolo AWS Identity and Access Management (IAM) all'utente. Facoltativamente, puoi fornire una politica di sessione per limitare l'accesso degli utenti solo alla home directory del tuo bucket Amazon S3.

> **Important**
>
> AWS Transfer Familyimpedisce ai nomi utente di 1 o 2 caratteri di autenticarsi sui server SFTP. Inoltre, blocchiamo anche il nome utente. `root`
> Il motivo alla base di ciò è dovuto all'elevato volume di tentativi di accesso malevoli da parte degli scanner di password.

Confronto tra Amazon EFS e Amazon S3

Caratteristiche di ciascuna opzione di storage:

- Per limitare l'accesso: Amazon S3 supporta le policy di sessione; Amazon EFS supporta gli ID utente, di gruppo e di gruppo secondari POSIX
- Entrambi supportano chiavi pubbliche/private
- Entrambi supportano le home directory
- Entrambi supportano le directory logiche

> **Note**
>
> Per Amazon S3, la maggior parte del supporto per le directory logiche avviene tramite API/CLI. Puoi utilizzare la casella di controllo Restricted nella console per bloccare un utente nella sua home directory, ma non puoi specificare una struttura di directory virtuale.

Directory logiche

Se si specificano valori di directory logica per l'utente, il parametro utilizzato dipende dal tipo di utente.

- Per gli utenti gestiti dal servizio, fornisci i valori della directory logica in. `HomeDirectoryMappings`
- Per gli utenti di provider di identità personalizzati, fornisci i valori della directory logica in. `HomeDirectoryDetails`

Argomenti

- Lavorare con utenti gestiti dal servizio
- Utilizzo del provider di identità AWS Directory Service
- Lavorare con provider di identità personalizzati

Lavorare con utenti gestiti dal servizio

Puoi aggiungere utenti gestiti dal servizio Amazon S3 o Amazon EFS al tuo server, a seconda dell'impostazione del dominio del server. Per ulteriori informazioni, consulta Configurazione di un endpoint server SFTP, FTPS o FTP.

Per aggiungere un utente gestito dal servizio a livello di codice, consulta l'esempio relativo all'API. CreateUser

> **Note**
>
> Per gli utenti gestiti dal servizio è previsto un limite di 2.000 voci della directory logica. Per informazioni sull'utilizzo delle directory logiche, vedere. Utilizzo di directory logiche per semplificare le strutture di directory Transfer Family

Argomenti

- Aggiungere utenti gestiti dal servizio Amazon S3
- Aggiungere utenti gestiti dal servizio Amazon EFS
- Gestione degli utenti gestiti dal servizio

Aggiungere utenti gestiti dal servizio Amazon S3

> **Note**
>
> Se desideri configurare un bucket Amazon S3 con più account, segui i passaggi indicati in questo articolo del Knowledge Center: Come posso configurare il mio AWS Transfer Family server per utilizzare un bucket Amazon Simple Storage Service che si trova in un altro account? AWS .

Per aggiungere un utente gestito dal servizio Amazon S3 al tuo server

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/, quindi seleziona Server dal pannello di navigazione.
2. Nella pagina Server, seleziona la casella di controllo del server a cui desideri aggiungere un utente.
3. Scegli Add user (Aggiungi utente).
4. Nella sezione Configurazione utente, per Nome utente, inserisci il nome utente. Questo nome utente deve contenere un minimo di 3 e un massimo di 100 caratteri. È possibile utilizzare i seguenti caratteri nel nome utente: a—z, A-Z, 0—9, trattino basso '_', trattino '-', punto ' . ', e al segno «@». Il nome utente non può iniziare con un trattino '-', punto ' . ', o al segno «@».
5. Per Access, scegli il ruolo IAM che hai creato in precedenza che fornisce l'accesso al tuo bucket Amazon S3.

   Questo ruolo IAM è stato creato utilizzando la procedura in Crea un ruolo e una policy IAM. Tale ruolo IAM include una policy IAM che fornisce l'accesso al tuo bucket Amazon S3. Include inoltre una relazione di trust con il servizio AWS Transfer Family, definito in un'altra policy IAM. Se hai bisogno di un controllo granulare degli accessi per i tuoi utenti, consulta il post del blog Enhance data access control with and Amazon AWS Transfer Family S3.
6. (Facoltativo) Per Policy, seleziona una delle seguenti opzioni:

   - Nessuno
   - Politica esistente
   - Seleziona una policy da IAM: ti permette di scegliere una policy di sessione esistente. Scegli Visualizza per vedere un oggetto JSON contenente i dettagli della policy.

- Genera automaticamente una politica basata sulla home directory: genera automaticamente una politica di sessione. Scegli Visualizza per visualizzare un oggetto JSON contenente i dettagli della politica.

> **Note**
>
> Se scegli la politica di generazione automatica in base alla cartella home, non selezionare Restricted per questo utente.

Per ulteriori informazioni sui criteri di sessione, consultaCrea un ruolo e una policy IAM. Per ulteriori informazioni sulla creazione di una politica di sessione, consultaCreazione di una politica di sessione per un bucket Amazon S3.

7. Per la directory Home, scegli il bucket Amazon S3 in cui archiviare i dati da trasferire. AWS Transfer Family Inserisci il percorso della home directory in cui l'utente atterra quando accede utilizzando il suo client.

   Se lasci vuoto questo parametro, viene utilizzata la `root` directory del tuo bucket Amazon S3. In questo caso, assicurarsi che il ruolo IAM fornisca l'accesso a questa directory `root`.

   > **Note**
   >
   > Ti consigliamo di scegliere un percorso di directory che contenga il nome utente dell'utente, che ti consenta di utilizzare in modo efficace una politica di sessione. La policy di sessione limita l'accesso degli utenti nel bucket Amazon S3 alla directory di quell'utente. home

8. (Facoltativo) Per Restricted, seleziona la casella di controllo in modo che i tuoi utenti non possano accedere a nulla al di fuori di quella cartella e non possano vedere il bucket o il nome della cartella Amazon S3.

   > **Note**
   >
   > L'assegnazione all'utente di una home directory e la limitazione dell'utente a tale directory dovrebbero essere sufficienti per bloccare l'accesso dell'utente alla cartella designata. Se devi applicare ulteriori controlli, utilizza una politica di sessione.

Se si seleziona Limitato per questo utente, non è possibile selezionare Genera automaticamente criteri in base alla cartella home, poiché la cartella principale non è un valore definito per gli utenti con restrizioni.

9. Per la chiave pubblica SSH, inserisci la parte della chiave SSH pubblica della coppia di chiavi SSH.

   La chiave viene convalidata dal servizio prima di aggiungere il nuovo utente.

   > **Note**
   >
   > Per istruzioni su come generare una coppia di chiavi SSH, consulta Genera chiavi SSH per gli utenti gestiti dal servizio.

10. (Facoltativo) Per Chiave e Valore, inserite uno o più tag come coppie chiave-valore e scegliete Aggiungi tag.
11. Scegliere Add (Aggiungi) per aggiungere il nuovo utente al server scelto.

    Il nuovo utente viene visualizzato nella sezione Utenti della pagina dei dettagli del server.

Passaggi successivi: per il passaggio successivo, continua conTrasferimento di file su un endpoint server utilizzando un client.

Aggiungere utenti gestiti dal servizio Amazon EFS

Amazon EFS utilizza il modello di autorizzazione dei file POSIX (Portable Operating System Interface) per rappresentare la proprietà dei file.

- Per ulteriori dettagli sulla proprietà dei file di Amazon EFS, consulta la pagina Proprietà dei file di Amazon EFS.
- Per ulteriori dettagli sulla configurazione delle directory per gli utenti EFS, vedereConfigurazione degli utenti Amazon EFS per Transfer Family.

Per aggiungere un utente gestito dal servizio Amazon EFS al tuo server

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/, quindi seleziona Server dal pannello di navigazione.
2. Nella pagina Server, seleziona il server Amazon EFS a cui desideri aggiungere un utente.

3. Scegli Aggiungi utente per visualizzare la pagina Aggiungi utente.
4. Nella sezione Configurazione utente, utilizza le seguenti impostazioni.

   a. Il nome utente deve contenere un minimo di 3 e un massimo di 100 caratteri. È possibile utilizzare i seguenti caratteri nel nome utente: a—z, A-Z, 0—9, trattino basso '_', trattino '-', punto ' . ', e al segno «@». Il nome utente non può iniziare con un trattino '-', punto ' . ', o al segno «@».

   b. Per ID utente e ID gruppo, tieni presente quanto segue:

      - Per il primo utente che crei, ti consigliamo di inserire un valore sia **`0`** per l'ID del gruppo che per l'ID utente. Ciò concede all'utente i privilegi di amministratore per Amazon EFS.
      - Per utenti aggiuntivi, inserisci l'ID utente POSIX e l'ID del gruppo dell'utente. Questi ID vengono utilizzati per tutte le operazioni di Amazon Elastic File System eseguite dall'utente.
      - Per ID utente e ID gruppo, non utilizzare zeri iniziali. Ad esempio, **`12345`** è accettabile, non lo **`012345`** è.

   c. (Facoltativo) Per gli ID di gruppo secondari, inserite uno o più ID di gruppo POSIX aggiuntivi per ogni utente, separati da virgole.

   d. Per Access, scegli il ruolo IAM che:

      - Fornisce all'utente l'accesso solo alle risorse Amazon EFS (file system) a cui desideri che acceda.
      - Definisce quali operazioni sul file system l'utente può e non può eseguire.

      Ti consigliamo di utilizzare il ruolo IAM per la selezione del file system Amazon EFS con accesso al montaggio e autorizzazioni di lettura/scrittura. Ad esempio, la combinazione delle seguenti due politiche AWS gestite, sebbene piuttosto permissiva, concede le autorizzazioni necessarie all'utente:

      - AmazonElasticFileSystemClientFullAccess
      - AWSTransferConsoleFullAccess

      Per ulteriori informazioni, consulta il post di blog dedicato al AWS Transfer Familysupporto per Amazon Elastic File System.

   e. Per la directory Home, procedi come segue:

- Scegli il file system Amazon EFS che desideri utilizzare per archiviare i dati da trasferireAWS Transfer Family.
- Decidi se impostare la home directory su Restricted. L'impostazione della home directory su Restricted ha i seguenti effetti:
  - Gli utenti di Amazon EFS non possono accedere a file o directory al di fuori di quella cartella.
  - Gli utenti di Amazon EFS non possono vedere il nome del file system Amazon EFS (fs-xxxxxxx).

  > **Note**
  >
  > Quando selezioni l'opzione Restricted, i collegamenti simbolici non si risolvono per gli utenti di Amazon EFS.

- (Facoltativo) Inserisci il percorso della home directory in cui desideri che si trovino gli utenti quando accedono utilizzando il loro client.

  Se non si specifica una directory home, viene utilizzata la directory principale del file system Amazon EFS. In questo caso, assicurati che il tuo ruolo IAM fornisca l'accesso a questa directory principale.

5. Per la chiave pubblica SSH, inserisci la parte della chiave SSH pubblica della coppia di chiavi SSH.

   La chiave viene convalidata dal servizio prima di aggiungere il nuovo utente.

   > **Note**
   >
   > Per istruzioni su come generare una coppia di chiavi SSH, consulta Genera chiavi SSH per gli utenti gestiti dal servizio.

6. (Facoltativo) Immettete i tag per l'utente. Per Chiave e Valore, inserite uno o più tag come coppie chiave-valore e scegliete Aggiungi tag.
7. Scegliere Add (Aggiungi) per aggiungere il nuovo utente al server scelto.

   Il nuovo utente viene visualizzato nella sezione Utenti della pagina dei dettagli del server.

Problemi che potresti riscontrare quando esegui per la prima volta un SFTP sul tuo server Transfer Family:

- Se si esegue il `sftp` comando e il prompt non viene visualizzato, è possibile che venga visualizzato il seguente messaggio:

  ```
  Couldn't canonicalize: Permission denied

  Need cwd
  ```

  In questo caso, è necessario aumentare le autorizzazioni relative alle policy per il ruolo dell'utente. È possibile aggiungere una politica AWS gestita, ad esempio`AmazonElasticFileSystemClientFullAccess`.
- Se si immette pwd al `sftp` prompt di visualizzare la home directory dell'utente, è possibile che venga visualizzato il seguente messaggio, in cui *`USER-HOME-DIRECTORY è la home directory dell'utente`* SFTP:

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

  In questo caso, dovreste essere in grado di accedere alla directory principale (`cd ..`) e creare la home directory dell'utente (). `mkdir` *`username`*

Passaggi successivi: per il passaggio successivo, continua conTrasferimento di file su un endpoint server utilizzando un client.

Gestione degli utenti gestiti dal servizio

In questa sezione, puoi trovare informazioni su come visualizzare un elenco di utenti, come modificare i dettagli degli utenti e come aggiungere una chiave pubblica SSH.

- Visualizza un elenco di utenti
- Visualizza o modifica i dettagli dell'utente
- Eliminazione di un utente
- Aggiungi la chiave pubblica SSH
- Elimina la chiave pubblica SSH

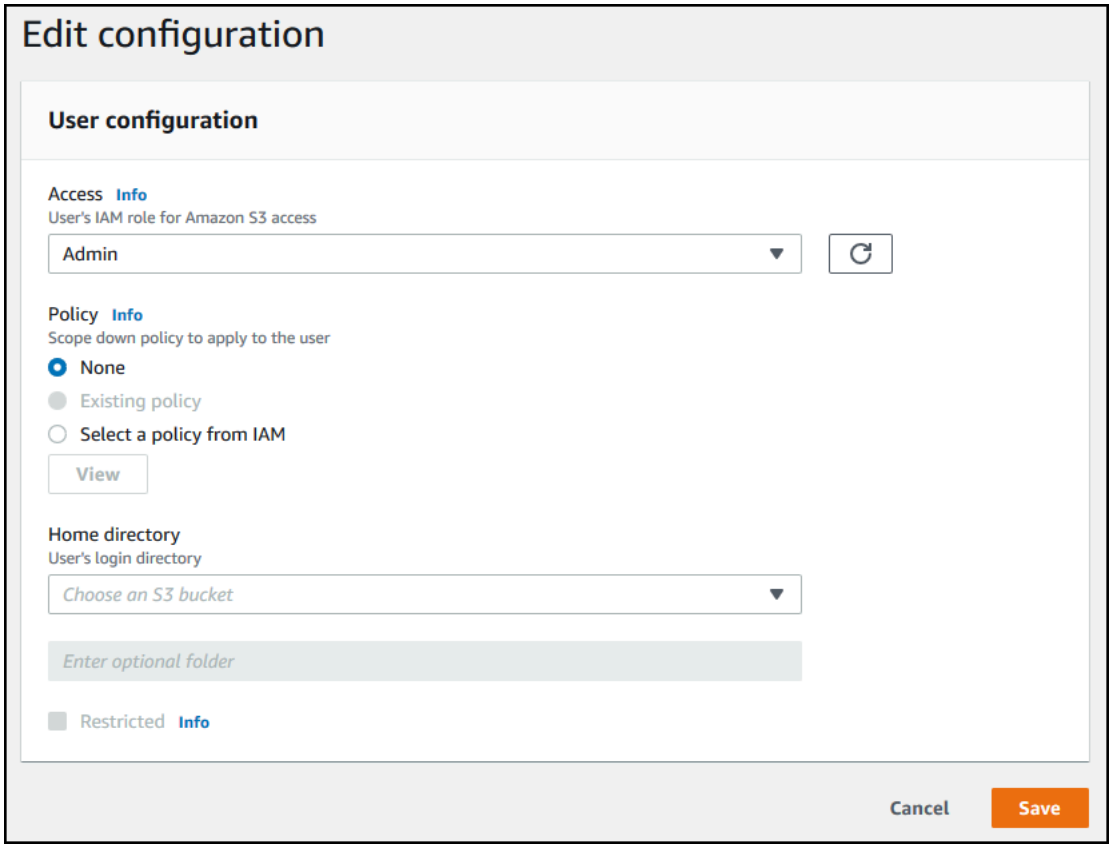
Per trovare un elenco dei tuoi utenti

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Seleziona Server dal pannello di navigazione per visualizzare la pagina Server.
3. Scegli l'identificatore nella colonna Server ID per visualizzare la pagina dei dettagli del server.
4. In Utenti, visualizza un elenco di utenti.

Per visualizzare o modificare i dettagli dell'utente

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Seleziona Server dal pannello di navigazione per visualizzare la pagina Server.
3. Scegli l'identificatore nella colonna Server ID per visualizzare la pagina dei dettagli del server.
4. In Utenti, scegli un nome utente per visualizzare la pagina dei dettagli dell'utente.

   Puoi modificare le proprietà dell'utente in questa pagina scegliendo Modifica.
5. Nella pagina dei dettagli degli utenti, scegli Modifica accanto a Configurazione utente.



6. Nella pagina Modifica configurazione, per Access, scegli il ruolo IAM creato in precedenza che fornisce l'accesso al tuo bucket Amazon S3.

Questo ruolo IAM è stato creato utilizzando la procedura in Crea un ruolo e una policy IAM. Tale ruolo IAM include una policy IAM che fornisce l'accesso al tuo bucket Amazon S3. Include inoltre una relazione di trust con il servizio AWS Transfer Family, definito in un'altra policy IAM.

7. (Facoltativo) Per Policy, scegli una delle seguenti opzioni:

   - Nessuno
   - Politica esistente
   - Seleziona una policy da IAM per scegliere una policy esistente. Scegli Visualizza per vedere un oggetto JSON contenente i dettagli della policy.

   Per ulteriori informazioni sulle politiche di sessione, consultaCrea un ruolo e una policy IAM. Per ulteriori informazioni sulla creazione di una politica di sessione, consultaCreazione di una politica di sessione per un bucket Amazon S3.

8. Per la directory Home, scegli il bucket Amazon S3 in cui archiviare i dati da trasferire. AWS Transfer Family Inserisci il percorso della home directory in cui l'utente atterra quando accede utilizzando il suo client.

   Se lasci vuoto questo parametro, viene utilizzata la `root` directory del tuo bucket Amazon S3. In questo caso, assicurarsi che il ruolo IAM fornisca l'accesso a questa directory `root`.

   > **Note**
   >
   > Ti consigliamo di scegliere un percorso di directory che contenga il nome utente dell'utente, che ti consenta di utilizzare in modo efficace una politica di sessione. La policy di sessione limita l'accesso degli utenti nel bucket Amazon S3 alla directory di quell'utente. home

9. (Facoltativo) Per Restricted, seleziona la casella di controllo in modo che i tuoi utenti non possano accedere a nulla al di fuori di quella cartella e non possano vedere il bucket o il nome della cartella Amazon S3.

> **Note**
>
> Quando si assegna all'utente una home directory e si limita l'utente a tale directory, ciò dovrebbe essere sufficiente per bloccare l'accesso dell'utente alla cartella designata. Utilizza una politica di sessione quando devi applicare ulteriori controlli.

10. Scegliere Salva per salvare le modifiche.

Per eliminare un utente

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Seleziona Server dal pannello di navigazione per visualizzare la pagina Server.
3. Scegli l'identificatore nella colonna Server ID per visualizzare la pagina dei dettagli del server.
4. In Utenti, scegli un nome utente per visualizzare la pagina dei dettagli dell'utente.
5. Nella pagina dei dettagli degli utenti, scegli Elimina a destra del nome utente.
6. Nella finestra di dialogo di conferma che appare, inserisci la parola**`delete`**, quindi scegli Elimina per confermare che desideri eliminare l'utente.

L'utente viene eliminato dall'elenco degli utenti.

Per aggiungere una chiave pubblica SSH per un utente

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione, selezionare Servers (Server).
3. Scegli l'identificatore nella colonna Server ID per visualizzare la pagina dei dettagli del server.
4. In Utenti, scegli un nome utente per visualizzare la pagina dei dettagli dell'utente.
5. Scegliere Add SSH public key (Aggiungi chiave pubblica SSH) per aggiungere una nuova chiave pubblica SSH a un utente.

> **Note**
>
> Le chiavi SSH vengono utilizzate solo dai server abilitati per il protocollo SFTP (Secure Shell) (SSH). Per informazioni su come generare una coppia di chiavi SSH, vedereGenera chiavi SSH per gli utenti gestiti dal servizio.

6. Per SSH public key (Chiave pubblica SSH), immettere la parte di chiave pubblica SSH della coppia di chiavi SSH.

   La chiave viene convalidata dal servizio prima di aggiungere il nuovo utente. Il formato della chiave SSH è `ssh-rsa` *`string`*. Per generare una coppia di chiavi SSH, vedereGenera chiavi SSH per gli utenti gestiti dal servizio.
7. Scegliere Add key (Aggiungi chiave).

Per eliminare una chiave pubblica SSH per un utente

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione, selezionare Servers (Server).
3. Scegli l'identificatore nella colonna Server ID per visualizzare la pagina dei dettagli del server.
4. In Utenti, scegli un nome utente per visualizzare la pagina dei dettagli dell'utente.
5. Per eliminare una chiave pubblica, seleziona la casella di controllo della relativa chiave SSH e scegli Elimina.

Utilizzo del provider di identità AWS Directory Service

Questo argomento descrive come utilizzare il provider di identità del AWS Directory Service per AWS Transfer Family.

Argomenti

- Usando AWS Directory Service for Microsoft Active Directory
- Usare AWS Directory Service per Azure Active Directory Domain Services

Usando AWS Directory Service for Microsoft Active Directory

È possibile utilizzare AWS Transfer Family per autenticare gli utenti finali di trasferimento di file utilizzando AWS Directory Service for Microsoft Active Directory. Consente la migrazione senza interruzioni dei flussi di lavoro di trasferimento di file che si basano sull'autenticazione di Active Directory senza modificare le credenziali degli utenti finali o richiedere un'autorizzazione personalizzata.

Con AWS Managed Microsoft AD, puoi fornire a AWS Directory Service utenti e gruppi l'accesso sicuro tramite SFTP, FTPS e FTP ai dati archiviati in Amazon Simple Storage Service (Amazon S3)

o Amazon Elastic File System (Amazon EFS). Se utilizzi Active Directory per archiviare le credenziali degli utenti, ora disponi di un modo più semplice per abilitare i trasferimenti di file per questi utenti.

Puoi fornire l'accesso ai gruppi di Active Directory AWS Managed Microsoft AD nel tuo ambiente locale o nel AWS cloud utilizzando i connettori Active Directory. Puoi consentire agli utenti già configurati nel tuo ambiente Microsoft Windows, nel AWS cloud o nella loro rete locale, l'accesso a un AWS Transfer Family server che utilizza AWS Managed Microsoft AD l'identità.

> **Note**
>
> - AWS Transfer Family non supporta Simple AD.
> - Transfer Family non supporta configurazioni Active Directory interregionali: supportiamo solo le integrazioni di Active Directory che si trovano nella stessa regione di quella del server Transfer Family.
> - Transfer Family non supporta l'utilizzo né di AD AWS Managed Microsoft AD Connector per abilitare l'autenticazione a più fattori (MFA) per l'infrastruttura MFA esistente basata su RADIUS.
> - AWS Transfer Family non supporta le regioni replicate di Managed Active Directory.

Per utilizzarlo AWS Managed Microsoft AD, è necessario eseguire le seguenti operazioni:

1. Crea una o più AWS Managed Microsoft AD directory utilizzando la AWS Directory Service console.
2. Usa la console Transfer Family per creare un server che utilizzi AWS Managed Microsoft AD come provider di identità.
3. Aggiungi l'accesso da uno o più dei tuoi AWS Directory Service gruppi.
4. Sebbene non sia obbligatorio, ti consigliamo di testare e verificare l'accesso degli utenti.

Argomenti

- Test degli utenti
- Eliminazione dell'accesso al server per un gruppo
- Connessione al server tramite SSH (Secure Shell)
- Connessione AWS Transfer Family a un Active Directory autogestito utilizzando foreste e trust

Prima di iniziare a utilizzare AWS Directory Service for Microsoft Active Directory

Fornisci un identificatore univoco per i tuoi gruppi di annunci

Prima di poter utilizzare AWS Managed Microsoft AD, è necessario fornire un identificatore univoco per ogni gruppo nella directory Microsoft AD. A tale scopo, è possibile utilizzare l'identificatore di sicurezza (SID) per ogni gruppo. Gli utenti del gruppo che associ hanno accesso alle tue risorse Amazon S3 o Amazon EFS tramite i protocolli abilitati utilizzando AWS Transfer Family.

Usa il seguente PowerShell comando di Windows per recuperare il SID di un gruppo, sostituendolo *YourGroupName* con il nome del gruppo.

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

> **Note**
>
> Se lo utilizzi AWS Directory Service come provider di identità `userPrincipalName` e `SamAccountName` hai valori diversi, AWS Transfer Family accetta il valore in. `SamAccountName` Transfer Family non accetta il valore specificato in`userPrincipalName`.

Aggiungi AWS Directory Service autorizzazioni al tuo ruolo

Ti servono anche le autorizzazioni AWS Directory Service API da utilizzare AWS Directory Service come provider di identità. Le seguenti autorizzazioni sono obbligatorie o suggerite:

- `ds:DescribeDirectories`è necessario per consentire a Transfer Family di cercare l'elenco
- `ds:AuthorizeApplication`è necessario aggiungere l'autorizzazione per Transfer Family
- `ds:UnauthorizeApplication`si consiglia di rimuovere tutte le risorse create provvisoriamente, nel caso in cui qualcosa vada storto durante il processo di creazione del server

Aggiungi queste autorizzazioni al ruolo che stai utilizzando per creare i tuoi server Transfer Family. Per maggiori dettagli su queste autorizzazioni, consulta Autorizzazioni AWS Directory Service API: riferimento alle azioni, alle risorse e alle condizioni.

Utilizzo dei realm di Active Directory

Quando state valutando come fare in modo che gli utenti di Active Directory accedano ai AWS Transfer Family server, tenete presente l'area dell'utente e quella del gruppo. Idealmente, l'area dell'utente e quella del gruppo dovrebbero corrispondere. Cioè, sia l'utente che il gruppo si trovano nel realm predefinito o entrambi si trovano nell'area di fiducia. In caso contrario, l'utente non può essere autenticato da Transfer Family.

Puoi testare l'utente per assicurarti che la configurazione sia corretta. Per informazioni dettagliate, vedi Test degli utenti. Se c'è un problema con il realm utente/gruppo, viene visualizzato l'errore Nessun accesso associato trovato per i gruppi di utenti.

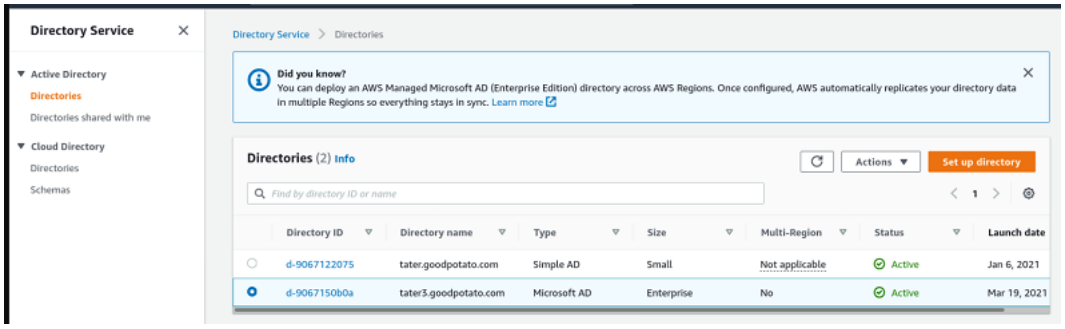
Scelta AWS Managed Microsoft AD come provider di identità

Questa sezione descrive come utilizzarlo AWS Directory Service for Microsoft Active Directory con un server.

Da usare AWS Managed Microsoft AD con Transfer Family

1. Accedi AWS Management Console e apri la AWS Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.

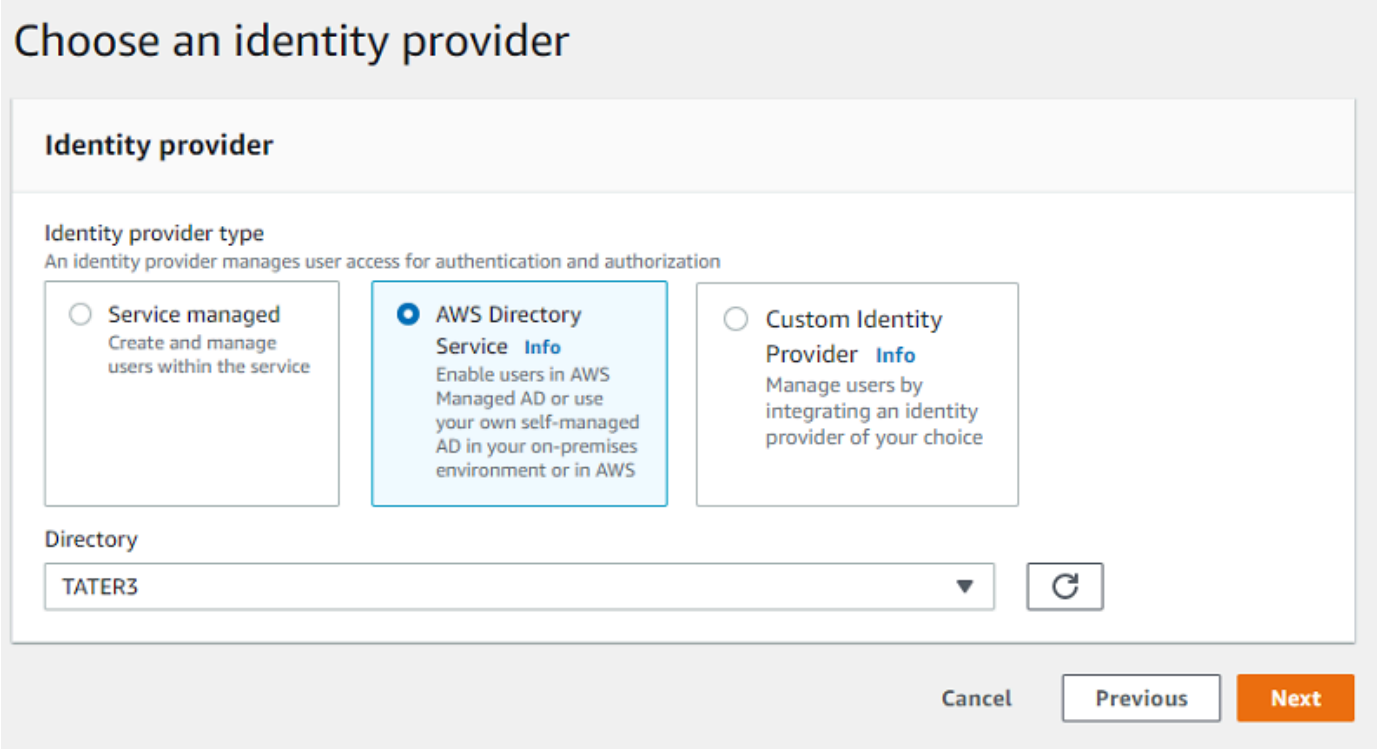
   Usa la AWS Directory Service console per configurare una o più directory gestite. Per ulteriori informazioni, consulta AWS Managed Microsoft AD nella Guida per gli amministratori AWS Directory Service .



2. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/ e scegli Crea server.
3. Nella pagina Scegli i protocolli, scegli uno o più protocolli dall'elenco.

> **Note**
>
> Se si seleziona FTPS, è necessario fornire il AWS Certificate Manager certificato.

4. Per Scegli un provider di identità, scegli AWS Directory Service.



5. L'elenco delle directory contiene tutte le directory gestite che hai configurato. Scegliete una directory dall'elenco e scegliete Avanti.

> **Note**
>
> - Le directory Cross-Account e Shared non sono supportate per. AWS Managed Microsoft AD
> - Per configurare un server con Directory Service come provider di identità, è necessario aggiungere alcune AWS Directory Service autorizzazioni. Per informazioni dettagliate, vedi Prima di iniziare a utilizzare AWS Directory Service for Microsoft Active Directory.

6. Per completare la creazione del server, utilizzare una delle seguenti procedure:

- Crea un server compatibile con SFTP
- Creare un server compatibile con FTPS

- Crea un server abilitato all'FTP

In queste procedure, continua con il passaggio successivo alla scelta di un provider di identità.

> **Important**
>
> Non puoi eliminare una directory Microsoft AD AWS Directory Service se l'hai usata in un server Transfer Family. È necessario prima eliminare il server, quindi è possibile eliminare la directory.

Concessione dell'accesso ai gruppi

Dopo aver creato il server, è necessario scegliere quali gruppi della directory devono avere accesso al caricamento e al download di file tramite AWS Transfer Family i protocolli abilitati. A tale scopo, è necessario creare un accesso.

> **Note**
>
> Gli utenti devono appartenere direttamente al gruppo a cui si concede l'accesso. Ad esempio, supponiamo che Bob sia un utente e appartenga al gruppo A e che lo stesso gruppo A sia incluso nel gruppo B.
>
> - Se concedi l'accesso a GroupA, a Bob viene concesso l'accesso.
> - Se concedi l'accesso a GroupB (e non a GroupA), Bob non ha accesso.

Per concedere l'accesso a un gruppo

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Vai alla pagina dei dettagli del server.
3. Nella sezione Accessi, scegli Aggiungi accesso.
4. Inserisci il SID per la AWS Managed Microsoft AD directory a cui desideri che acceda a questo server.

> **Note**
>
> Per informazioni su come trovare il SID per il gruppo, consulta. the section called “Prima di iniziare a utilizzare AWS Directory Service for Microsoft Active Directory”

5. Per Access, scegli un ruolo AWS Identity and Access Management (IAM) per il gruppo.
6. Nella sezione Politica, scegli una politica. L'impostazione predefinita è Nessuna.
7. Per la directory Home, scegli un bucket S3 che corrisponda alla home directory del gruppo.

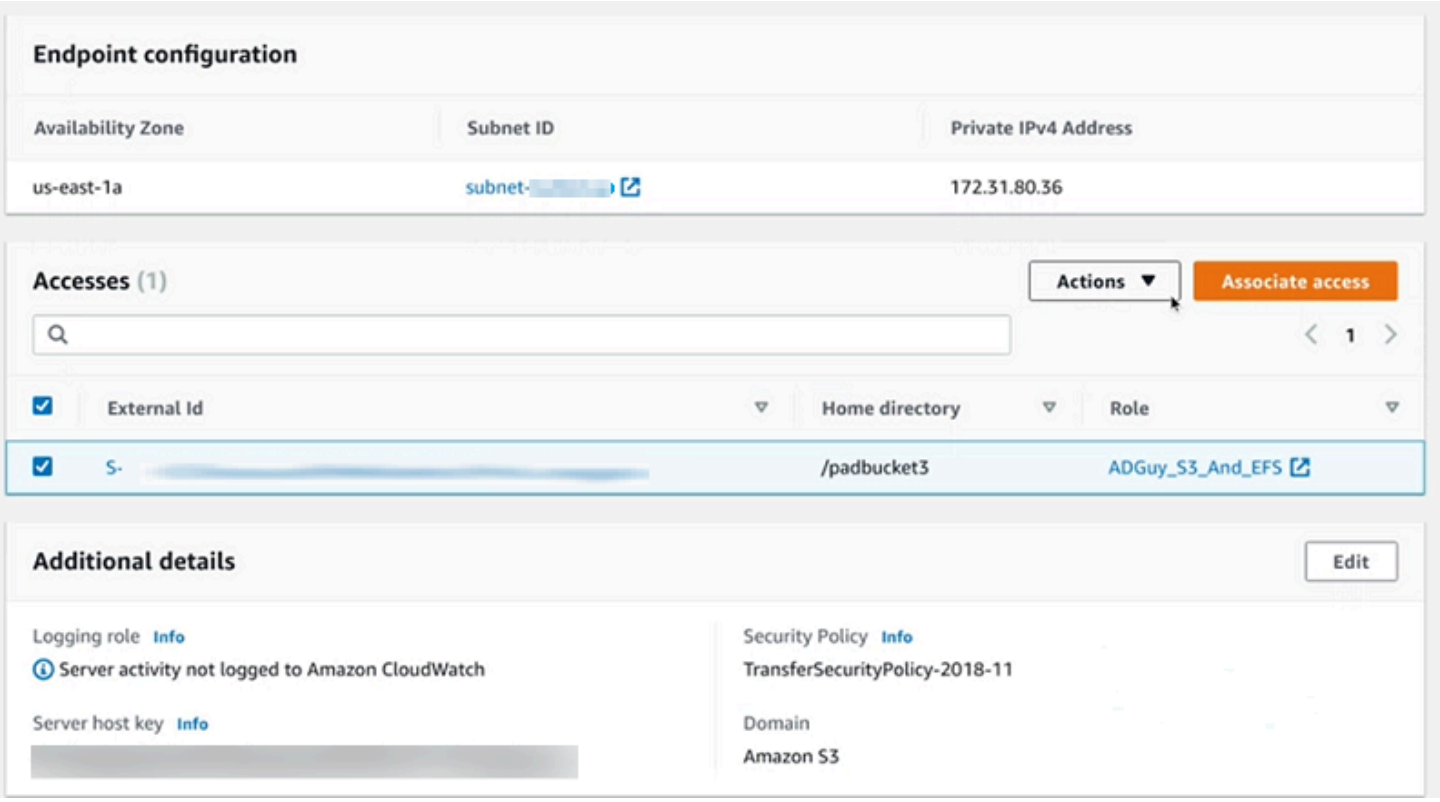
> **Note**
>
> Puoi limitare le porzioni del bucket visualizzate dagli utenti creando una politica di sessione. Ad esempio, per limitare gli utenti alla propria cartella all'interno della `/filetest` directory, inserisci il seguente testo nella casella.
>
> ```
> /filetest/${transfer:UserName}
> ```
>
> Per ulteriori informazioni sulla creazione di una politica di sessione, consultaCreazione di una politica di sessione per un bucket Amazon S3.

8. Scegli Aggiungi per creare l'associazione.
9. Scegli il tuo server.
10. Scegli Aggiungi accesso.
    - Inserisci il SID per il gruppo.

    > **Note**
    >
    > Per informazioni su come trovare il SID, vedere. the section called “Prima di iniziare a utilizzare AWS Directory Service for Microsoft Active Directory”

11. Scegli Aggiungi accesso.

Nella sezione Accessi, sono elencati gli accessi per il server.



Test degli utenti

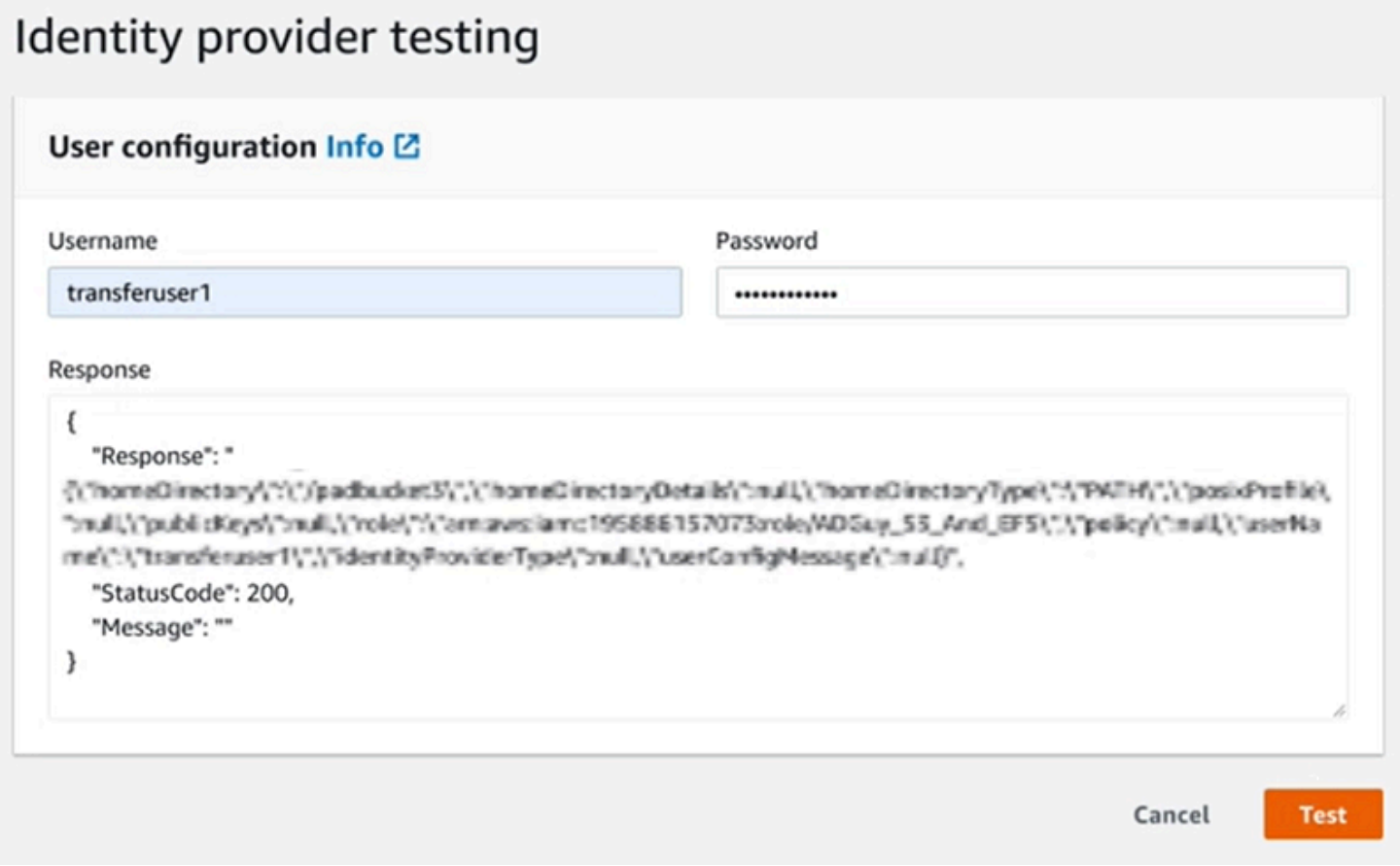
Puoi verificare se un utente ha accesso alla AWS Managed Microsoft AD directory del tuo server.

> **Note**
>
> Un utente deve appartenere esattamente a un gruppo (un ID esterno) elencato nella sezione Accesso della pagina di configurazione dell'endpoint. Se l'utente non fa parte di alcun gruppo o fa parte di più di un singolo gruppo, a quell'utente non viene concesso l'accesso.

Per verificare se un utente specifico ha accesso

1. Nella pagina dei dettagli del server, scegli Azioni, quindi scegli Test.
2. Per il test del provider di identità, inserisci le credenziali di accesso per un utente che fa parte di uno dei gruppi con accesso.
3. Scegli Test (Esegui test).

Viene visualizzato un test del provider di identità riuscito, che dimostra che all'utente selezionato è stato concesso l'accesso al server.



Se l'utente appartiene a più di un gruppo con accesso, riceverai la seguente risposta.

```
"Response":"",
"StatusCode":200,
"Message":"More than one associated access found for user's groups."
```

Eliminazione dell'accesso al server per un gruppo

Per eliminare l'accesso al server per un gruppo

1. Nella pagina dei dettagli del server, scegli Azioni, quindi scegli Elimina accesso.
2. Nella finestra di dialogo, conferma che desideri rimuovere l'accesso per questo gruppo.

Quando si torna alla pagina dei dettagli del server, si nota che l'accesso per questo gruppo non è più elencato.

Connessione al server tramite SSH (Secure Shell)

Dopo aver configurato il server e gli utenti, è possibile connettersi al server tramite SSH e utilizzare il nome utente completo per un utente che ha accesso.

```
sftp user@active-directory-domain@vpc-endpoint
```

Ad esempio: `transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-svc-987654zyxabc.us-east-1.vpce.amazonaws.com`.

Questo formato è destinato alla ricerca della federazione, limitando la ricerca di un Active Directory potenzialmente grande.

> **Note**
>
> È possibile specificare il nome utente semplice. Tuttavia, in questo caso, il codice di Active Directory deve cercare in tutte le directory della federazione. Ciò potrebbe limitare la ricerca e l'autenticazione potrebbe non riuscire anche se l'utente dovesse avere accesso.

Dopo l'autenticazione, l'utente si trova nella home directory specificata al momento della configurazione dell'utente.

Connessione AWS Transfer Family a un Active Directory autogestito utilizzando foreste e trust

Gli utenti dell'Active Directory (AD) autogestito possono utilizzare anche l'accesso Single Sign-On AWS IAM Identity Center ai server Transfer Family e ai server Transfer Account AWS Family. A tale scopo, sono disponibili AWS Directory Service le seguenti opzioni:

- L'attendibilità unidirezionale delle foreste (in uscita AWS Managed Microsoft AD e in entrata per Active Directory locale) funziona solo per il dominio radice.
- Per i domini secondari, puoi utilizzare uno dei seguenti:
  - Utilizza l'attendibilità bidirezionale tra Active Directory locale AWS Managed Microsoft AD e viceversa
  - Utilizza la fiducia esterna unidirezionale per ogni dominio figlio.

Quando si connette al server utilizzando un dominio affidabile, l'utente deve specificare il dominio affidabile, ad esempio`transferuserexample@mycompany.com`.

Usare AWS Directory Service per Azure Active Directory Domain Services

- Per sfruttare la foresta di Active Directory esistente per le tue esigenze di trasferimento SFTP, puoi usare Active Directory Connector.
- Se desideri i vantaggi di Active Directory e l'elevata disponibilità in un servizio completamente gestito, puoi utilizzare AWS Directory Service for Microsoft Active Directory. Per informazioni dettagliate, vedi Utilizzo del provider di identità AWS Directory Service.

Questo argomento descrive come usare un connettore Active Directory e Azure Active Directory Domain Services (Azure ADDS) per autenticare gli utenti di SFTP Transfer con Azure Active Directory.

Argomenti

Prima di iniziare a usare AWS Directory Service per Azure Active Directory Domain Services

Perché AWS, è necessario quanto segue:

- Un cloud privato virtuale (VPC) in una AWS regione in cui utilizzi i server Transfer Family
- Almeno due sottoreti private nel tuo VPC
- Il VPC deve disporre di connettività Internet
- Un gateway per i clienti e un gateway privato virtuale per la connessione site-to-site VPN con Microsoft Azure

Per Microsoft Azure, è necessario quanto segue:

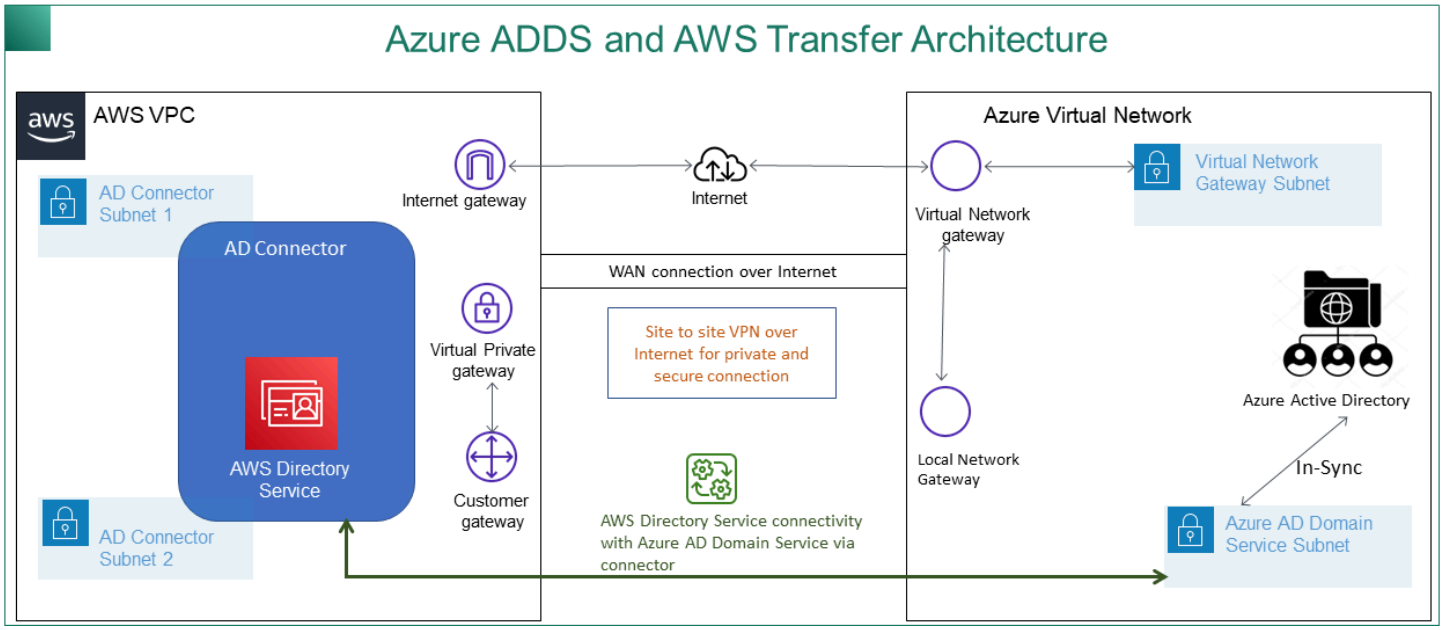
- Un servizio di dominio Azure Active Directory e Active Directory (Azure ADDS)
- Un gruppo di risorse di Azure

- Una rete virtuale di Azure
- Connettività VPN tra Amazon VPC e il tuo gruppo di risorse Azure

> **Note**
>
> Ciò può avvenire tramite tunnel IPSEC nativi o utilizzando dispositivi VPN. In questo argomento, utilizziamo i tunnel IPSEC tra un gateway di rete virtuale di Azure e un gateway di rete locale. I tunnel devono essere configurati per consentire il traffico tra gli endpoint di Azure ADDS e le sottoreti che ospitano il tuo VPC. AWS

- Un gateway per i clienti e un gateway privato virtuale per la connessione site-to-site VPN con Microsoft Azure

Il diagramma seguente mostra la configurazione necessaria prima di iniziare.

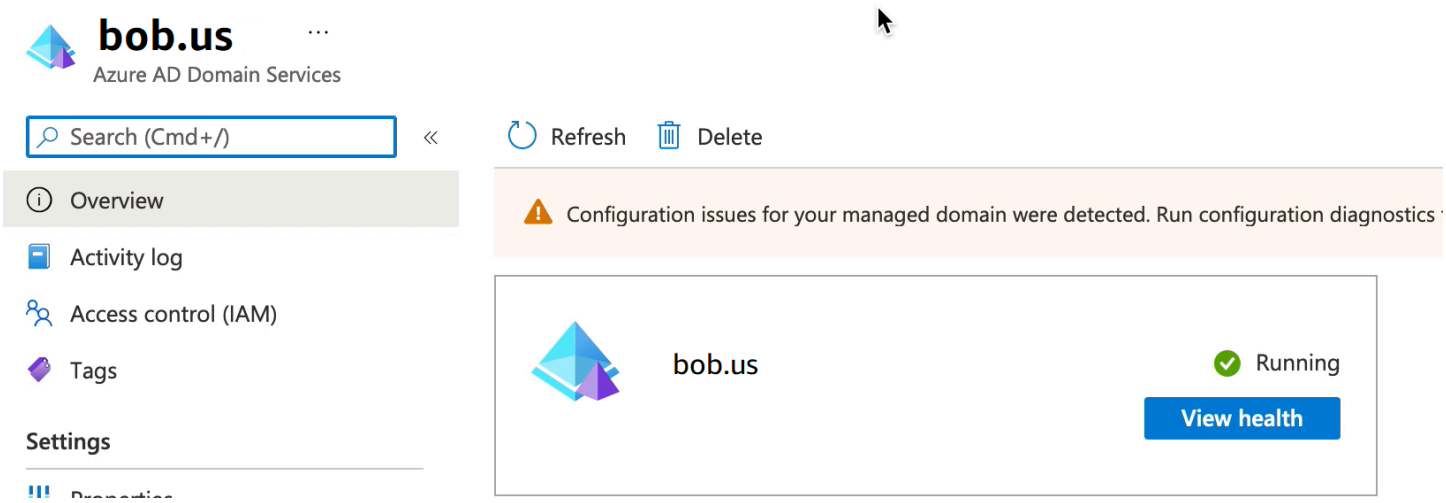


Fase 1: Aggiungere Azure Active Directory Domain Services

Azure AD non supporta le istanze di aggiunta al dominio per impostazione predefinita. Per eseguire azioni come Domain Join e usare strumenti come Group Policy, gli amministratori devono abilitare Azure Active Directory Domain Services. Se non hai già aggiunto Azure AD DS o l'implementazione esistente non è associata al dominio che desideri venga utilizzato dal server di trasferimento SFTP, devi aggiungere una nuova istanza.

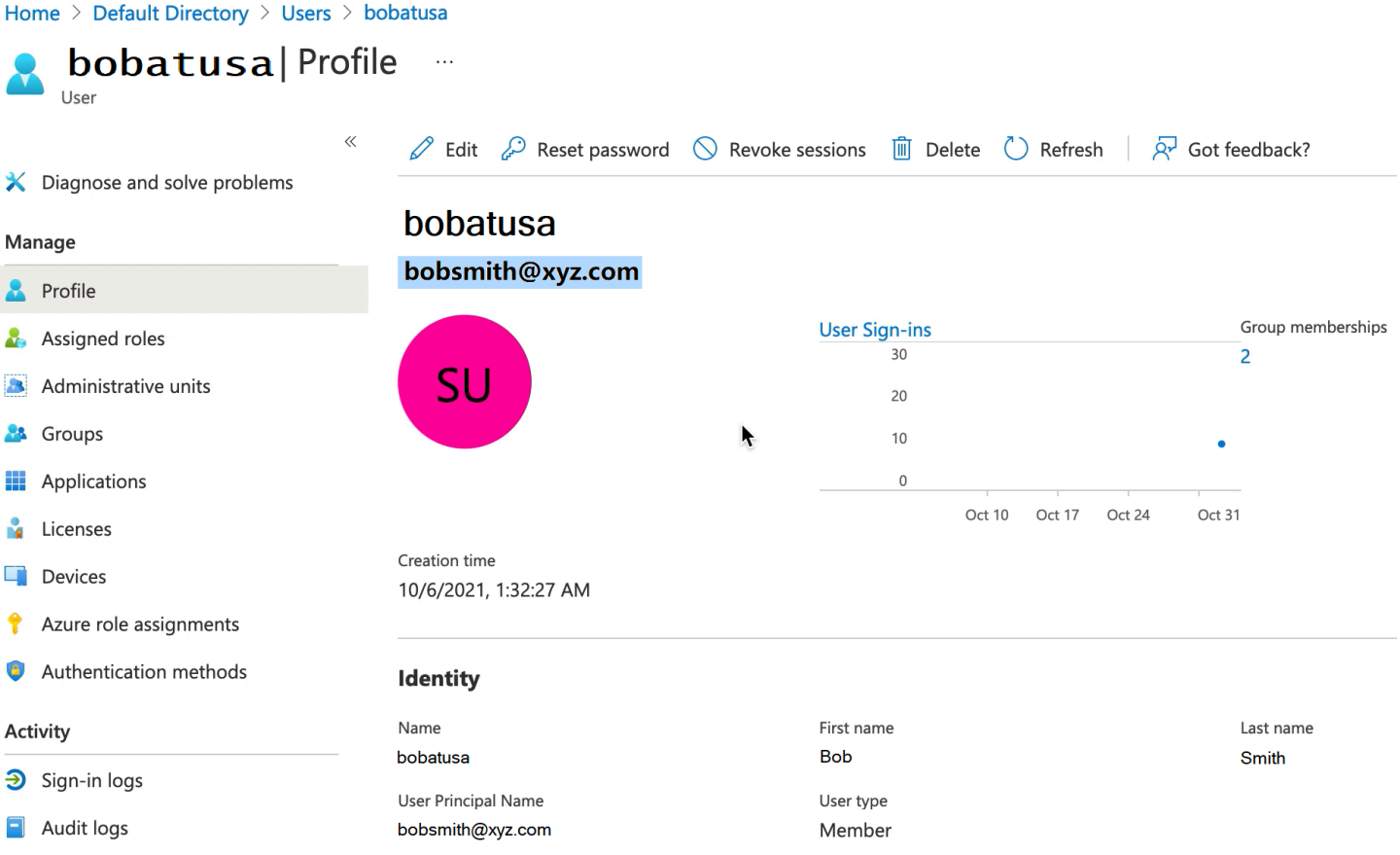
Per informazioni sull'abilitazione di Azure Active Directory Domain Services (Azure ADDS), vedi Tutorial: Creare e configurare un dominio gestito di Azure Active Directory Domain Services.

> **Note**
>
> Quando abiliti Azure ADDS, assicurati che sia configurato per il gruppo di risorse e il dominio Azure AD a cui stai connettendo il tuo server di trasferimento SFTP.



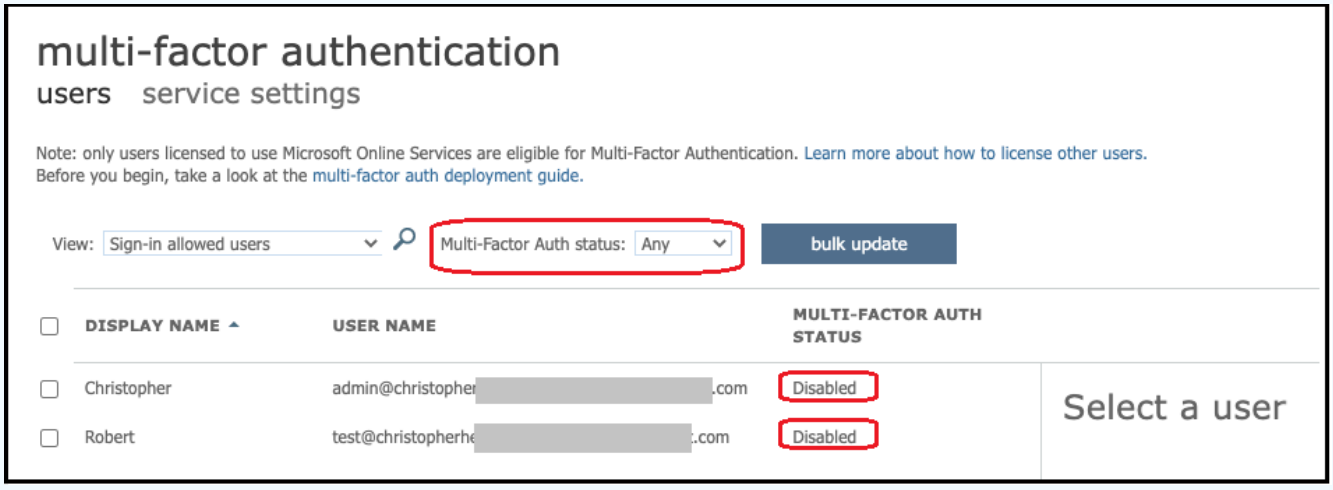
Passaggio 2: creazione di un account di servizio

Azure AD deve avere un account di servizio che faccia parte di un gruppo di amministratori in Azure ADDS. Questo account viene utilizzato con il connettore AWS Active Directory. Assicurati che questo account sia sincronizzato con Azure ADDS.



Tip

L'autenticazione a più fattori per Azure Active Directory non è supportata per i server Transfer Family che usano il protocollo SFTP. Il server Transfer Family non può fornire il token MFA dopo che un utente si è autenticato su SFTP. Assicurati di disabilitare l'MFA prima di provare a connetterti.



Fase 3: Configurazione della AWS directory tramite AD Connector

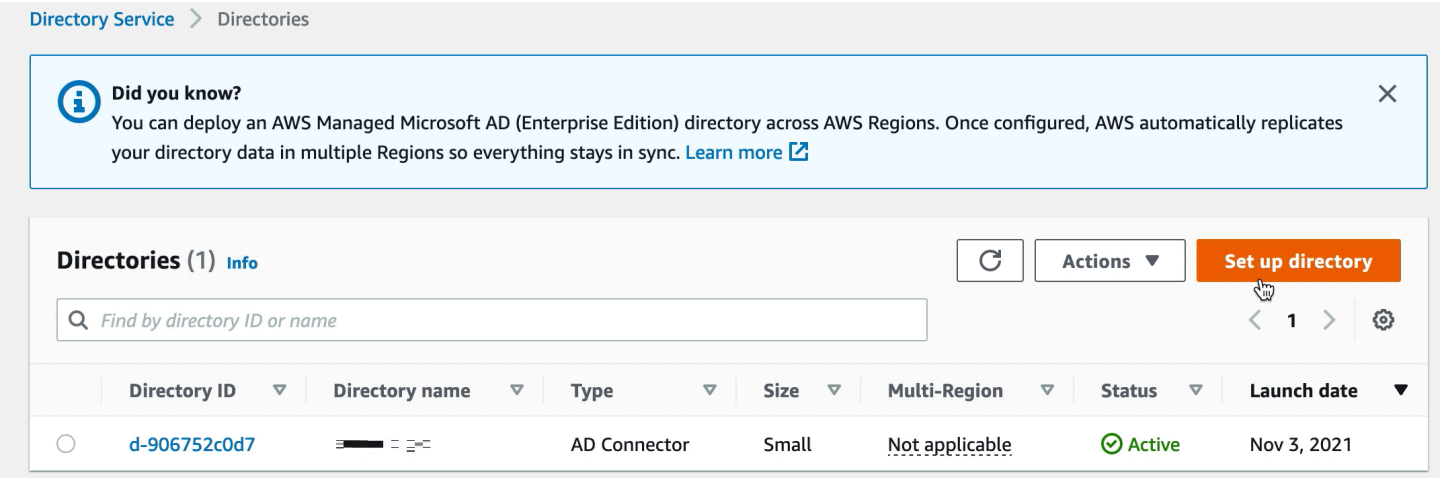
Dopo aver configurato Azure ADDS e creato un account di servizio con tunnel VPN IPSEC tra il tuo AWS VPC e la rete virtuale di Azure, puoi testare la connettività eseguendo il ping dell'indirizzo IP DNS di Azure ADDS da qualsiasi istanza EC2. AWS

Dopo aver verificato che la connessione sia attiva, puoi continuare di seguito.

Per configurare la tua AWS directory utilizzando AD Connector

1. Apri la console Directory Service e seleziona Directory.
2. Seleziona Configura la directory.
3. Per il tipo di directory, scegli AD Connector.
4. Seleziona la dimensione della directory, seleziona Avanti, quindi seleziona il tuo VPC e le sottoreti.
5. Seleziona Avanti, quindi compila i campi come segue:
   - Nome DNS della directory: inserisci il nome di dominio che stai usando per Azure ADDS.
   - Indirizzi IP DNS: inserisci gli indirizzi IP di Azure ADDS.
   - Nome utente e password dell'account del server: inserisci i dettagli per l'account di servizio che hai creato nel Passaggio 2: Crea un account di servizio.
6. Completa le schermate per creare il servizio di directory.

Ora lo stato della directory dovrebbe essere Attivo ed è pronto per essere utilizzato con un server di trasferimento SFTP.



Fase 4: Configurazione AWS Transfer Family del server

Crea un server Transfer Family con il protocollo SFTP e il tipo di provider di identità AWS Directory Service. Dall'elenco a discesa Directory, seleziona la directory che hai aggiunto nel Passaggio 3: Configurazione della AWS directory utilizzando AD Connector.

> **Note**
>
> Non puoi eliminare una directory Microsoft AD in AWS Directory Service se l'hai usata in un server Transfer Family. È necessario prima eliminare il server, quindi è possibile eliminare la directory.

Fase 5: Concessione dell'accesso ai gruppi

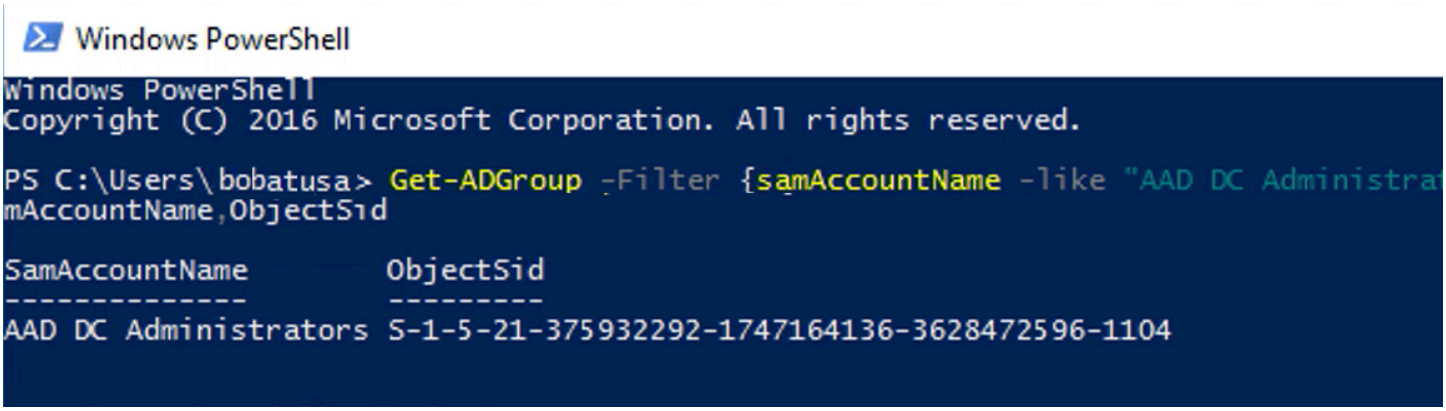
Dopo aver creato il server, è necessario scegliere quali gruppi della directory devono avere accesso al caricamento e al download di file tramite AWS Transfer Family i protocolli abilitati. A tale scopo, è necessario creare un accesso.

> **Note**
>
> Gli utenti devono appartenere direttamente al gruppo a cui si concede l'accesso. Ad esempio, supponiamo che Bob sia un utente e appartenga al gruppo A e che lo stesso gruppo A sia incluso nel gruppo B.
>
> - Se concedi l'accesso a GroupA, a Bob viene concesso l'accesso.
> - Se concedi l'accesso a GroupB (e non a GroupA), Bob non ha accesso.

Per concedere l'accesso è necessario recuperare il SID del gruppo.

Utilizzate il seguente PowerShell comando di Windows per recuperare il SID di un gruppo, sostituendolo *YourGroupName*con il nome del gruppo.

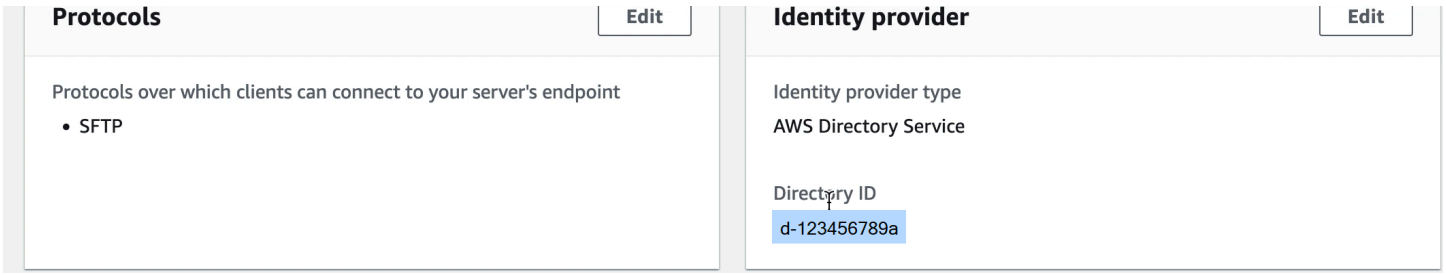
```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select
 SamAccountName,ObjectSid
```

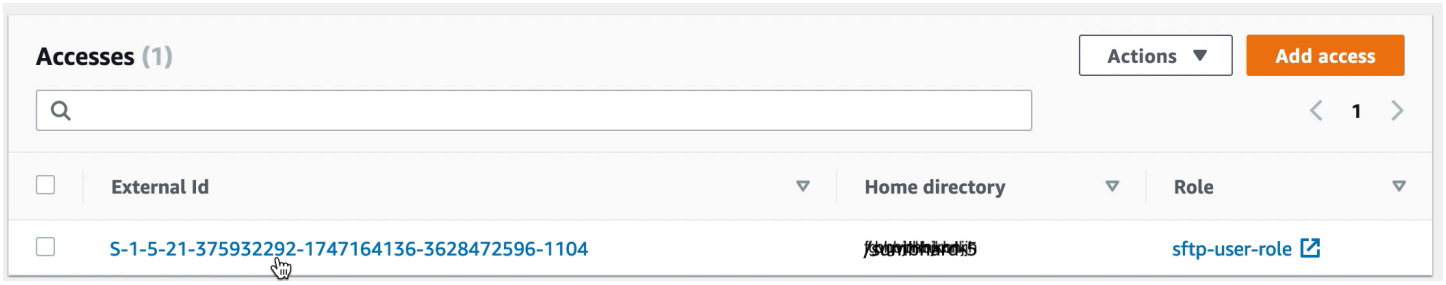


Concedi l'accesso ai gruppi

1. Apri https://console.aws.amazon.com/transfer/.
2. Vai alla pagina dei dettagli del server e nella sezione Accessi, scegli Aggiungi accesso.
3. Inserisci il SID ricevuto dall'output della procedura precedente.
4. Per Access, scegli un AWS Identity and Access Management ruolo per il gruppo.
5. Nella sezione Politica, scegli una politica. Il valore predefinito è None (Nessuna).
6. Per la home directory, scegli un bucket S3 che corrisponda alla home directory del gruppo.
7. Scegli Aggiungi per creare l'associazione.

I dettagli del server di trasferimento dovrebbero essere simili ai seguenti:





Fase 6: Test degli utenti

Puoi verificare (Test degli utenti) se un utente ha accesso alla AWS Managed Microsoft AD directory del tuo server. Un utente deve appartenere esattamente a un gruppo (un ID esterno) elencato nella sezione Accesso della pagina di configurazione dell'endpoint. Se l'utente non fa parte di alcun gruppo o fa parte di più di un singolo gruppo, a quell'utente non viene concesso l'accesso.

Lavorare con provider di identità personalizzati

Per autenticare gli utenti, puoi utilizzare il tuo provider di identità esistente con. AWS Transfer Family Integri il tuo provider di identità utilizzando una AWS Lambda funzione che autentica e autorizza gli utenti ad accedere ad Amazon S3 o Amazon Elastic File System (Amazon EFS). Per informazioni dettagliate, vedi Utilizzo AWS Lambda per integrare il proprio provider di identità. Puoi anche accedere a CloudWatch grafici per metriche come il numero di file e byte trasferiti nella Console di AWS Transfer Family gestione, offrendoti un unico pannello di controllo per monitorare i trasferimenti di file utilizzando una dashboard centralizzata.

In alternativa, puoi fornire un'interfaccia RESTful con un unico metodo Amazon API Gateway. Transfer Family utilizza questo metodo per connettersi al tuo provider di identità, che autentica e autorizza gli utenti ad accedere ad Amazon S3 o Amazon EFS. Utilizza questa opzione se hai bisogno di un'API RESTful per integrare il tuo provider di identità o se desideri utilizzarla per sfruttarne le funzionalità per il geo-blocking o AWS WAF le richieste di limitazione della velocità. Per informazioni dettagliate, vedi Utilizzo di Amazon API Gateway per integrare il tuo provider di identità.

In entrambi i casi, puoi creare un nuovo server utilizzando la console o l'operazione API.AWS Transfer FamilyCreateServer

> **Note**
>
> Transfer Family offre un post sul blog e un workshop che ti guidano nella creazione di una soluzione per il trasferimento di file. Questa soluzione sfrutta gli endpoint SFTP/FTPS gestiti e Amazon Cognito e DynamoDB AWS Transfer Family per la gestione degli utenti.
> Il post del blog è disponibile in Utilizzo di Amazon Cognito come provider di identità con AWS Transfer Family Amazon S3. Puoi visualizzare i dettagli del workshop qui.

AWS Transfer Family fornisce le seguenti opzioni per lavorare con provider di identità personalizzati.

- AWS Lambda Utilizzalo per connettere il tuo provider di identità: puoi utilizzare un provider di identità esistente, supportato da una funzione Lambda. Fornisci il nome della funzione Lambda. Per ulteriori informazioni, consulta Utilizzo AWS Lambda per integrare il proprio provider di identità.
- Usa Amazon API Gateway per connettere il tuo provider di identità: puoi creare un metodo API Gateway supportato da una funzione Lambda da utilizzare come provider di identità. Fornisci un URL di Amazon API Gateway e un ruolo di chiamata. Per ulteriori informazioni, consulta Utilizzo di Amazon API Gateway per integrare il tuo provider di identità.

Per entrambe le opzioni, puoi anche specificare come effettuare l'autenticazione.

- Password O chiave: gli utenti possono autenticarsi con la propria password o la propria chiave. Si tratta del valore di default.
- SOLO password: gli utenti devono fornire la propria password per connettersi.
- SOLO chiave: gli utenti devono fornire la propria chiave privata per connettersi.
- Password E chiave: gli utenti devono fornire sia la chiave privata che la password per connettersi. Il server controlla prima la chiave e poi, se la chiave è valida, il sistema richiede una password. Se la chiave privata fornita non corrisponde alla chiave pubblica archiviata, l'autenticazione fallisce.

Utilizzo di più metodi di autenticazione per l'autenticazione con il provider di identità personalizzato

Il server Transfer Family controlla la logica AND quando si utilizzano più metodi di autenticazione. Transfer Family considera queste richieste come due richieste separate al tuo provider di identità personalizzato: tuttavia, il loro effetto è combinato.

Entrambe le richieste devono restituire correttamente la risposta corretta per consentire il completamento dell'autenticazione. Transfer Family richiede che le due risposte siano complete, il che significa che contengono tutti gli elementi richiesti (ruolo, home directory, policy e profilo POSIX se utilizzi Amazon EFS per lo storage). Transfer Family richiede inoltre che la risposta alla password non includa chiavi pubbliche.

La richiesta di chiave pubblica deve avere una risposta separata dal provider di identità. Tale comportamento rimane invariato quando si utilizza Password OR Key o Password AND Key.

Il protocollo SSH/SFTP sfida il client software prima con un'autenticazione a chiave pubblica, quindi richiede un'autenticazione con password. Questa operazione richiede che entrambe abbiano esito positivo prima che l'utente possa completare l'autenticazione.

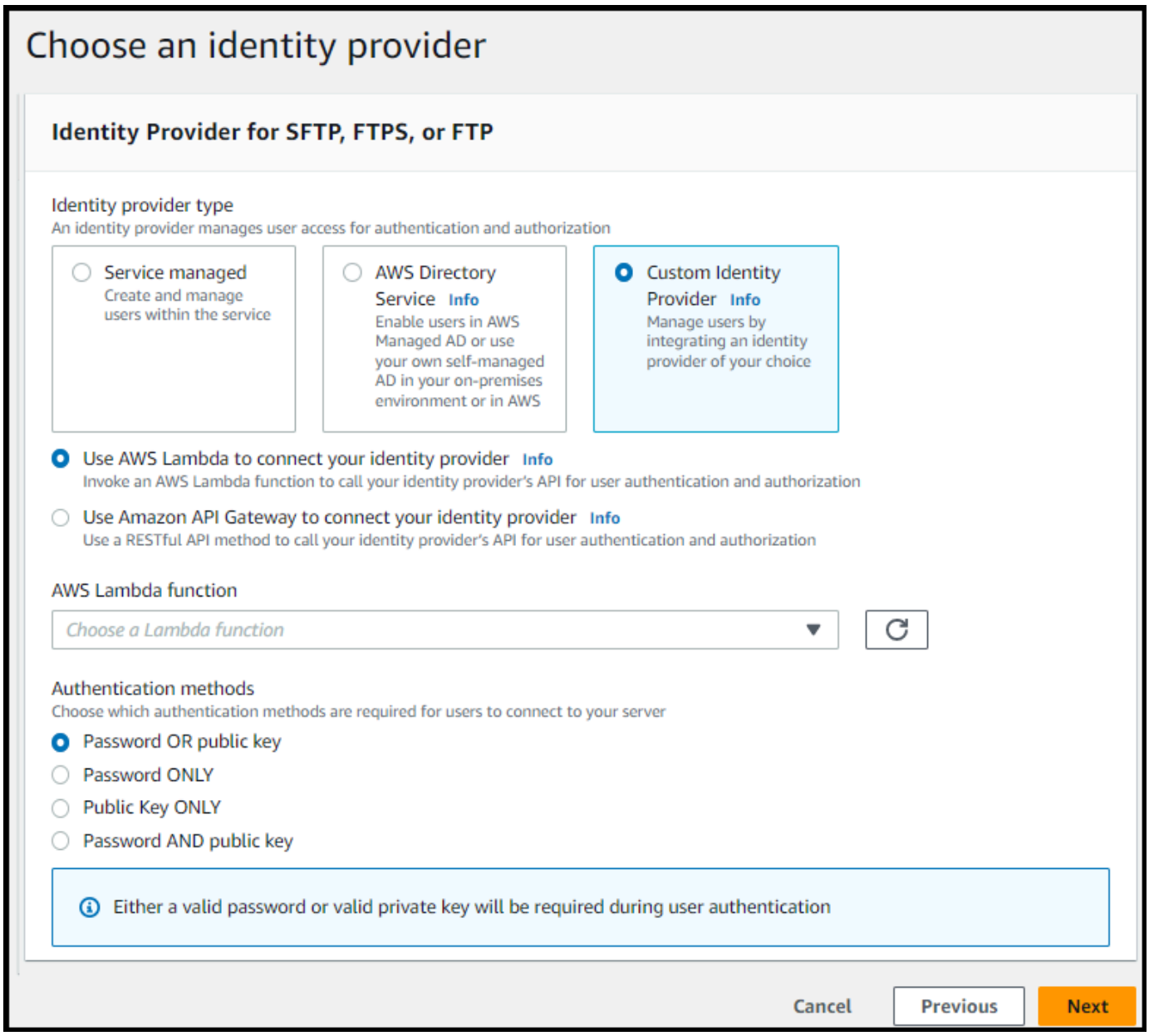
Argomenti

Utilizzo AWS Lambda per integrare il proprio provider di identità

Crea una AWS Lambda funzione che si connetta al tuo provider di identità personalizzato. Puoi utilizzare qualsiasi provider di identità personalizzato, come Okta, Secrets Manager OneLogin, o un data store personalizzato che includa la logica di autorizzazione e autenticazione.

> **Note**
>
> Prima di creare un server Transfer Family che utilizza Lambda come provider di identità, è necessario creare la funzione. Per un esempio di funzione Lambda, consulta Esempi di funzioni Lambda. In alternativa, puoi distribuire uno CloudFormation stack che utilizza uno dei. Modelli di funzioni Lambda Inoltre, assicurati che la tua funzione Lambda utilizzi una politica basata sulle risorse che si affidi a Transfer Family. Per un esempio di policy, consulta Policy Lambda basata sulle risorse.

1. Apri la AWS Transfer Family console.
2. Scegli Crea server per aprire la pagina Crea server. Per Scegli un provider di identità, scegli Custom Identity Provider, come mostrato nella schermata seguente.



> **Note**
>
> La scelta dei metodi di autenticazione è disponibile solo se abiliti SFTP come uno dei protocolli per il tuo server Transfer Family.

3. Assicurati che il valore predefinito, Usa AWS Lambda per connettere il tuo provider di identità, sia selezionato.
4. Per AWS Lambda la funzione, scegli il nome della tua funzione Lambda.

5. Compila le caselle rimanenti, quindi scegli Crea server. Per i dettagli sui passaggi rimanenti per la creazione di un server, consultaConfigurazione di un endpoint server SFTP, FTPS o FTP.

Policy Lambda basata sulle risorse

È necessario disporre di una policy che faccia riferimento al server Transfer Family e agli ARN Lambda. Ad esempio, puoi utilizzare la seguente politica con la funzione Lambda che si connette al tuo provider di identità. La policy viene salvata in formato JSON come stringa.

```
"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**
>
> Nella politica di esempio precedente, sostituisci ogni *segnaposto di input dell'utente* con le tue informazioni.

Struttura del messaggio di evento

La struttura dei messaggi di evento dal server SFTP inviati alla funzione di autorizzazione Lambda per un IDP personalizzato è la seguente.

```
{
    "username": "value",
    "password": "value",
    "protocol": "SFTP",
    "serverId": "s-abcd123456",
    "sourceIp": "192.168.0.100"
}
```

Dove `username` e `password` sono i valori per le credenziali di accesso inviate al server.

Ad esempio, si immette il seguente comando per connettersi:

```
sftp bobusa@server_hostname
```

Ti viene quindi richiesto di inserire la password:

```
Enter password:
    mysecretpassword
```

Puoi verificarlo dalla tua funzione Lambda stampando l'evento passato dall'interno della funzione Lambda. Dovrebbe essere simile al seguente blocco di testo.

```
{
    "username": "bobusa",
    "password": "mysecretpassword",
    "protocol": "SFTP",
    "serverId": "s-abcd123456",
    "sourceIp": "192.168.0.100"
}
```

La struttura degli eventi è simile per FTP e FTPS: l'unica differenza è che i valori vengono utilizzati per il `protocol` parametro, anziché SFTP.

Funzioni Lambda per l'autenticazione

Per implementare diverse strategie di autenticazione, modifica la funzione Lambda. Per aiutarti a soddisfare le esigenze della tua applicazione, puoi implementare uno CloudFormation stack. Per

ulteriori informazioni su Lambda, consulta la AWS Lambda Developer Guide o Building Lambda functions with Node.js.

Argomenti

- Modelli di funzioni Lambda
- Valori Lambda validi
- Esempi di funzioni Lambda
- Verifica della configurazione

Modelli di funzioni Lambda

È possibile distribuire uno AWS CloudFormation stack che utilizza una funzione Lambda per l'autenticazione. Forniamo diversi modelli che autenticano e autorizzano gli utenti utilizzando le credenziali di accesso. Puoi modificare questi modelli o AWS Lambda codici per personalizzare ulteriormente l'accesso degli utenti.

> **Note**
>
> È possibile creare un AWS Transfer Family server compatibile con FIPS AWS CloudFormation specificando una politica di sicurezza compatibile con FIPS nel modello. Le politiche di sicurezza disponibili sono descritte in Politiche di sicurezza per AWS Transfer Family i server

Per creare uno AWS CloudFormation stack da utilizzare per l'autenticazione

1. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
2. Segui le istruzioni per distribuire uno AWS CloudFormation stack da un modello esistente in Selezione di un modello di stack nella Guida per l'AWS CloudFormation utente.
3. Utilizza uno dei seguenti modelli per creare una funzione Lambda da utilizzare per l'autenticazione in Transfer Family.

   - Modello di pila classico (Amazon Cognito)

     Un modello di base per la creazione di un AWS Lambda file da utilizzare come provider di identità personalizzato in. AWS Transfer Family Si autentica con Amazon Cognito

per l'autenticazione basata su password e le chiavi pubbliche vengono restituite da un bucket Amazon S3 se viene utilizzata l'autenticazione basata su chiave pubblica. Dopo la distribuzione, puoi modificare il codice della funzione Lambda per fare qualcosa di diverso.

- AWS Secrets Manager modello di pila

  Un modello di base che si utilizza AWS Lambda con un AWS Transfer Family server per integrare Secrets Manager come provider di identità. Si autentica in base a una voce AWS Secrets Manager del formato. `aws/transfer/server-id/username` Inoltre, il segreto deve contenere le coppie chiave-valore per tutte le proprietà utente restituite a Transfer Family. Dopo la distribuzione, puoi modificare il codice della funzione Lambda per fare qualcosa di diverso.

- Modello stack Okta: un modello di base che utilizza AWS Lambda un AWS Transfer Family server per integrare Okta come provider di identità personalizzato.
- Modello di stack Okta-MFA: un modello di base che viene utilizzato AWS Lambda con un AWS Transfer Family server per integrare Okta, con autenticazione, come provider di identità personalizzato. MultiFactor
- Modello di Azure Active Directory: i dettagli per questo stack sono descritti nel post del blog Authenticating to with Azure Active Directory and. AWS Transfer FamilyAWS Lambda

Dopo aver distribuito lo stack, puoi visualizzarne i dettagli nella scheda Output della console. CloudFormation

L'implementazione di uno di questi stack è il modo più semplice per integrare un provider di identità personalizzato nel flusso di lavoro Transfer Family.

Valori Lambda validi

La tabella seguente descrive i dettagli dei valori che Transfer Family accetta per le funzioni Lambda utilizzate per i provider di identità personalizzati.

Valore	Descrizione	Richiesto
`Role`	Speciifica l'Amazon Resource Name (ARN) del ruolo IAM che controlla l'accesso degli utenti al bucket Amazon S3 o	Richiesto

Valore	Descrizione	Richiesto
	al file system Amazon EFS. Le policy associate a questo ruolo determinano il livello di accesso che desideri fornire ai tuoi utenti durante il trasferim ento di file da e verso il tuo file system Amazon S3 o Amazon EFS. Il ruolo IAM deve contenere anche una relazione di trust che consente al server di accedere alle proprie risorse durante la manutenzione delle richieste di trasferimento degli utenti. Per i dettagli su come stabilire una relazione di fiducia, consulta. Per stabilire una relazione di trust	
`PosixProfile`	L'identità POSIX completa, inclusi ID utente (`Uid`), ID di gruppo (`Gid`) ed eventuali ID di gruppo secondari (`SecondaryGids`), che controlla l'accesso degli utenti ai file system Amazon EFS. Le autorizzazioni POSIX impostate su file e directory nel file system determinano il livello di accesso che gli utenti ottengono durante il trasferim ento dei file da e verso i file system Amazon EFS.	Necessario per lo storage di backup di Amazon EFS

Valore	Descrizione	Richiesto
`PublicKeys`	Un elenco di valori di chiave pubblica SSH validi per questo utente. Un elenco vuoto implica che non si tratta di un accesso valido. Non deve essere restituito durante l'autenticazione della password.	Facoltativo
`Policy`	Una politica di sessione per il tuo utente in modo da poter utilizzare lo stesso ruolo IAM su più utenti. Questa policy definisce gli ambiti di accesso degli utenti alle porzioni dei loro bucket di Amazon S3.	Facoltativo

Valore	Descrizione	Richiesto
`HomeDirectoryType`	Il tipo di directory (cartella) di destinazione in cui deve trovarsi la directory home degli utenti quando accedono al server. • Se lo imposti su`PATH`, l'utente vede il bucket Amazon S3 assoluto o i percorsi Amazon EFS così come sono nei client del protocollo di trasferimento file. • Se lo imposti su`LOGICAL`, devi fornire mappature nel `HomeDirectoryDetails` parametro per rendere i percorsi Amazon S3 o Amazon EFS visibili ai tuoi utenti.	Facoltativo
`HomeDirectoryDetails`	Mappature di directory logiche che specificano quali percorsi e chiavi di Amazon S3 o Amazon EFS devono essere visibili all'utente e in che modo desideri renderli visibili. È necessario specificare la `Target` coppia `Entry` and, dove `Entry` mostra come il percorso viene reso visibile ed `Target` è il percorso effettivo di Amazon S3 o Amazon EFS.	Obbligatorio se `HomeDirectoryType` ha un valore di `LOGICAL`

Valore	Descrizione	Richiesto
`HomeDirectory`	La directory di destinazione di un utente quando accede al server utilizzando il client.	Facoltativo

> **Note**
>
> `HomeDirectoryDetails`è una rappresentazione in formato stringa di una mappa JSON. Ciò è in contrasto con`PosixProfile`, che è un vero oggetto della mappa JSON e `PublicKeys` che è un array di stringhe JSON. Vedi gli esempi di codice per i dettagli specifici della lingua.

Esempi di funzioni Lambda

Questa sezione presenta alcuni esempi di funzioni Lambda, sia in NodeJS che in Python.

> **Note**
>
> In questi esempi, i dettagli relativi all'utente, al ruolo, al profilo POSIX, alla password e alla home directory sono tutti esempi e devono essere sostituiti con i valori effettivi.

Logical home directory, NodeJS

La seguente funzione di esempio NodeJS fornisce i dettagli per un utente che dispone di una home directory logica.

```
// 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 seguente funzione di esempio NodeJS fornisce i dettagli per un utente che dispone di una home directory basata su percorsi.

```
// 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 seguente funzione di esempio in Python fornisce i dettagli per un utente che ha una home directory logica.

```
# 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 seguente funzione di esempio in Python fornisce i dettagli per un utente che dispone di una home directory basata su percorsi.

```
# 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
```

Verifica della configurazione

Dopo aver creato il tuo provider di identità personalizzato, dovresti testare la configurazione.

Console

Per testare la configurazione utilizzando la AWS Transfer Family console

1. Apri la AWS Transfer Family console.
2. Nella pagina Server, scegli il tuo nuovo server, scegli Azioni, quindi scegli Test.
3. Inserisci il testo per nome utente e password che hai impostato quando hai distribuito lo AWS CloudFormation stack. Se hai mantenuto le opzioni predefinite, il nome utente è `myuser` e la password è. `MySuperSecretPassword`
4. Scegli il protocollo Server e inserisci l'indirizzo IP per l'IP di origine, se lo hai impostato quando hai distribuito lo AWS CloudFormation stack.

CLI

Per testare la configurazione utilizzando la AWS CLI

1. Esegui il comando test-identity-provider. Sostituisci ciascuno *user input placeholder* con le tue informazioni, come descritto nei passaggi successivi.

```
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. Inserisci l'ID del server.
3. Inserisci il nome utente e la password che hai impostato quando hai distribuito lo AWS CloudFormation stack. Se hai mantenuto le opzioni predefinite, il nome utente è `myuser` e la password è. `MySuperSecretPassword`
4. Inserisci il protocollo del server e l'indirizzo IP di origine, se li hai impostati quando hai distribuito lo AWS CloudFormation stack.

Se l'autenticazione dell'utente ha esito positivo, il test restituisce una risposta `StatusCode: 200` HTTP, una stringa vuota `Message: ""` (che altrimenti conterrebbe un motivo dell'errore) e un campo. `Response`

> **Note**
>
> Nell'esempio di risposta riportato di seguito, il `Response` campo è un oggetto JSON che è stato «stringato» (convertito in una stringa JSON flat che può essere utilizzata all'interno di un programma) e contiene i dettagli dei ruoli e delle autorizzazioni dell'utente.


```
{
    "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": ""
}
```


Utilizzo di Amazon API Gateway per integrare il tuo provider di identità

Questo argomento descrive come utilizzare una AWS Lambda funzione per supportare un metodo API Gateway. Utilizza questa opzione se hai bisogno di un'API RESTful per integrare il tuo provider di identità o se desideri AWS WAF utilizzarla per sfruttarne le funzionalità per il blocco geografico o le richieste di limitazione della velocità.

Limitazioni relative all'utilizzo di un API Gateway per l'integrazione del provider di identità

- Questa configurazione non supporta domini personalizzati.
- Questa configurazione non supporta un URL API Gateway privato.

Se hai bisogno di uno di questi, puoi usare Lambda come provider di identità, senza API Gateway. Per informazioni dettagliate, vedi Utilizzo AWS Lambda per integrare il proprio provider di identità.

Autenticazione tramite un metodo API Gateway

Puoi creare un metodo API Gateway da utilizzare come provider di identità per Transfer Family. Questo approccio offre un modo estremamente sicuro per creare e fornire API. Con API Gateway, puoi creare un endpoint HTTPS in modo che tutte le chiamate API in entrata vengano trasmesse

con maggiore sicurezza. Per ulteriori dettagli sul servizio API Gateway, consulta la API Gateway Developer Guide.

API Gateway offre un metodo di autorizzazione denominato`AWS_IAM`, che offre la stessa autenticazione basata su AWS Identity and Access Management (IAM) AWS utilizzata internamente. Se abiliti l'autenticazione con`AWS_IAM`, solo i chiamanti con autorizzazioni esplicite per chiamare un'API possono raggiungere il metodo API Gateway dell'API.

Per utilizzare il tuo metodo API Gateway come provider di identità personalizzato per Transfer Family, abilita IAM per il tuo metodo API Gateway. Come parte di questo processo, fornisci a un ruolo IAM le autorizzazioni affinché Transfer Family utilizzi il tuo gateway.

> **Note**
>
> Per migliorare la sicurezza, puoi configurare un firewall per applicazioni Web. AWS WAF è un firewall per applicazioni Web che consente di monitorare le richieste HTTP e HTTPS inoltrate a un Amazon API Gateway. Per informazioni dettagliate, vedi Aggiungi un firewall per applicazioni Web.

Per utilizzare il metodo API Gateway per l'autenticazione personalizzata con Transfer Family

1. Crea uno AWS CloudFormation stack. Per farlo:

   > **Note**
   >
   > I modelli di stack sono stati aggiornati per utilizzare password con codifica Base64: per i dettagli, vedere. Miglioramenti ai modelli AWS CloudFormation

   a. AWS CloudFormation Apri la console all'indirizzo https://console.aws.amazon.com/cloudformation.

   b. Segui le istruzioni per distribuire uno AWS CloudFormation stack da un modello esistente in Selezione di un modello di stack nella Guida per l'AWS CloudFormation utente.

   c. Utilizza uno dei seguenti modelli di base per creare un metodo API Gateway AWS Lambda supportato da utilizzare come provider di identità personalizzato in Transfer Family.

      - Modello di stack di base

Per impostazione predefinita, il metodo API Gateway viene utilizzato come provider di identità personalizzato per autenticare un singolo utente in un singolo server utilizzando una chiave o una password SSH (Secure Shell) codificata. Dopo la distribuzione, puoi modificare il codice della funzione Lambda per fare qualcosa di diverso.

- AWS Secrets Manager modello di pila

  Per impostazione predefinita, il metodo API Gateway si autentica in base a una voce in Secrets Manager del formato. `aws/transfer/server-id/username` Inoltre, il segreto deve contenere le coppie chiave-valore per tutte le proprietà utente restituite a Transfer Family. Dopo la distribuzione, puoi modificare il codice della funzione Lambda per fare qualcosa di diverso. Per ulteriori informazioni, consulta il post del blog Abilita l'autenticazione tramite password per l' AWS Transfer Family utilizzo AWS Secrets Manager.

- Modello di stack Okta

  Il tuo metodo API Gateway si integra con Okta come provider di identità personalizzato in Transfer Family. Per ulteriori informazioni, consulta il post del blog Utilizzo di Okta come provider di identità con. AWS Transfer Family

L'implementazione di uno di questi stack è il modo più semplice per integrare un provider di identità personalizzato nel flusso di lavoro Transfer Family. Ogni stack utilizza la funzione Lambda per supportare il metodo API basato su API Gateway. Puoi quindi utilizzare il tuo metodo API come provider di identità personalizzato in Transfer Family. Per impostazione predefinita, la funzione Lambda autentica un singolo utente chiamato `myuser` con una password di. `MySuperSecretPassword` Dopo la distribuzione, puoi modificare queste credenziali o aggiornare il codice della funzione Lambda per fare qualcosa di diverso.

> **Important**
>
> Ti consigliamo di modificare le credenziali utente e password predefinite.

Dopo aver distribuito lo stack, puoi visualizzarne i dettagli nella scheda Output della console. CloudFormation Questi dettagli includono l'Amazon Resource Name (ARN) dello stack, l'ARN del ruolo IAM creato dallo stack e l'URL del nuovo gateway.

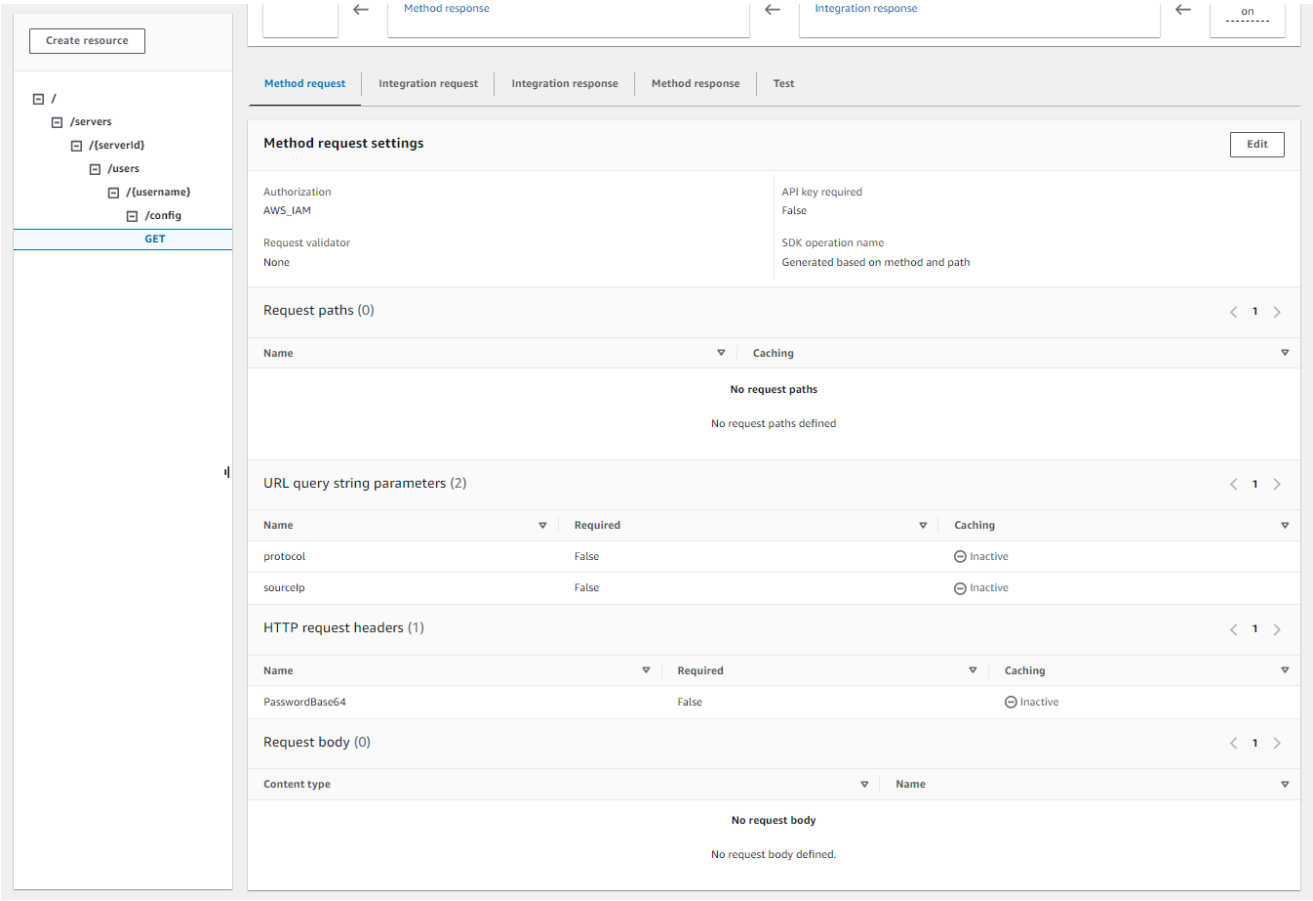
> **Note**
>
> Se utilizzi l'opzione provider di identità personalizzato per abilitare l'autenticazione basata su password per i tuoi utenti e abiliti la registrazione di richieste e risposte fornita da API Gateway, API Gateway registra le password degli utenti nei tuoi Amazon Logs. CloudWatch Non è consigliabile utilizzare questo registro nel tuo ambiente di produzione. Per ulteriori informazioni, consulta Configurare la registrazione delle CloudWatch API in API Gateway nella API Gateway Developer Guide.

2. Controlla la configurazione del metodo API Gateway per il tuo server. Per farlo:

   a. Aprire la console Gateway API all'indirizzo https://console.aws.amazon.com/apigateway/.

   b. Scegli l'API del modello di base di Transfer Custom Identity Provider generata dal AWS CloudFormation modello. Potrebbe essere necessario selezionare la regione per visualizzare i gateway.

   c. Nel riquadro Risorse, scegli GET. La schermata seguente mostra la configurazione corretta del metodo.

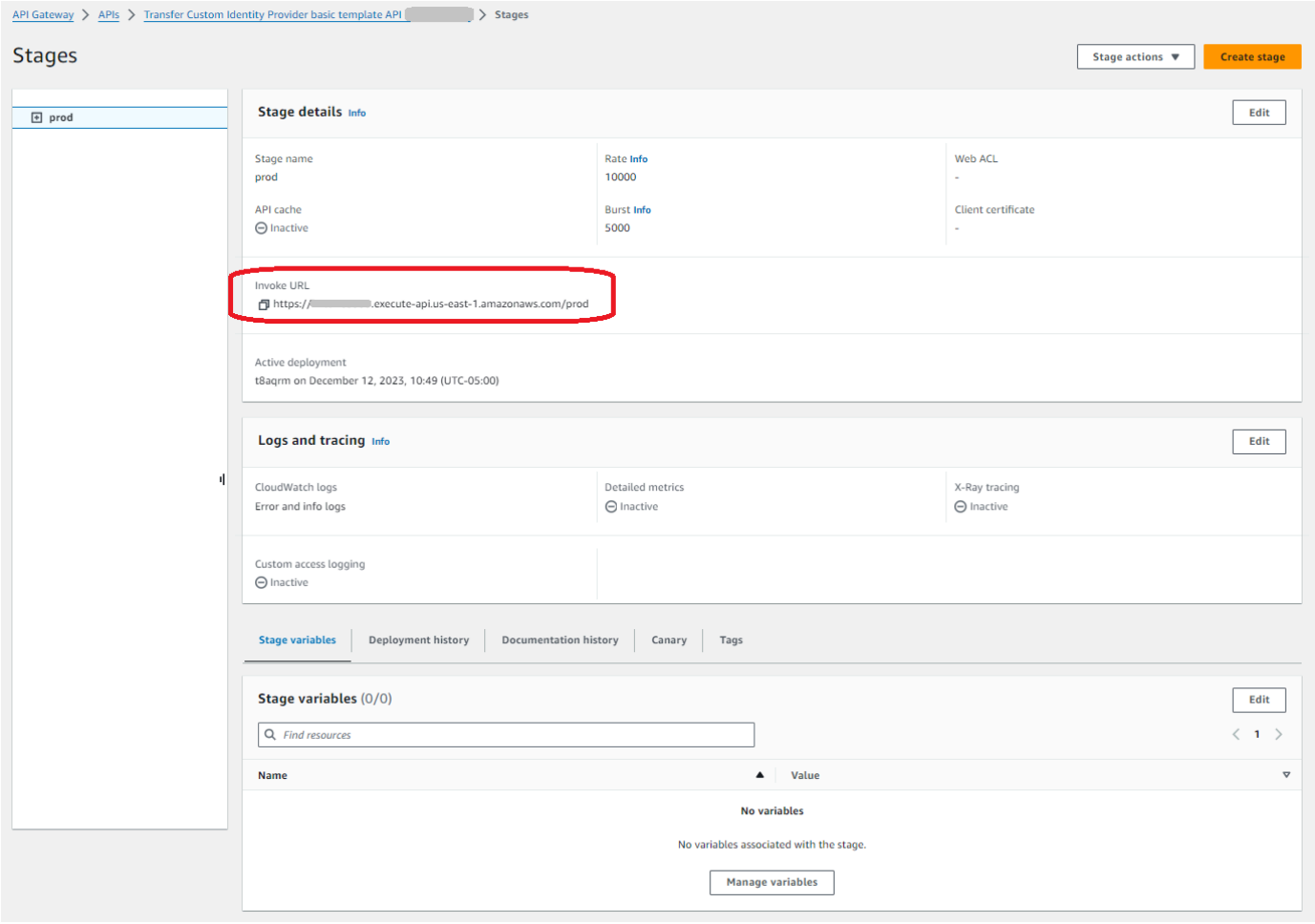


A questo punto, il gateway API è pronto per essere distribuito.

3. Per Azioni, scegli Deploy API. Per la fase di distribuzione, scegli prod, quindi scegli Deploy.

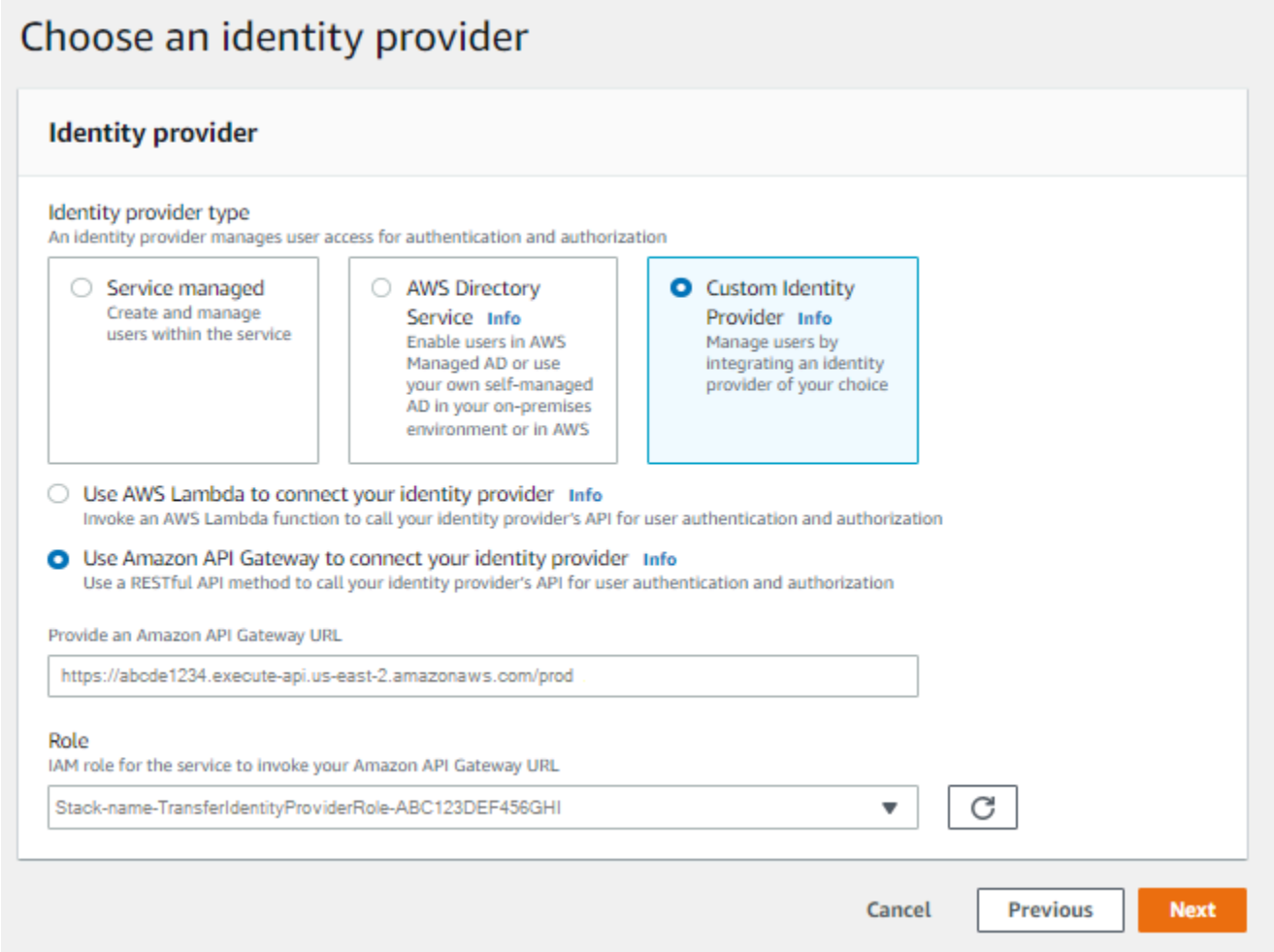
   Dopo che il metodo API Gateway è stato distribuito correttamente, visualizzane le prestazioni in Stages > Stage details, come mostrato nella schermata seguente.

> **Note**
>
> Copia l'indirizzo URL di Invoke visualizzato nella parte superiore dello schermo. Potresti averne bisogno per il passaggio successivo.



4. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
5. Una Transfer Family avrebbe dovuto essere creata per te quando hai creato lo stack. In caso contrario, configura il server seguendo questi passaggi.

a. Scegli Crea server per aprire la pagina Crea server. Per Scegli un provider di identità, scegli Personalizzato, quindi seleziona Usa Amazon API Gateway per connetterti al tuo provider di identità, come mostrato nella schermata seguente.



b. Nella casella di testo Fornisci un URL di Amazon API Gateway, incolla l'indirizzo URL Invoke dell'endpoint API Gateway che hai creato nel passaggio 3 di questa procedura.

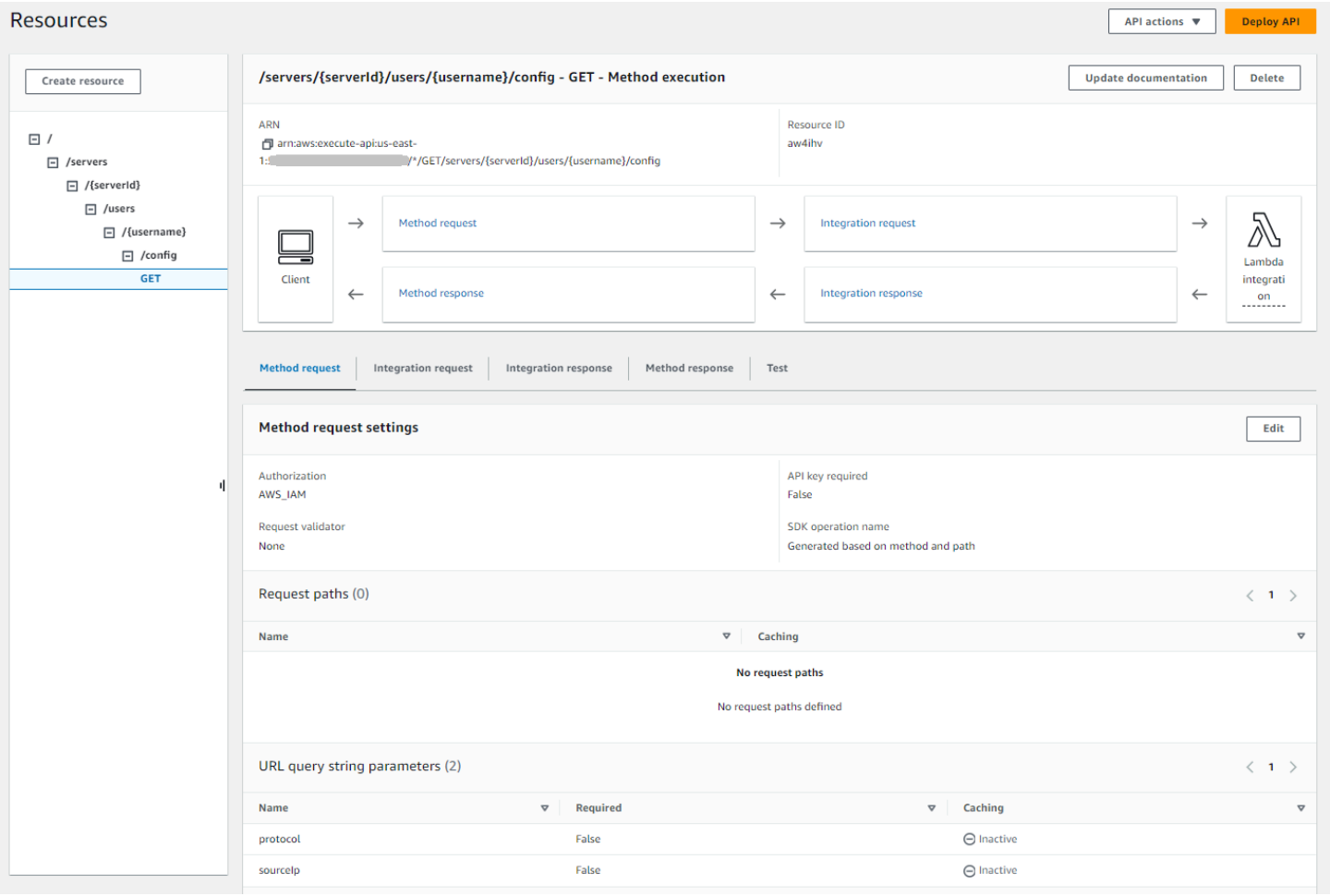
c. Per Ruolo, scegli il ruolo IAM creato dal AWS CloudFormation modello. Questo ruolo consente a Transfer Family di richiamare il metodo del gateway API.

   Il ruolo di invocazione contiene il nome AWS CloudFormation dello stack selezionato per lo stack creato nel passaggio 1. Ha il seguente formato:. *`CloudFormation-stack-name`*`-TransferIdentityProviderRole-`*`ABC123DEF456GHI`*

d. Compila le caselle rimanenti, quindi scegli Crea server. Per i dettagli sui passaggi rimanenti per la creazione di un server, consulta[Configurazione di un endpoint server SFTP, FTPS o FTP](#).

Implementazione del metodo API Gateway

Per creare un provider di identità personalizzato per Transfer Family, il metodo API Gateway deve implementare un unico metodo con un percorso di risorse di`/servers/`*`serverId`*`/users/`*`username`*`/config`. I *`username`* valori *`serverId`* and provengono dal percorso di risorse RESTful. Inoltre, aggiungete `sourceIp` e `protocol` come parametri della stringa di query URL nella richiesta del metodo, come mostrato nell'immagine seguente.



> **Note**
>
> Il nome utente deve contenere un minimo di 3 e un massimo di 100 caratteri. È possibile utilizzare i seguenti caratteri nel nome utente: a—z, A-Z, 0—9, trattino basso (_), trattino (-), punto (.) e segno di chiocciola (@). Tuttavia, il nome utente non può iniziare con un trattino (-), un punto (.) o un segno di chiavetta (@).

Se Transfer Family tenta l'autenticazione tramite password per l'utente, il servizio fornisce un campo di `Password:` intestazione. In assenza di un'`Password:`intestazione, Transfer Family tenta l'autenticazione a chiave pubblica per autenticare l'utente.

Quando utilizzi un provider di identità per autenticare e autorizzare gli utenti finali, oltre a convalidare le loro credenziali, puoi consentire o negare le richieste di accesso in base agli indirizzi IP dei client utilizzati dagli utenti finali. Puoi utilizzare questa funzionalità per assicurarti che i dati archiviati nei bucket S3 o nel file system Amazon EFS siano accessibili tramite i protocolli supportati solo da indirizzi IP che hai specificato come affidabili. Per abilitare questa funzionalità, devi includerla `sourceIp` nella stringa Query.

Se hai abilitato più protocolli per il tuo server e desideri fornire l'accesso utilizzando lo stesso nome utente su più protocolli, puoi farlo purché le credenziali specifiche per ogni protocollo siano state configurate nel tuo provider di identità. Per abilitare questa funzionalità, è necessario includere il *`protocol`* valore nel percorso della risorsa RESTful.

Il metodo API Gateway deve sempre restituire il codice di stato HTTP`200`. Qualsiasi altro codice di stato HTTP indica che si è verificato un errore durante l'accesso all'API.

Esempio di risposta di Amazon S3

Il corpo della risposta di esempio è un documento JSON del seguente modulo per 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 policy viene salvata in formato JSON come stringa. Per esempio:
>
> ```
> "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\"}]
}"
```

Il seguente esempio di risposta mostra che un utente ha un tipo di home directory logica.

```
{
   "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
   "HomeDirectoryType":"LOGICAL",
   "HomeDirectoryDetails":"[{\"Entry\":\"/\",\"Target\":\"/MY-HOME-BUCKET\"}]",
   "PublicKeys":[""]
}
```

Esempio di risposta Amazon EFS

Il corpo della risposta di esempio è un documento JSON del seguente modulo per 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"
}
```

Il `Role` campo mostra che l'autenticazione è avvenuta con successo. Quando si esegue l'autenticazione con password (quando si fornisce un'`Password:`intestazione), non è necessario fornire chiavi pubbliche SSH. Se un utente non può essere autenticato, ad esempio, se la password non è corretta, il metodo dovrebbe restituire una risposta senza set. `Role` Un esempio di tale risposta è un oggetto JSON vuoto.

Il seguente esempio di risposta mostra un utente con un tipo di home directory logica.

```
{
    "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
    "HomeDirectoryType": "LOGICAL",
    "HomeDirectoryDetails":"[{\"Entry\":\"/\",\"Target\":\"/faa1a123\"}]",
    "PublicKeys":[""],
    "PosixProfile":{"Uid":65534,"Gid":65534}
}
```

È possibile includere politiche utente nella funzione Lambda in formato JSON. Per ulteriori informazioni sulla configurazione delle politiche utente in Transfer Family, vedereGestione dei controlli di accesso.

Funzione Lambda predefinita

Per implementare diverse strategie di autenticazione, modifica la funzione Lambda utilizzata dal gateway. Per aiutarti a soddisfare le esigenze della tua applicazione, puoi utilizzare le funzioni Lambda di esempio seguenti in Node.js. Per ulteriori informazioni su Lambda, consulta la AWS Lambda Developer Guide o Building Lambda functions with Node.js.

L'esempio seguente della funzione Lambda utilizza il nome utente, la password (se si esegue l'autenticazione tramite password), l'ID del server, il protocollo e l'indirizzo IP del client. Puoi utilizzare una combinazione di questi input per cercare il tuo provider di identità e determinare se l'accesso deve essere accettato.

> **Note**
>
> Se hai abilitato più protocolli per il tuo server e desideri fornire l'accesso utilizzando lo stesso nome utente su più protocolli, puoi farlo purché le credenziali specifiche del protocollo siano state configurate nel tuo provider di identità.
> Per File Transfer Protocol (FTP), consigliamo di mantenere credenziali separate da Secure Shell (SSH) File Transfer Protocol (SFTP) e File Transfer Protocol over SSL (FTPS). Consigliamo di mantenere credenziali separate per FTP perché, a differenza di SFTP e FTPS, FTP trasmette le credenziali in testo non crittografato. Isolando le credenziali FTP da SFTP o FTPS, se le credenziali FTP sono condivise o esposte, i carichi di lavoro che utilizzano SFTP o FTPS rimangono sicuri.

Questa funzione di esempio restituisce il ruolo e i dettagli logici della home directory, insieme alle chiavi pubbliche (se esegue l'autenticazione a chiave pubblica).

Quando si creano utenti gestiti dai servizi, si imposta la loro home directory, logica o fisica. Allo stesso modo, abbiamo bisogno dei risultati della funzione Lambda per comunicare la struttura di directory fisica o logica desiderata dall'utente. I parametri impostati dipendono dal valore del campo. HomeDirectoryType

- `HomeDirectoryType`impostato su`PATH`: il `HomeDirectory` campo deve quindi essere un prefisso assoluto del bucket Amazon S3 o un percorso assoluto di Amazon EFS visibile ai tuoi utenti.
- `HomeDirectoryType`impostato su `LOGICAL` — Non impostare un campo. `HomeDirectory` Invece, impostiamo un `HomeDirectoryDetails` campo che fornisce le mappature Entry/Target desiderate, simili ai valori descritti nel HomeDirectoryDetailsparametro per gli utenti gestiti dal servizio.

Le funzioni di esempio sono elencate in. Esempi di funzioni Lambda

Funzione Lambda da utilizzare con AWS Secrets Manager

Per AWS Secrets Manager utilizzarla come provider di identità, puoi utilizzare la funzione Lambda nel modello di esempio AWS CloudFormation . La funzione Lambda interroga il servizio Secrets Manager con le tue credenziali e, in caso di successo, restituisce un segreto designato. Per ulteriori informazioni su Secrets Manager, consultare la Guida per l'utente di AWS Secrets Manager.

Per scaricare un AWS CloudFormation modello di esempio che utilizza questa funzione Lambda, vai al bucket Amazon S3 fornito da. AWS Transfer Family

Miglioramenti ai modelli AWS CloudFormation

Sono stati apportati miglioramenti all'interfaccia API Gateway ai CloudFormation modelli pubblicati. I modelli ora utilizzano password con codifica Base64 con API Gateway. Le distribuzioni esistenti continuano a funzionare anche senza questo miglioramento, ma non consentono l'utilizzo di password con caratteri diversi dal set di caratteri US-ASCII di base.

Le modifiche nel modello che abilitano questa funzionalità sono le seguenti:

- La `GetUserConfigRequest AWS::ApiGateway::Method` risorsa deve avere questo `RequestTemplates` codice (la riga in corsivo è la riga aggiornata)

```
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')"
}
```

- Il comando `RequestParameters` for the `GetUserConfig` resource deve cambiare per utilizzare l'`PasswordBase64`header (la riga in corsivo è la riga aggiornata):

```
RequestParameters:
   method.request.header.PasswordBase64: false
   method.request.querystring.protocol: false
   method.request.querystring.sourceIp: false
```

Per verificare se il modello per il tuo stack è il più recente

1. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
2. Dall'elenco degli stack, scegli il tuo stack.

3. Dal pannello dei dettagli, scegli la scheda Modello.
4. Cerca quanto segue:

   - Cerca `RequestTemplates` e assicurati di avere questa riga:

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

   - Cerca `RequestParameters` e assicurati di avere questa riga:

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

Se non vedi le righe aggiornate, modifica lo stack. Per i dettagli su come aggiornare lo AWS CloudFormation stack, consulta Modificare un modello di stack nella; Guida per l'AWS CloudFormation utente.

Utilizzo di directory logiche per semplificare le strutture di directory Transfer Family

Per semplificare la struttura delle directory AWS Transfer Family del server, è possibile utilizzare le directory logiche. Con le directory logiche, puoi creare una struttura di directory virtuale che utilizza nomi intuitivi che gli utenti utilizzano quando si connettono al tuo bucket Amazon S3 o al file system Amazon EFS. Quando utilizzi le directory logiche, puoi evitare di divulgare percorsi di directory assoluti, nomi di bucket Amazon S3 e nomi di file system EFS agli utenti finali.

> **Note**
>
> È necessario utilizzare politiche di sessione in modo che gli utenti finali possano eseguire solo le operazioni che consentite loro di eseguire.
> È necessario utilizzare le directory logiche per creare una directory virtuale intuitiva per gli utenti finali e astrarre i nomi dei bucket. Le mappature delle directory logiche consentono solo agli utenti di accedere ai percorsi logici e alle sottodirectory designati e vietano i percorsi relativi che attraversano le radici logiche.
> Transfer Family convalida ogni percorso che potrebbe includere elementi relativi e blocca attivamente la risoluzione di questi percorsi prima di trasferirli ad Amazon S3; questo impedisce agli utenti di andare oltre le loro mappature logiche.

Anche se Transfer Family impedisce agli utenti finali di accedere a directory al di fuori della loro directory logica, ti consigliamo di utilizzare anche ruoli o policy di sessione unici per applicare il privilegio minimo a livello di storage.

È possibile utilizzare le directory logiche per impostare la directory principale dell'utente nella posizione desiderata all'interno della gerarchia di archiviazione, eseguendo una cosiddetta operazione. chroot In questa modalità, gli utenti non sono in grado di accedere a una directory esterna alla home o alla directory principale che avete configurato per loro.

Ad esempio, sebbene un utente Amazon S3 sia stato limitato al solo accesso`/mybucket/home/${transfer:UserName}`, alcuni client consentono agli utenti di attraversare una cartella fino a. `/mybucket/home` In questa situazione, l'utente torna alla home directory desiderata solo dopo essersi disconnesso e aver nuovamente effettuato il login al server Transfer Family. L'esecuzione di un'chrootoperazione può impedire il verificarsi di questa situazione.

È possibile creare una struttura di directory personalizzata tra bucket e prefissi. Questa funzionalità è utile se hai un flusso di lavoro che prevede una struttura di directory specifica che non puoi replicare tramite i prefissi dei bucket. Puoi anche collegarti a più posizioni non contigue all'interno di Amazon S3, in modo simile alla creazione di un collegamento simbolico in un file system Linux in cui il percorso della directory fa riferimento a una posizione diversa nel file system.

Mappature dei FILE delle directory logiche

Il tipo di `HomeDirectoryMapEntry` dati ora include un `Type` parametro. Prima che questo parametro esistesse, avresti potuto creare una mappatura logica di directory in cui la destinazione era un file. Se in precedenza è stato creato uno di questi tipi di mappature di directory logiche, è necessario `Type` impostarlo in modo esplicito su`FILE`, altrimenti tali mappature non funzioneranno correttamente in futuro.
Un modo per farlo è chiamare l'`UpdateUser`API e impostarla per la mappatura esistente`Type`. `FILE`

Regole per l'utilizzo delle directory logiche

Prima di creare le mappature delle directory logiche, è necessario comprendere le seguenti regole:

- In caso `Entry` `"/"` affermativo, è possibile avere una sola mappatura perché non sono consentiti percorsi sovrapposti.
- Le directory logiche supportano mappature fino a 2,1 MB (per gli utenti gestiti dai servizi, questo limite è di 2.000 voci). Cioè, la struttura dati che contiene le mappature ha una dimensione massima di 2,1 MB. Se disponi di molte mappature, puoi calcolarne le dimensioni nel modo seguente:

  1. Scrivi una mappatura tipica nel formato`{"Entry":"/`*`entry-path`*`","Target":"/`*`target-path`*`"}`, dove *`entry-path`* e dove *`target-path`* sono i valori effettivi che utilizzerai.
  2. Conta i caratteri in quella stringa, quindi aggiungine uno (1).
  3. Moltiplica quel numero per il numero approssimativo di mappature che hai per il tuo server.

  Se il numero stimato nel passaggio 3 è inferiore a 2,1 MB, le mappature rientrano nel limite accettabile.
- Le destinazioni possono utilizzare la `${transfer:UserName}` variabile se il percorso del bucket o del file system è stato parametrizzato in base al nome utente.
- Le destinazioni possono essere percorsi in diversi bucket o file system, ma è necessario assicurarsi che il ruolo mappato AWS Identity and Access Management (IAM) (il `Role` parametro nella risposta) fornisca l'accesso a tali bucket o file system.
- Non specificate il `HomeDirectory` parametro, poiché questo valore è implicito nelle `Entry` `Target` coppie quando utilizzate il `LOGICAL` valore per il parametro. `HomeDirectoryType`
- Le destinazioni devono iniziare con un carattere forward slash (`/`), ma non utilizzare la barra finale (`/`) quando si specifica il. `Target` Ad esempio, `/DOC-EXAMPLE-BUCKET/images` è accettabile, ma non lo `DOC-EXAMPLE-BUCKET/images` è. `/DOC-EXAMPLE-BUCKET/images/`
- Amazon S3 è un archivio di oggetti, il che significa che le cartelle sono un concetto virtuale e non esiste una vera gerarchia di directory. Se la tua applicazione esegue un'`stat`operazione da un client, tutto viene classificato come file quando utilizzi Amazon S3 per lo storage. Questo comportamento è descritto in Organizzazione degli oggetti nella console Amazon S3 utilizzando le cartelle nella Guida per l'utente di Amazon Simple Storage Service. Se la tua applicazione richiede che mostri `stat` con precisione se qualcosa è un file o una cartella, puoi utilizzare Amazon Elastic File System (Amazon EFS) come opzione di storage per i tuoi server Transfer Family.
- Se stai specificando valori di directory logica per il tuo utente, il parametro da utilizzare dipende dal tipo di utente:
  - Per gli utenti gestiti dal servizio, fornisci i valori della directory logica in. `HomeDirectoryMappings`

- Per gli utenti di provider di identità personalizzati, fornisci i valori della directory logica in. `HomeDirectoryDetails`

> **Important**
>
> A meno che tu non scelga di ottimizzare le prestazioni per le tue directory Amazon S3 (quando crei o aggiorni un server), la directory principale deve esistere all'avvio. Per Amazon S3, ciò significa che devi aver già creato un oggetto a zero byte che termina con una barra (/) per creare la cartella principale. Evitare questo problema è un motivo per prendere in considerazione l'ottimizzazione delle prestazioni di Amazon S3.

Implementazione di directory logiche e `chroot`

Per utilizzare le directory e le chroot funzionalità logiche, è necessario effettuare le seguenti operazioni:

Attiva le directory logiche per ogni utente. A tale scopo, imposta il `HomeDirectoryType` parametro su `LOGICAL` quando crei o aggiorni l'utente.

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

`chroot`

Perchroot, crea una struttura di directory composta da una singola `Entry` `Target` combinazione per ogni utente. La cartella principale è il `Entry` punto e la `Target` posizione nel bucket o nel file system a cui eseguire la mappatura.

Example for Amazon S3

```
[{"Entry": "/", "Target": "/mybucket/jane"}]
```

Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

È possibile utilizzare un percorso assoluto come nell'esempio precedente oppure utilizzare una sostituzione dinamica del nome utente con`${transfer:UserName}`, come nell'esempio seguente.

```
[{"Entry": "/", "Target":
"/mybucket/${transfer:UserName}"}]
```

Nell'esempio precedente, l'utente è bloccato nella propria directory principale e non può spostarsi più in alto nella gerarchia.

Struttura delle directory virtuali

Per una struttura di directory virtuale, puoi creare più `Entry` `Target` abbinamenti, con destinazioni ovunque nei bucket S3 o nei file system EFS, anche su più bucket o file system, purché la mappatura dei ruoli IAM dell'utente disponga delle autorizzazioni per accedervi.

Nel seguente esempio di struttura virtuale, quando l'utente accede a AWS SFTP, si trova nella directory principale con le sottodirectory di,, e. `/pics` `/doc` `/reporting` `/anotherpath/subpath/financials`

> **Note**
>
> A meno che tu non scelga di ottimizzare le prestazioni per le tue directory Amazon S3 (quando crei o aggiorni un server), l'utente o un amministratore devono creare le directory se non esistono già. Evitare questo problema è un motivo per prendere in considerazione l'ottimizzazione delle prestazioni di Amazon S3.
> Per Amazon EFS, è comunque necessario che l'amministratore crei le mappature logiche o la `/` directory.

```
[
{"Entry": "/pics", "Target": "/bucket1/pics"},
{"Entry": "/doc", "Target": "/bucket1/anotherpath/docs"},
{"Entry": "/reporting", "Target": "/reportingbucket/Q1"},
{"Entry": "/anotherpath/subpath/financials", "Target": "/reportingbucket/financials"}]
```

> **Note**
>
> Puoi caricare file solo nelle cartelle specifiche che mappi. Ciò significa che nell'esempio precedente non è possibile caricare `/anotherpath` nelle nostre `anotherpath/subpath`

directory, ma soloanotherpath/subpath/financials. Inoltre, non è possibile eseguire la mappatura diretta su tali percorsi, poiché non sono consentiti percorsi sovrapposti. Ad esempio, si supponga di creare le seguenti mappature:

```
{
   "Entry": "/pics",
   "Target": "/mybucket/pics"
},
{
   "Entry": "/doc",
   "Target": "/mybucket/mydocs"
},
{
   "Entry": "/temp",
   "Target": "/mybucket"
}
```

Puoi caricare file solo in quei bucket. La prima volta che ti connettisftp, verrai inserito nella directory principale,/. Se tenti di caricare un file in quella directory, il caricamento non riesce. I comandi seguenti mostrano una sequenza di esempio:

```
sftp> pwd
Remote working directory: /
sftp> put file
Uploading file to /file
remote open("/file"): No such file or directory
```

Per eseguire il caricamento su qualsiasidirectory/sub-directory, è necessario mappare in modo esplicito il percorso a. sub-directory

Per ulteriori informazioni sulla configurazione delle directory logiche e chroot per gli utenti, incluso un AWS CloudFormation modello da scaricare e utilizzare, consulta Semplifica la struttura AWS SFTP con chroot e directory logiche nello Storage Blog. AWS

Esempio di configurazione delle directory logiche

In questo esempio, creiamo un utente e assegniamo due directory logiche. Il comando seguente crea un nuovo utente (per un server Transfer Family esistente) con directory logiche pics edoc.

```
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
```

Se **`marymajor`** è un utente esistente e il suo tipo di home directory èPATH, puoi cambiarlo `LOGICAL` con un comando simile a quello precedente.

```
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\"}]"
```

Tieni presente quanto segue:

- Se le directory `/DOC-EXAMPLE-BUCKET1/pics` e `/DOC-EXAMPLE-BUCKET2/test/mydocs` io non esistono già, l'utente (o un amministratore) deve crearle.
- Quando **`marymajor`** si connette al server ed esegue il `ls -l` comando, vede quanto segue:

  ```
  drwxr--r--   1        -        -        0 Mar 17 15:42 doc
  drwxr--r--   1        -        -        0 Mar 17 16:04 pics
  ```

- **`marymajor`**non può creare file o directory a questo livello. Tuttavia, all'interno di `pics` and`doc`, può aggiungere sottodirectory.
- File che aggiunge `pics` e che `doc` vengono aggiunti rispettivamente ai percorsi `/DOC-EXAMPLE-BUCKET1/pics` di Amazon S3. `/DOC-EXAMPLE-BUCKET2/test/mydocs`
- In questo esempio, specifichiamo due diversi bucket per illustrare questa possibilità. Tuttavia, è possibile utilizzare lo stesso bucket per diverse o tutte le directory logiche specificate per l'utente.

Configurazione di directory logiche per Amazon EFS

Se il tuo server Transfer Family utilizza Amazon EFS, la home directory dell'utente deve essere creata con accesso in lettura e scrittura prima che l'utente possa lavorare nella sua home directory logica. L'utente non può creare questa directory da solo, poiché non avrebbe le autorizzazioni per la `mkdir` sua home directory logica.

Se la directory home dell'utente non esiste e l'utente esegue un `ls` comando, il sistema risponde come segue:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Un utente con accesso amministrativo alla directory principale deve creare la home directory logica dell'utente.

AWS Lambda Risposta personalizzata

Puoi utilizzare le directory logiche con una funzione Lambda che si connette al tuo provider di identità personalizzato. A tale scopo, nella funzione Lambda, si specificano i `Target` valori `HomeDirectoryType` as **`LOGICAL`** e add `Entry` and per il `HomeDirectoryDetails` parametro. Per esempio:

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{\"Entry\": \"/\", \"Target\": \"/DOC-EXAMPLE-BUCKET/
theRealFolder"}]"
```

Il codice seguente è un esempio di risposta riuscita da una chiamata di autenticazione Lambda personalizzata.

```
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 `"Url":` riga viene restituita solo se si utilizza un metodo API Gateway come provider di identità personalizzato.

AWS Transfer Family Connettori SFTP

AWS Transfer Family I connettori SFTP stabiliscono una relazione per l'invio di file e messaggi tra lo storage Amazon e un partner esterno, utilizzando il protocollo SFTP. Puoi inviare file da Amazon S3 a una destinazione esterna di proprietà del partner. Puoi anche utilizzare un connettore SFTP per recuperare file dal server SFTP di un partner.

> **Note**
>
> Attualmente, i connettori SFTP possono essere utilizzati solo per connettersi a server SFTP remoti che offrono un endpoint accessibile da Internet.

I seguenti post del blog forniscono un'architettura di riferimento per creare un flusso di lavoro MFT utilizzando connettori SFTP, inclusa la crittografia dei file tramite PGP prima di inviarli a un server SFTP remoto utilizzando connettori SFTP: Progettazione di trasferimenti di file gestiti sicuri e conformi con connettori SFTP e crittografia PGP. AWS Transfer Family

Visualizza i connettori AWS Transfer Family SFTP per una breve introduzione ai connettori SFTP Transfer Family.

Argomenti

Configurare i connettori SFTP

Questo argomento descrive come creare connettori SFTP, gli algoritmi di sicurezza ad essi associati, come memorizzare un segreto per conservare le credenziali, dettagli sulla formattazione della chiave privata e istruzioni per testare i connettori.

Argomenti

- Memorizza un segreto da utilizzare con un connettore SFTP
- Genera e formatta la chiave privata del connettore SFTP
- Provate un connettore SFTP

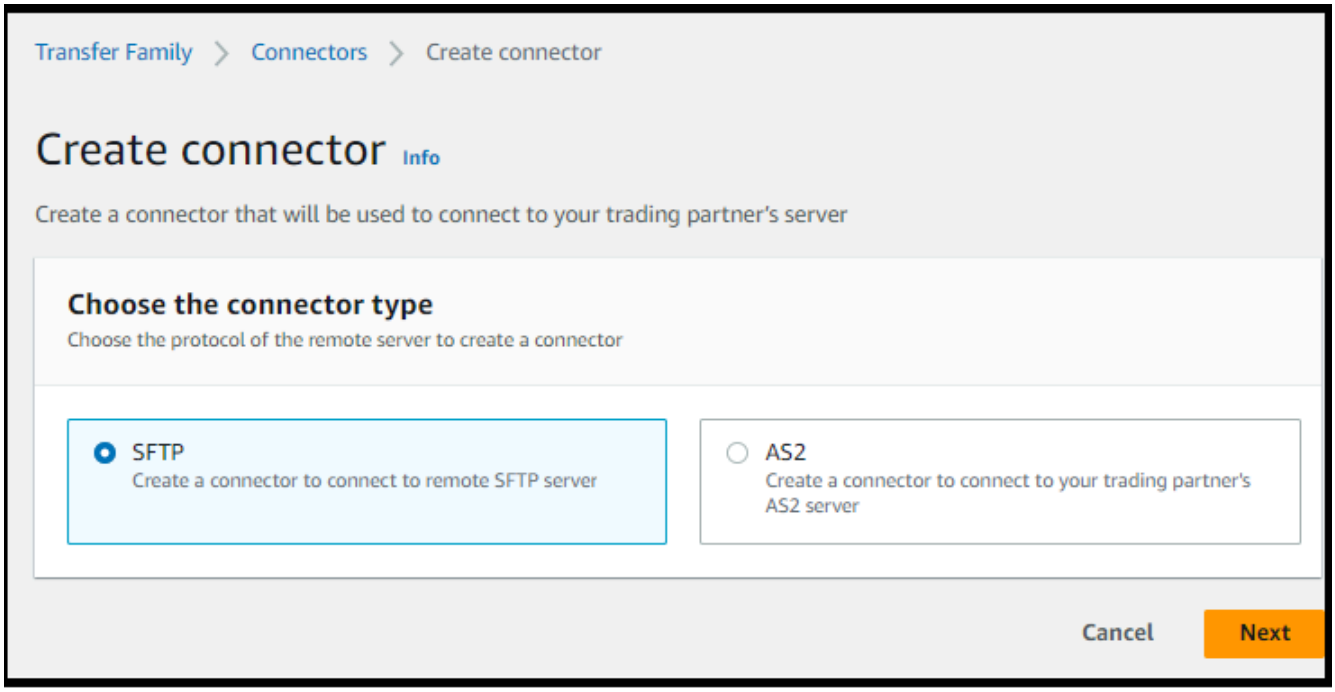
Creare un connettore SFTP

Questa procedura spiega come creare connettori SFTP utilizzando la AWS Transfer Family console o. AWS CLI

Console

Per creare un connettore SFTP

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Connettori, quindi scegli Crea connettore.
3. Scegli SFTP come tipo di connettore per creare un connettore SFTP, quindi scegli Avanti.



4. Nella sezione Configurazione del connettore, fornite le seguenti informazioni:
   - Per l'URL, inserite l'URL di un server SFTP remoto. Questo URL deve essere formattato come`sftp://`*`partner-SFTP-server-url`*, ad esempio. `sftp://AnyCompany.com`

> **Note**
>
> Facoltativamente, puoi fornire un numero di porta nel tuo URL. Il formato è `sftp://`*`partner-SFTP-server-url`*`:`*`port-number`*. Il numero di porta predefinito (quando non viene specificata alcuna porta) è la porta 22.

- Per il ruolo Access, scegli l'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) da utilizzare.
  - Assicurati che questo ruolo fornisca l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta.
  - Assicurati che questo ruolo fornisca l'autorizzazione `secretsmanager:GetSecretValue` per accedere al segreto.

    > **Note**
    >
    > Nella policy, è necessario specificare l'ARN per il segreto. L'ARN contiene il nome segreto, ma aggiunge al nome sei caratteri alfanumerici casuali. Un ARN per un segreto ha il seguente formato.
    >
    > ```
    > arn:aws:secretsmanager:region:account-id:secret:aws/
    > transfer/SecretName-6RandomCharacters
    > ```

  - Assicurati che questo ruolo contenga una relazione di fiducia che consenta al connettore di accedere alle tue risorse per soddisfare le richieste di trasferimento degli utenti. Per i dettagli su come stabilire una relazione di fiducia, consulta. Per stabilire una relazione di trust

L'esempio seguente concede le autorizzazioni necessarie per accedere al *DOC-EXAMPLE-BUCKET* in Amazon S3 e al segreto specificato archiviato in 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

Per il ruolo di accesso, l'esempio concede l'accesso a un singolo segreto. Tuttavia, puoi utilizzare un carattere jolly, che può far risparmiare lavoro se desideri riutilizzare lo stesso ruolo IAM per più utenti e segreti. Ad esempio, la seguente dichiarazione di risorsa concede le autorizzazioni per tutti i segreti il cui nome inizia con. `aws/transfer`

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/*"
```

È inoltre possibile archiviare i segreti contenenti le credenziali SFTP in un altro. Account AWS Per i dettagli sull'abilitazione dell'accesso segreto tra account, consulta Autorizzazioni ai AWS Secrets Manager segreti per gli utenti di un altro account.

- (Facoltativo) Per il ruolo di registrazione, scegli il ruolo IAM per il connettore da utilizzare per inviare eventi ai tuoi log. CloudWatch La seguente policy di esempio elenca le autorizzazioni necessarie per registrare gli eventi per i connettori SFTP.

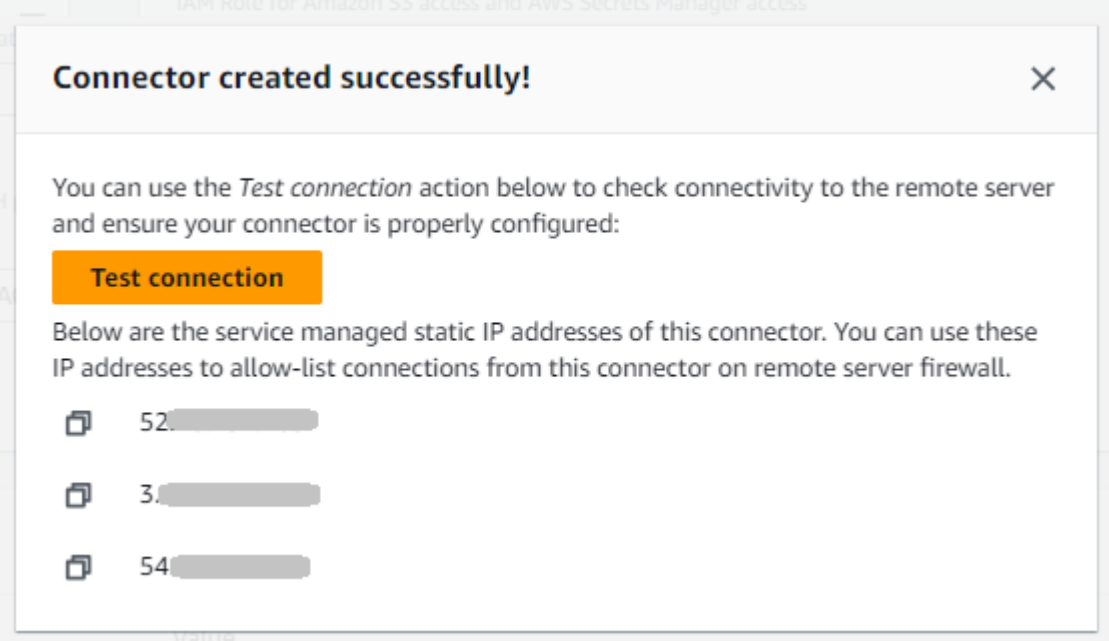
```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "SFTPConnectorPermissions",
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogStream",
            "logs:DescribeLogStreams",
            "logs:CreateLogGroup",
            "logs:PutLogEvents"
        ],
  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

5. Nella sezione Configurazione SFTP, fornite le seguenti informazioni:

   - Per le credenziali del connettore, dall'elenco a discesa, scegli il nome di un segreto AWS Secrets Manager che contiene la chiave privata o la password dell'utente SFTP. È necessario creare un segreto e archiviarlo in un modo specifico. Per informazioni dettagliate, vedi Memorizza un segreto da utilizzare con un connettore SFTP.
   - Per le chiavi host affidabili, incolla la parte pubblica della chiave host utilizzata per identificare il server esterno. Puoi aggiungere più di una chiave, scegliendo Aggiungi chiave host affidabile per aggiungere una chiave aggiuntiva. È possibile utilizzare il `ssh-keyscan` comando sul server SFTP per recuperare la chiave necessaria. Per informazioni

dettagliate sul formato e sul tipo di chiavi host affidabili supportate da Transfer Family, vedere SFTPConnectorConfig.

6. Nella sezione Opzioni dell'algoritmo di crittografia, scegli una politica di sicurezza dall'elenco a discesa nel campo Politica di sicurezza. La politica di sicurezza consente di selezionare gli algoritmi crittografici supportati dal connettore. Per i dettagli sulle politiche e sugli algoritmi di sicurezza disponibili, vedere. Politiche AWS Transfer Family di sicurezza per i connettori SFTP
7. (Facoltativo) Nella sezione Tag, per Chiave e Valore, inserite uno o più tag come coppie chiave-valore.
8. Dopo aver confermato tutte le impostazioni, scegli Crea connettore per creare il connettore SFTP. Se il connettore viene creato correttamente, viene visualizzata una schermata con un elenco degli indirizzi IP statici assegnati e un pulsante Test di connessione. Utilizzate il pulsante per testare la configurazione del nuovo connettore.



Viene visualizzata la pagina Connettori, con l'ID del nuovo connettore SFTP aggiunto all'elenco. Per visualizzare i dettagli dei connettori, consultaVisualizza i dettagli del connettore SFTP.

CLI

Il create-connectorcomando viene utilizzato per creare un connettore. Per utilizzare questo comando per creare un connettore SFTP, è necessario fornire le seguenti informazioni.

- L'URL di un server SFTP remoto. Questo URL deve essere formattato come`sftp://`*`partner-SFTP-server-url`*, ad esempio. `sftp://AnyCompany.com`
- Il ruolo di accesso. Scegli l'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) da utilizzare.
  - Assicurati che questo ruolo fornisca l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta.
  - Assicurati che questo ruolo fornisca l'autorizzazione `secretsmanager:GetSecretValue` per accedere al segreto.

    > **Note**
    >
    > Nella policy, è necessario specificare l'ARN per il segreto. L'ARN contiene il nome segreto, ma aggiunge al nome sei caratteri alfanumerici casuali. Un ARN per un segreto ha il seguente formato.
    >
    > ```
    > arn:aws:secretsmanager:region:account-id:secret:aws/
    > transfer/SecretName-6RandomCharacters
    > ```

  - Assicurati che questo ruolo contenga una relazione di fiducia che consenta al connettore di accedere alle tue risorse per soddisfare le richieste di trasferimento degli utenti. Per i dettagli su come stabilire una relazione di fiducia, consulta. Per stabilire una relazione di trust

L'esempio seguente concede le autorizzazioni necessarie per accedere al *DOC-EXAMPLE-BUCKET* in Amazon S3 e al segreto specificato archiviato in 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

Per il ruolo di accesso, l'esempio concede l'accesso a un singolo segreto. Tuttavia, puoi utilizzare un carattere jolly, che può far risparmiare lavoro se desideri riutilizzare lo stesso ruolo IAM per più utenti e segreti. Ad esempio, la seguente dichiarazione di risorsa concede le autorizzazioni per tutti i segreti il cui nome inizia con. `aws/transfer`

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/
*"
```

È inoltre possibile archiviare i segreti contenenti le credenziali SFTP in un altro. Account AWS Per i dettagli sull'abilitazione dell'accesso segreto tra account, consulta Autorizzazioni ai AWS Secrets Manager segreti per gli utenti di un altro account.

- (Facoltativo) Scegli il ruolo IAM per il connettore da utilizzare per inviare eventi ai tuoi CloudWatch log. La seguente policy di esempio elenca le autorizzazioni necessarie per registrare gli eventi per i connettori 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/*"
        ]
    }]
}
```

- Fornite le seguenti informazioni di configurazione SFTP.
  - L'ARN di un segreto AWS Secrets Manager che contiene la chiave privata o la password dell'utente SFTP.
  - La parte pubblica della chiave host utilizzata per identificare il server esterno. Se lo desideri, puoi fornire più chiavi host affidabili.

  Il modo più semplice per fornire le informazioni SFTP è salvarle in un file. Ad esempio, copiate il seguente testo di esempio in un file denominato`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="
   ]
}
```

- Specificate una politica di sicurezza per il connettore, inserendo il nome della politica di sicurezza.

> **Note**
>
> `SecretId`Può essere l'intero ARN o il nome del segreto (*`example-username-key`* nell'elenco precedente).

Quindi esegui il comando seguente per creare il connettore.

```
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
```

Memorizza un segreto da utilizzare con un connettore SFTP

È possibile utilizzare Secrets Manager per memorizzare le credenziali utente per i connettori SFTP. Quando crei il tuo segreto, devi fornire un nome utente. Inoltre, puoi fornire una password, una chiave privata o entrambe. Per informazioni dettagliate, vedi Quote per i connettori SFTP.

> **Note**
>
> Quando memorizzi segreti in Secrets Manager, ti vengono Account AWS addebitati dei costi. Per informazioni sui prezzi, consulta Prezzi di AWS Secrets Manager.

Per memorizzare le credenziali utente in Secrets Manager per un connettore SFTP

1. Accedere AWS Management Console e aprire la AWS Secrets Manager console all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Nel pannello di navigazione a sinistra, seleziona Segreti.
3. Nella pagina Segreti, scegli Memorizza un nuovo segreto.
4. Nella pagina Scegli il tipo di segreto, per Tipo segreto, scegli Altro tipo di segreto.
5. Nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.
   - Chiave: Invio. **`Username`**

- valore: immettere il nome dell'utente autorizzato a connettersi al server del partner.

6. Se desideri fornire una password, scegli Aggiungi riga e nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.

   Scegli Aggiungi riga e, nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.

   - Chiave: Invio. **`Password`**
   - valore: immettere la password per l'utente.

7. Se desideri fornire una chiave privata, vediGenera e formatta la chiave privata del connettore SFTP, che descrive come inserire i dati della chiave privata.

   > **Note**
   >
   > I dati della chiave privata immessi devono corrispondere alla chiave pubblica archiviata per questo utente nel server SFTP remoto.

8. Seleziona Successivo.
9. Nella pagina Configura segreto, inserisci un nome e una descrizione per il tuo segreto. Ti consigliamo di utilizzare il prefisso di **`aws/transfer/`** per il nome. Ad esempio, puoi dare un nome al tuo segreto**`aws/transfer/connector-1`**.
10. Scegli Avanti, quindi accetta le impostazioni predefinite nella pagina Configura rotazione. Quindi scegli Successivo.
11. Nella pagina Revisione, scegli Store per creare e archiviare il segreto.

Genera e formatta la chiave privata del connettore SFTP

I dettagli completi per la generazione di una coppia di chiavi pubblica/privata sono descritti in. Creazione di chiavi SSH su macOS, Linux o Unix

Ad esempio, per generare una chiave privata da utilizzare con i connettori SFTP, il seguente comando di esempio produce il tipo di chiave corretto (sostituisci *`key_name con il nome`* file effettivo per la tua coppia di chiavi):

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

> **Note**
>
> Quando si crea una key pair da utilizzare con i connettori SFTP, non utilizzare una passphrase. È necessaria una passphrase vuota per il corretto funzionamento della configurazione SFTP.

Questo comando crea una coppia di chiavi RSA, con una dimensione della chiave di 4096 bit. La chiave viene generata nel formato PEM legacy, richiesto da Transfer Family per l'utilizzo con il segreto del connettore SFTP. Le chiavi vengono salvate in *key_name* (chiave privata) e *key_name*`.pub` (chiave pubblica) nella directory corrente, ovvero la directory in cui si esegue il `ssh-keygen` comando.

> **Note**
>
> Transfer Family non supporta il formato OpenSSH `-----BEGIN OPENSSH PRIVATE KEY-----` () per le chiavi utilizzate per il connettore SFTP. La chiave deve essere in formato PEM precedente (o). `-----BEGIN RSA PRIVATE KEY-----` `-----BEGIN EC PRIVATE KEY-----` È possibile utilizzare lo ssh-keygen strumento per convertire la chiave, fornendo l'`-m PEM`opzione quando si esegue il comando.

Dopo aver generato la chiave, è necessario assicurarsi che la chiave privata sia formattata con caratteri di nuova riga incorporati (»\n«) in formato JSON.

Utilizzate un comando per convertire la chiave privata esistente nel formato corretto: il formato JSON con caratteri di nuova riga incorporati. Qui forniamo esempi per e Powershell. `jq` Puoi utilizzare qualsiasi strumento o comando per convertire la chiave privata in formato JSON con caratteri di nuova riga incorporati.

jq command

Questo esempio utilizza il `jq` comando, che può essere scaricato da Download jq.

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

Ad esempio, se il file della chiave privata si trova in`~/.ssh/my_private_key`, il comando è il seguente.

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

Ciò restituisce la chiave nel formato corretto (con caratteri di nuova riga incorporati) sullo standard output.

PowerShell

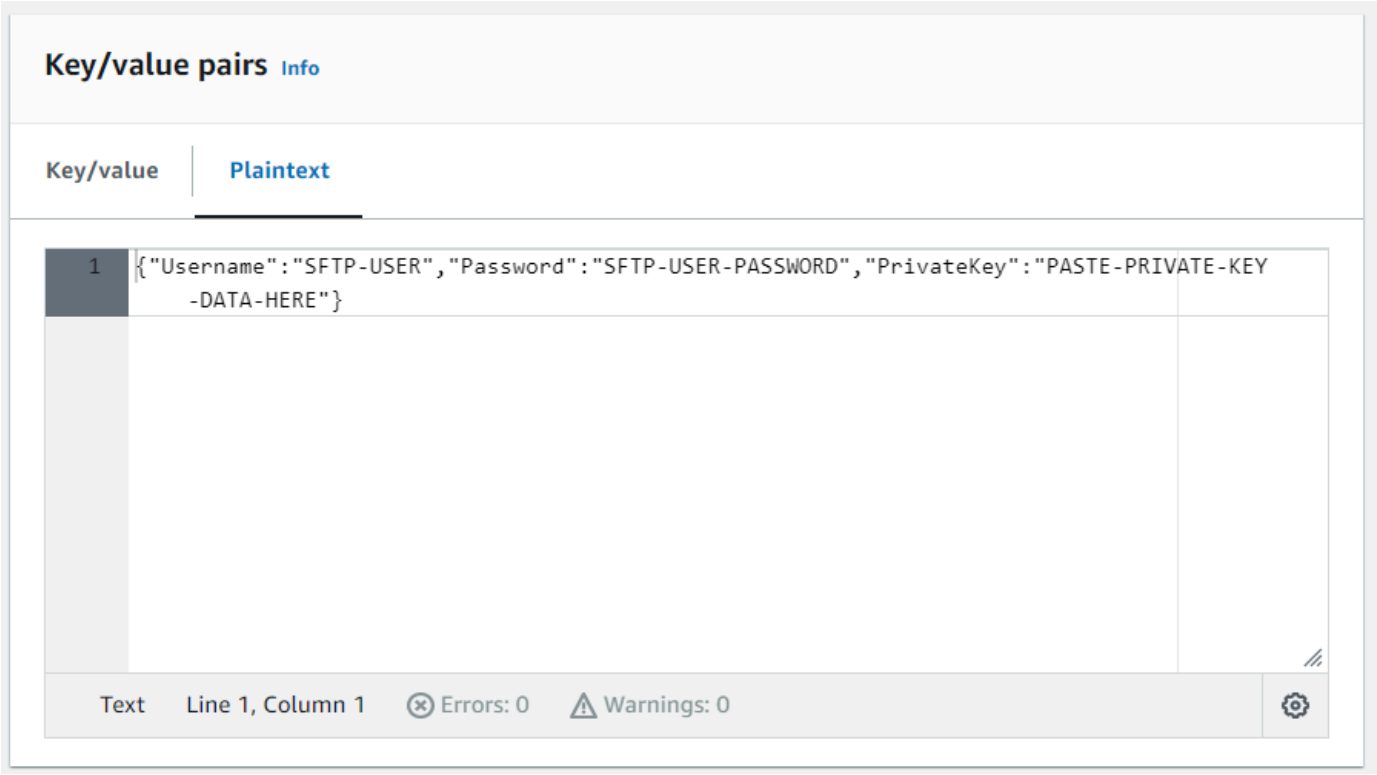
Se si utilizza Windows, è possibile utilizzare PowerShell per convertire la chiave nel formato corretto. Il seguente comando Powershell converte la chiave privata nel formato corretto.

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

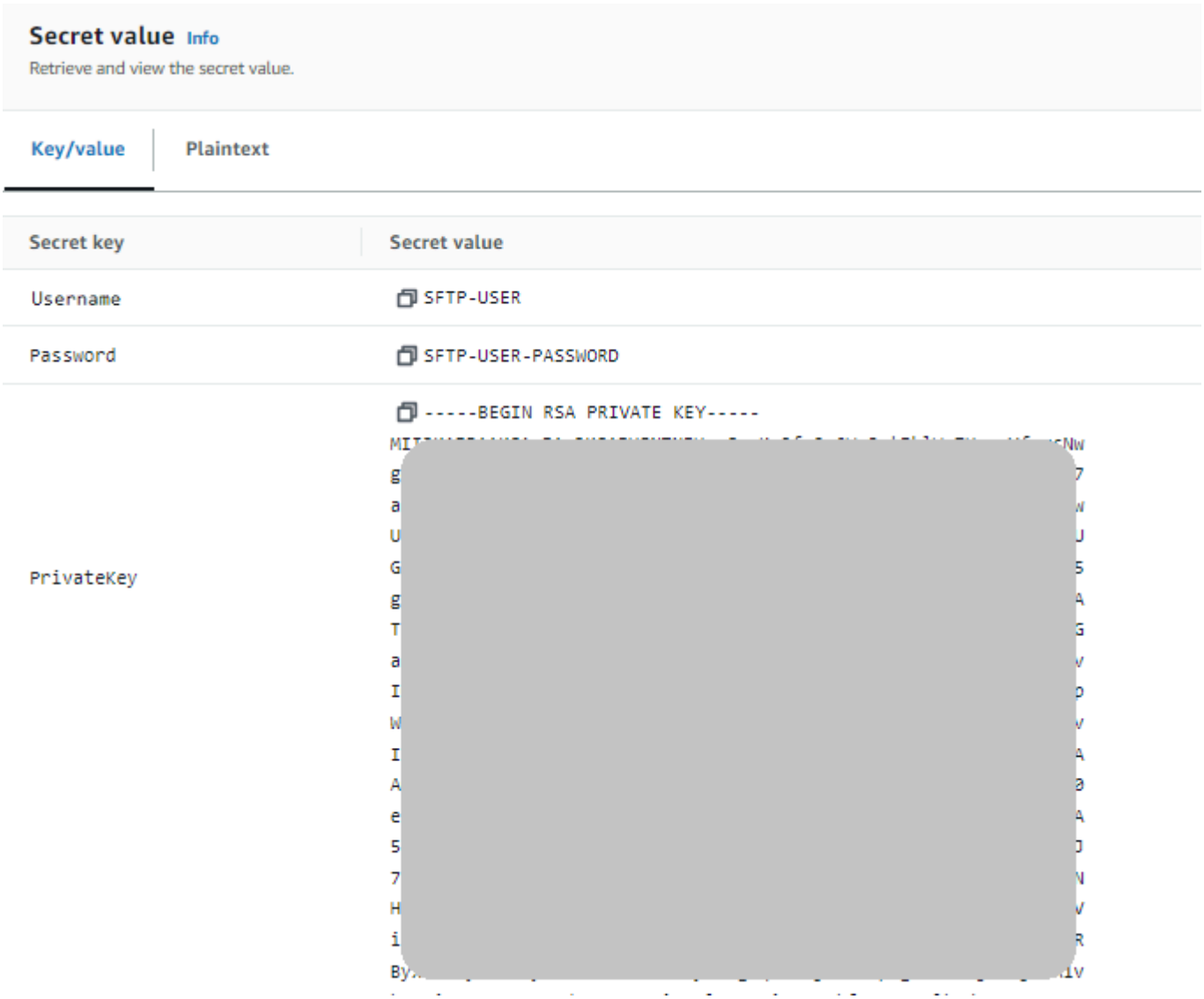
Per aggiungere dati di chiave privata al segreto da utilizzare con i connettori SFTP

1. Nella console Secrets Manager, quando memorizzi Altro tipo di segreto, scegli la scheda Testo normale. Il testo deve essere vuoto, con solo una parentesi di apertura e chiusura, {}.
2. Incolla il tuo nome utente, i dati della chiave privata e/o la password utilizzando il seguente formato. Per i dati della chiave privata, incolla l'output del comando eseguito nel passaggio 1.

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



Se incollate correttamente i dati della chiave privata, dovreste vedere quanto segue selezionando la scheda Chiave/valore. Notate che i dati della chiave privata vengono visualizzati line-by-line, anziché come una stringa di testo continua.



3. Continuate la procedura descritta Memorizza un segreto da utilizzare con un connettore SFTP al punto 8 e seguitela fino alla fine.

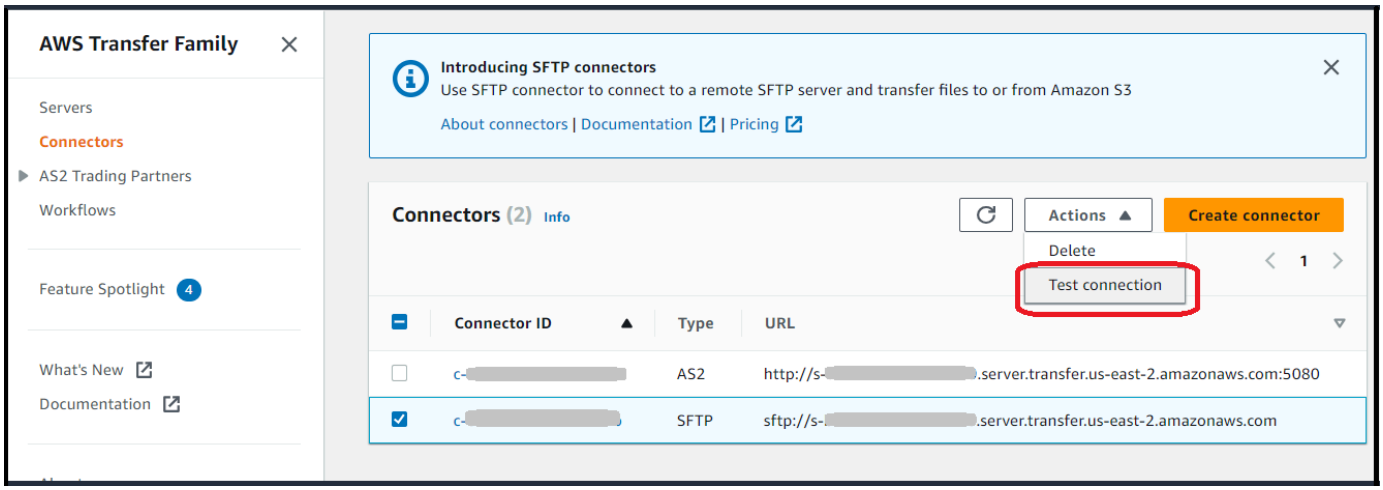
Provate un connettore SFTP

Dopo aver creato un connettore SFTP, si consiglia di testarlo prima di tentare di trasferire qualsiasi file utilizzando il nuovo connettore.

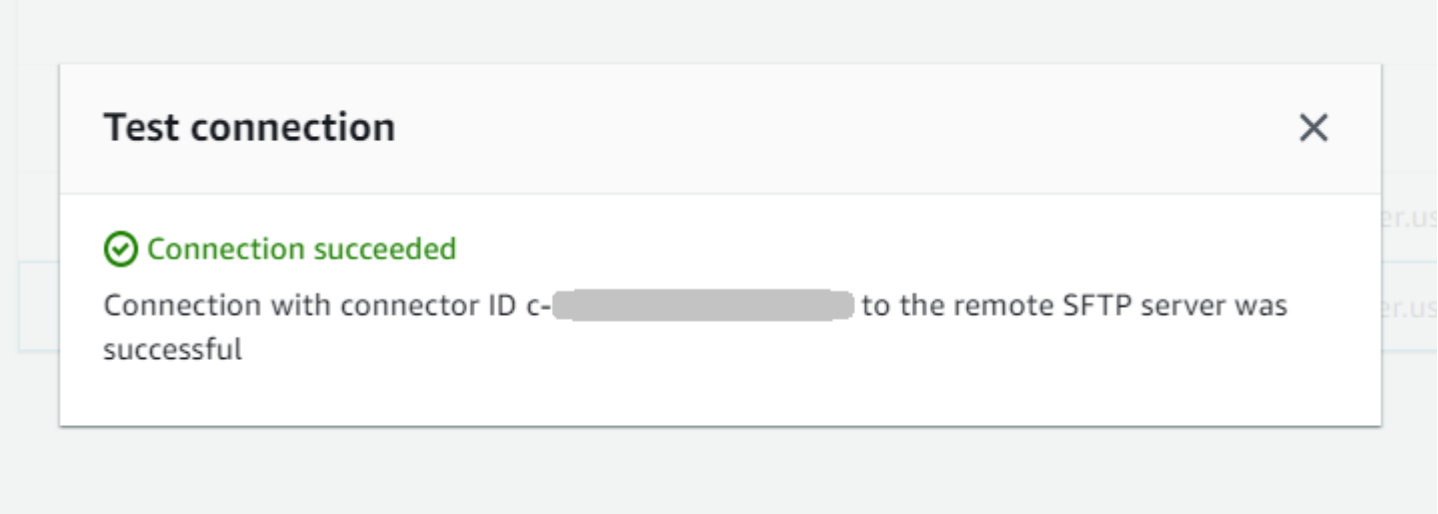
Per testare un connettore SFTP

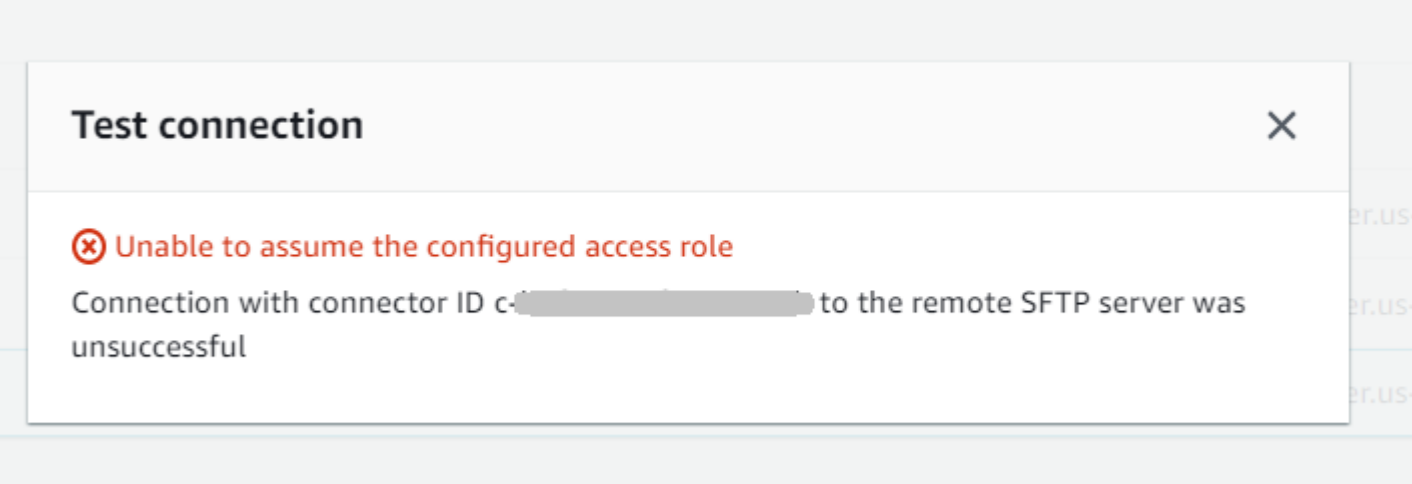
1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Connettori e seleziona un connettore.

3. Dal menu Azioni, scegli Verifica connessione.



Il sistema restituisce un messaggio che indica se il test ha esito positivo o negativo. Se il test fallisce, il sistema fornisce un messaggio di errore in base al motivo per cui il test non è riuscito.





> **Note**
>
> Per utilizzare l'API per testare il connettore, consulta la documentazione dell'TestConnectionAPI.

Inviare e recuperare file utilizzando un connettore SFTP

I connettori SFTP estendono le capacità AWS Transfer Family di comunicazione con server remoti sia nel cloud che in locale. Puoi integrare i dati generati e archiviati in fonti remote con i tuoi data warehouse AWS ospitati per analisi, applicazioni aziendali, report e audit.

Per avviare un trasferimento di file su un server SFTP remoto, si utilizza l'operazione StartFileTransferAPI, che utilizza connettori SFTP per eseguire il trasferimento. Ogni `StartFileTransfer` richiesta può contenere 10 percorsi distinti.

È possibile monitorare i trasferimenti di file controllando i log del server. L'attività del connettore viene registrata per registrare i flussi che hanno il formato, ad esempio`aws/transfer/connector-id`, di. `aws/transfer/c-1234567890abcdef0` Se non vedi alcun registro relativo al connettore, assicurati di aver specificato un ruolo di registrazione con le autorizzazioni corrette per il connettore.

Per i dettagli sulla creazione di connettori, consulta. Configurare i connettori SFTP

Per inviare e recuperare file utilizzando un connettore SFTP, utilizzate il comando `start-file-transfer` AWS Command Line Interface (AWS CLI). Specificate i seguenti parametri, a seconda che stiate inviando file (trasferimenti in uscita) o ricevendo file (trasferimenti in entrata).

- Trasferimenti in uscita
  - `send-file-paths`contiene da uno a dieci percorsi di file di origine, per i file da trasferire al server SFTP del partner.
  - `remote-directory-path`è il percorso remoto a cui inviare un file sul server SFTP del cliente.
- Trasferimenti in entrata
  - `retrieve-file-paths`contiene da uno a dieci percorsi remoti. Ogni percorso specifica una posizione per il trasferimento dei file dal server SFTP del partner al server Transfer Family.
  - `local-directory-path`è la posizione Amazon S3 (bucket e prefisso opzionale) in cui sono archiviati i file.

Per inviare file, devi specificare i parametri and. `send-file-paths` `remote-directory-path` È possibile specificare fino a 10 file per il `send-file-paths` parametro. Il seguente comando di esempio invia i file denominati `/DOC-EXAMPLE-SOURCE-BUCKET/file1.txt` e`/DOC-EXAMPLE-SOURCE-BUCKET/file2.txt`, che si trovano nello storage Amazon S3, alla `/tmp` directory sul server SFTP del tuo partner. Per utilizzare questo comando di esempio, sostituisci il *DOC-EXAMPLE-SOURCE-BUCKET* con il tuo 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
```

Per ricevere i file, specificate i `local-directory-path` parametri `retrieve-file-paths` and. *L'esempio seguente recupera i file /my/remote/file1.txt e li memorizza / my/remote/file2.txt sul server SFTP del partner e li colloca nel prefisso / DOC-EXAMPLE-BUCKET/della posizione Amazon S3.* Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
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
```

Gli esempi precedenti specificano percorsi assoluti sul server SFTP. È inoltre possibile utilizzare percorsi relativi, ovvero percorsi relativi alla home directory dell'utente SFTP. Ad esempio, se l'utente SFTP è `marymajor` e la sua home directory sul server SFTP è`/users/marymajor/`, il seguente comando invia a `/DOC-EXAMPLE-SOURCE-BUCKET/file1.txt` `/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
```

Elenca il contenuto di una directory remota

Prima di recuperare i file da un server SFTP remoto, è possibile recuperare il contenuto di una directory sul server SFTP remoto. A tale scopo, si utilizza la chiamata API. StartDirectoryListing

L'esempio seguente elenca il contenuto della home cartella sul server SFTP remoto, specificato nella configurazione del connettore. I risultati vengono inseriti nella posizione `/DOC-EXAMPLE-BUCKET/connector-files` Amazon S3 e in un file denominato. `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
```

Questo AWS CLI comando restituisce l'ID dell'elenco e il nome del file che contiene i risultati.

```
{
    "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",
    "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"
}
```

> **Note**
>
> La convenzione di denominazione per il file di output è*`connector-ID`*`-`*`listing-ID`*`.json`.

Il file JSON contiene le seguenti informazioni:

- `filePath`: il percorso completo di un file remoto, relativo alla directory della richiesta di quotazione per il connettore SFTP sul server remoto.
- `modifiedTimestamp`: l'ultima volta che il file è stato modificato, in secondi, in formato UTC (Coordinated Universal Time). Questo campo è facoltativo. Se gli attributi del file remoto non contengono un timestamp, questo viene omesso dall'elenco dei file.
- `size`: la dimensione del file, in byte. Questo campo è facoltativo. Se gli attributi del file remoto non contengono una dimensione del file, questo viene omesso dall'elenco dei file.
- `path`: il percorso completo di una directory remota, relativo alla directory della richiesta di elenco per il connettore SFTP sul server remoto.
- `truncated`: un flag che indica se l'output della lista contiene o meno tutti gli elementi contenuti nella directory remota. Se il valore di `truncated` output è vero, puoi aumentare il valore fornito nell'attributo `max-items` input opzionale per poter elencare più elementi (fino alla dimensione massima consentita dell'elenco di 10.000 elementi).

Di seguito è riportato un esempio del contenuto del file di output (`c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json`), in cui la directory remota contiene due file e due sottodirectory (percorsi).

```
{
    "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"
}
```

Gestione dei connettori SFTP

Questo argomento descrive come visualizzare e aggiornare i connettori SFTP ed elenca le quote rilevanti per i connettori SFTP.

> **Note**
>
> A ogni connettore vengono assegnati automaticamente indirizzi IP statici che rimangono invariati per tutta la durata del connettore. Ciò consente di connettersi a server SFTP remoti che accettano solo connessioni in entrata da indirizzi IP noti. Ai connettori viene assegnato un set di indirizzi IP statici condivisi da tutti i connettori che utilizzano lo stesso protocollo (SFTP o AS2) del tuo. Account AWS

Argomenti

Aggiorna i connettori SFTP

Per modificare i valori dei parametri esistenti per i connettori, puoi eseguire il `update-connector` comando. Il comando seguente aggiorna il segreto per il connettore*connector-id*, nella regione *region-id* a*secret-ARN*. Per utilizzare questo comando di esempio, sostituisci *user input placeholders* con le tue informazioni.

```
aws transfer update-connector --sftp-config '{"UserSecretId":"secret-ARN"}' \
   --connector-id connector-id --region region-id
```

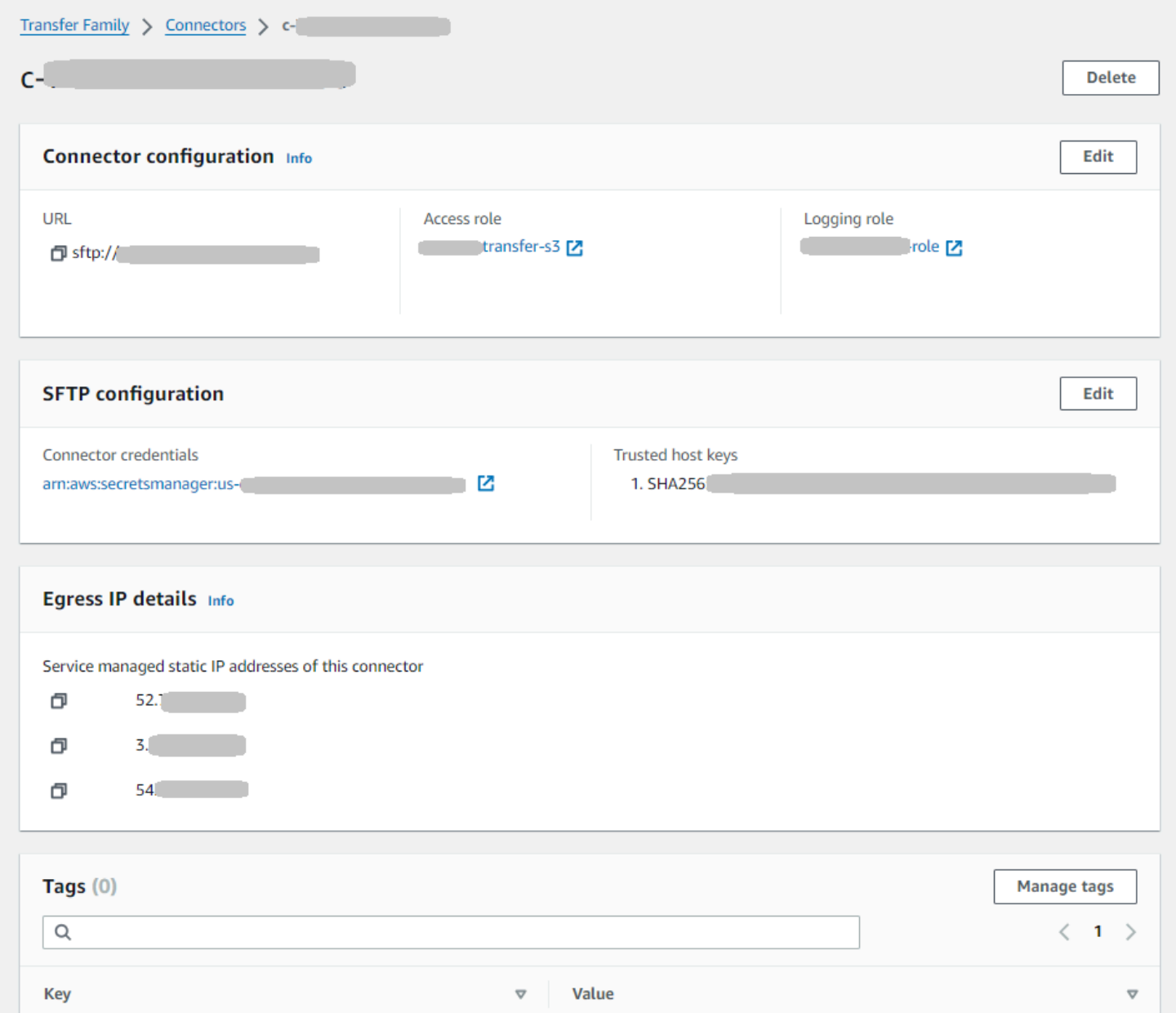
Visualizza i dettagli del connettore SFTP

È possibile trovare un elenco di dettagli e proprietà di un connettore SFTP nella AWS Transfer Family console.

Per visualizzare i dettagli del connettore

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, selezionare Connectors (Connettori).
3. Scegli l'identificatore nella colonna Connector ID per visualizzare la pagina dei dettagli del connettore selezionato.

È possibile modificare le proprietà del connettore SFTP scegliendo Modifica nella pagina dei dettagli del connettore.



> **Note**
>
> È possibile ottenere molte di queste informazioni, anche se in un formato diverso, eseguendo il comando seguente AWS Command Line Interface ()AWS CLI. Per utilizzare questo comando di esempio, sostituisci *`user input placeholders`* con le tue informazioni.
>
> ```
> aws transfer describe-connector --connector-id your-connector-id
> ```
>
> Per ulteriori informazioni, consulta il riferimento DescribeConnectorall'API.

Quote per i connettori SFTP

Le seguenti quote sono valide per i connettori SFTP.

> **Note**
>
> Altre quote di servizio per i connettori SFTP sono elencate negli AWS Transfer Family endpoint e le quote in. Riferimenti generali di Amazon Web Services

Quote dei connettori SFTP

Nome	Predefinita	Adattabile
Numero massimo di transazioni di connessione di test al secondo (TPS)	1 richiesta al secondo, per account	No
Dimensione massima della coda per i trasferimenti di file in sospeso	1000	No
Dimensione massima dei file	50 gibibyte (GiB)	No
Tempo massimo di trasferimento per file	6 ore	No
Tempo massimo di attesa della richiesta per file	6 ore	No
Larghezza di banda massima per i connettori per account (entrambi i connettori SFTP e AS2 contribuiscono a questo valore)	50 MBps	No

Per memorizzare le credenziali per i connettori SFTP, ci sono delle quote associate a ciascun segreto di Secrets Manager. Se si utilizza lo stesso segreto per archiviare più tipi di chiavi, per più scopi, è possibile che si verifichino queste quote.

- Lunghezza totale per un singolo segreto: 12.000 caratteri
- Lunghezza massima della **`Password`** stringa: 1024 caratteri
- Lunghezza massima della **`PrivateKey`** stringa: 8192 caratteri
- Lunghezza massima della **`Username`** stringa: 100 caratteri

AWS Transfer Family per AS2

La Dichiarazione di applicabilità 2 (AS2) è una specifica di trasmissione di file definita dalla RFC che include potenti meccanismi di protezione e verifica dei messaggi. Il protocollo AS2 è fondamentale per i flussi di lavoro con requisiti di conformità che si basano sull'integrazione di funzionalità di protezione e sicurezza dei dati nel protocollo.

> **Note**
>
> AS2 for Transfer Family è certificato Drummond.

I clienti di settori come la vendita al dettaglio, le scienze biologiche, la produzione, i servizi finanziari e i servizi di pubblica utilità che si affidano ad AS2 per i flussi di lavoro della catena di approvvigionamento, della logistica e dei pagamenti possono utilizzare gli endpoint AWS Transfer Family AS2 per effettuare transazioni in sicurezza con i propri partner commerciali. I dati oggetto di transazione sono accessibili in modo nativo per l'elaborazione, l'analisi e l'apprendimento automatico AWS . Questi dati sono disponibili anche per le integrazioni con i sistemi di pianificazione delle risorse aziendali (ERP) e di gestione delle relazioni con i clienti (CRM) che funzionano su. AWS Con AS2, i clienti possono eseguire le proprie transazioni business-to-business (B2B) su larga scala, mantenendo al AWS contempo le integrazioni e la conformità dei partner commerciali esistenti.

Se sei un cliente Transfer Family che desidera scambiare file con un partner che dispone di un server configurato abilitato per AS2, la configurazione prevede la generazione di una coppia di chiavi pubblica-privata per la crittografia e un'altra per la firma e lo scambio delle chiavi pubbliche con il partner.

Transfer Family offre un workshop a cui puoi partecipare, in cui puoi configurare un endpoint Transfer Family con AS2 abilitato e un connettore Transfer Family AS2. Puoi visualizzare i dettagli di questo workshop qui.

La protezione di un payload AS2 in transito prevede in genere l'uso della sintassi dei messaggi crittografici (CMS) e generalmente utilizza la crittografia e la firma digitale per fornire protezione dei dati e autenticazione tra pari. Un payload di risposta MDN (Message Disposition Notice) firmato consente di verificare (non ripudio) che un messaggio sia stato ricevuto e decifrato correttamente.

Il trasporto di questi payload CMS e delle risposte MDN avviene tramite HTTP.

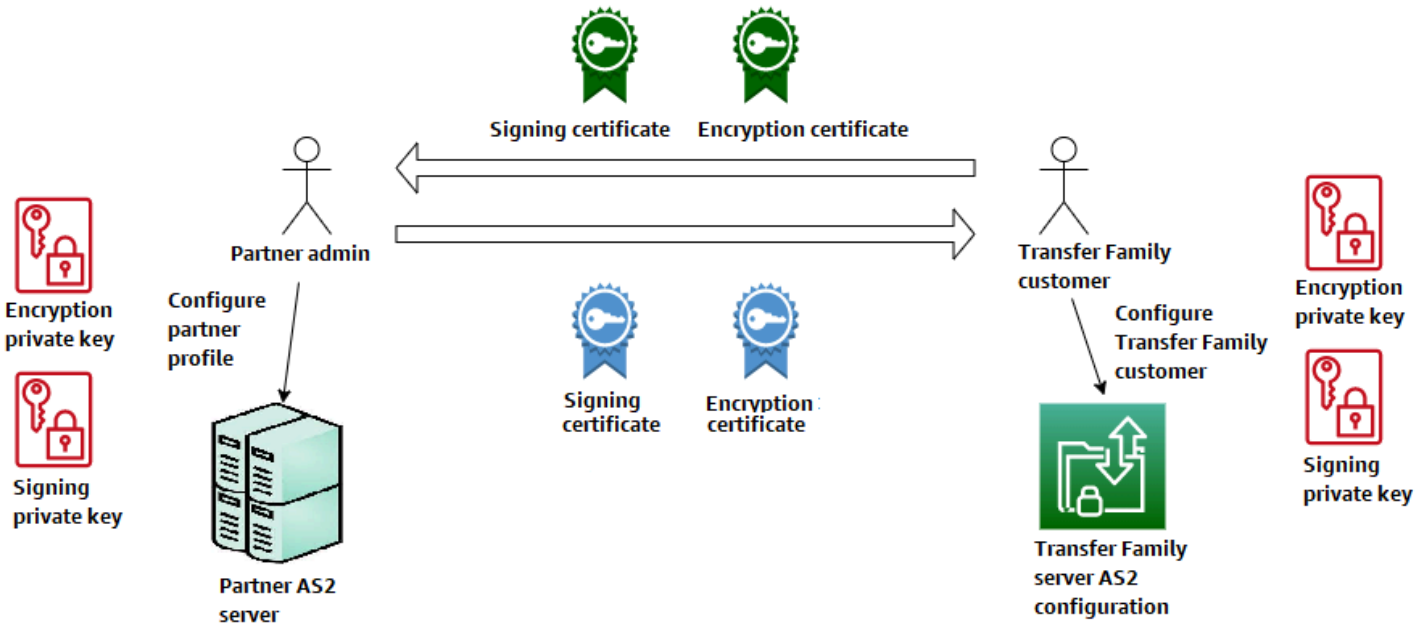
> **Note**
>
> Gli endpoint del server HTTPS AS2 non sono attualmente supportati. La risoluzione del TLS è attualmente responsabilità del cliente.

Per una step-by-step procedura dettagliata sulla configurazione di una configurazione dell'Applicability Statement 2 (AS2), consulta il tutorial,. Configurazione di una configurazione AS2

Argomenti

Casi d'uso di AS2

Se sei un AWS Transfer Family cliente che desidera scambiare file con un partner che dispone di un server AS2 configurato, la parte più complessa della configurazione prevede la generazione di una coppia di chiavi pubblica-privata per la crittografia e un'altra per la firma e lo scambio delle chiavi pubbliche con il partner.



Considerate le seguenti varianti per l'utilizzo con AWS Transfer Family AS2.

> **Note**
>
> Il partner commerciale è il partner associato a quel profilo di partner.
> Tutte le menzioni di MDN nella tabella seguente presuppongono mDNS firmati.

Casi d'uso di AS2

Casi d'uso solo in entrata

- Trasferisci messaggi AS2 crittografati da un partner commerciale a un server Transfer Family.

  In questo caso, esegui queste operazioni:

  1. Crea profili per te e per il tuo partner commerciale.
  2. Crea un server Transfer Family che utilizzi il protocollo AS2.
  3. Crea un accordo e aggiungilo al tuo server.
  4. Importa un certificato con una chiave privata e aggiungilo al tuo profilo, quindi importa la chiave pubblica nel tuo profilo partner per la crittografia.
  5. Dopo aver ricevuto questi elementi, invia la chiave pubblica del certificato al tuo partner commerciale.

Ora il tuo partner può inviarti messaggi crittografati e tu puoi decrittografarli e archiviarli nel tuo bucket Amazon S3.

- Trasferisci messaggi AS2 crittografati da un partner commerciale a un server Transfer Family e aggiungi la firma.

  In questo scenario, stai ancora effettuando solo trasferimenti in entrata, ma ora vuoi che il tuo partner firmi i messaggi che invia. In questo caso, importa la chiave pubblica di firma del partner commerciale (come certificato di firma aggiunto al profilo del partner).
- Trasferisci messaggi AS2 crittografati da un partner commerciale a un server Transfer Family e aggiungi la firma e l'invio di una risposta MDN.

  In questo scenario, stai ancora effettuando solo trasferimenti in entrata, ma ora, oltre a ricevere payload firmati, il tuo partner commerciale desidera ricevere una risposta MDN firmata.

  1. Importa le tue chiavi di firma pubbliche e private (come certificato di firma sul tuo profilo).
  2. Invia la chiave di firma pubblica al tuo partner commerciale.

Casi d'uso solo in uscita

- Trasferisci messaggi AS2 crittografati da un server Transfer Family a un partner commerciale.

  Questo caso è simile al caso di utilizzo del solo trasferimento in entrata, tranne per il fatto che invece di aggiungere un accordo al server AS2, si crea un connettore. In questo caso, importi la chiave pubblica del tuo partner commerciale nel suo profilo.
- Trasferisci messaggi AS2 crittografati da un server Transfer Family a un partner commerciale e aggiungi la firma.

  Stai ancora effettuando solo trasferimenti in uscita, ma ora il tuo partner commerciale vuole che tu firmi il messaggio che gli invii.

  1. Importa la tua chiave privata di firma (come certificato di firma aggiunto al tuo profilo).
  2. Invia al tuo partner commerciale la tua chiave pubblica.
- Trasferisci messaggi AS2 crittografati da un server Transfer Family a un partner commerciale, aggiungi la firma e invia una risposta MDN.

  Stai ancora effettuando solo trasferimenti in uscita, ma ora, oltre a inviare payload firmati, desideri ricevere una risposta MDN firmata dal tuo partner commerciale.

  1. Il tuo partner commerciale ti invia la sua chiave di firma pubblica.
  2. Importa la chiave pubblica del tuo partner commerciale (come certificato di firma aggiunto al tuo profilo di partner).

Casi d'uso in entrata e in uscita

- Trasferisci messaggi AS2 crittografati in entrambe le direzioni tra un server Transfer Family e un partner commerciale.

  In questo caso, esegui queste operazioni:

  1. Crea profili per te e per il tuo partner commerciale.
  2. Crea un server Transfer Family che utilizzi il protocollo AS2.
  3. Crea un accordo e aggiungilo al tuo server.
  4. Crea un connettore.
  5. Importa un certificato con una chiave privata e aggiungilo al tuo profilo, quindi importa la chiave pubblica nel tuo profilo partner per la crittografia.
  6. Ricevi una chiave pubblica dal tuo partner commerciale e aggiungila al suo profilo per la crittografia.
  7. Dopo aver ricevuto questi elementi, invia la chiave pubblica del certificato al tuo partner commerciale.

  Ora tu e il tuo partner commerciale potete scambiarvi messaggi crittografati ed entrambi potete decrittografarli. Puoi archiviare i messaggi che ricevi nel tuo bucket Amazon S3 e il tuo partner può decrittografare e archiviare i messaggi che gli invii.
- Trasferisci messaggi AS2 crittografati in entrambe le direzioni tra un server Transfer Family e un partner commerciale e aggiungi la firma.

  Ora tu e il tuo partner volete messaggi firmati.

  1. Importa la tua chiave privata per la firma (come certificato di firma aggiunto al tuo profilo).
  2. Invia al tuo partner commerciale la tua chiave pubblica.
  3. Importa la chiave pubblica per la firma del tuo partner commerciale e aggiungila al suo profilo.
- Trasferisci messaggi AS2 crittografati in entrambe le direzioni tra un server Transfer Family e un partner commerciale, aggiungi la firma e invia una risposta MDN.

  Ora vuoi scambiare payload firmati e sia tu che il tuo partner commerciale desiderate risposte MDN.

  1. Il tuo partner commerciale ti invia la sua chiave di firma pubblica.
  2. Importa la chiave pubblica del tuo partner commerciale (come certificato di firma sul tuo profilo di partner).

3. Invia la tua chiave pubblica al tuo partner commerciale.

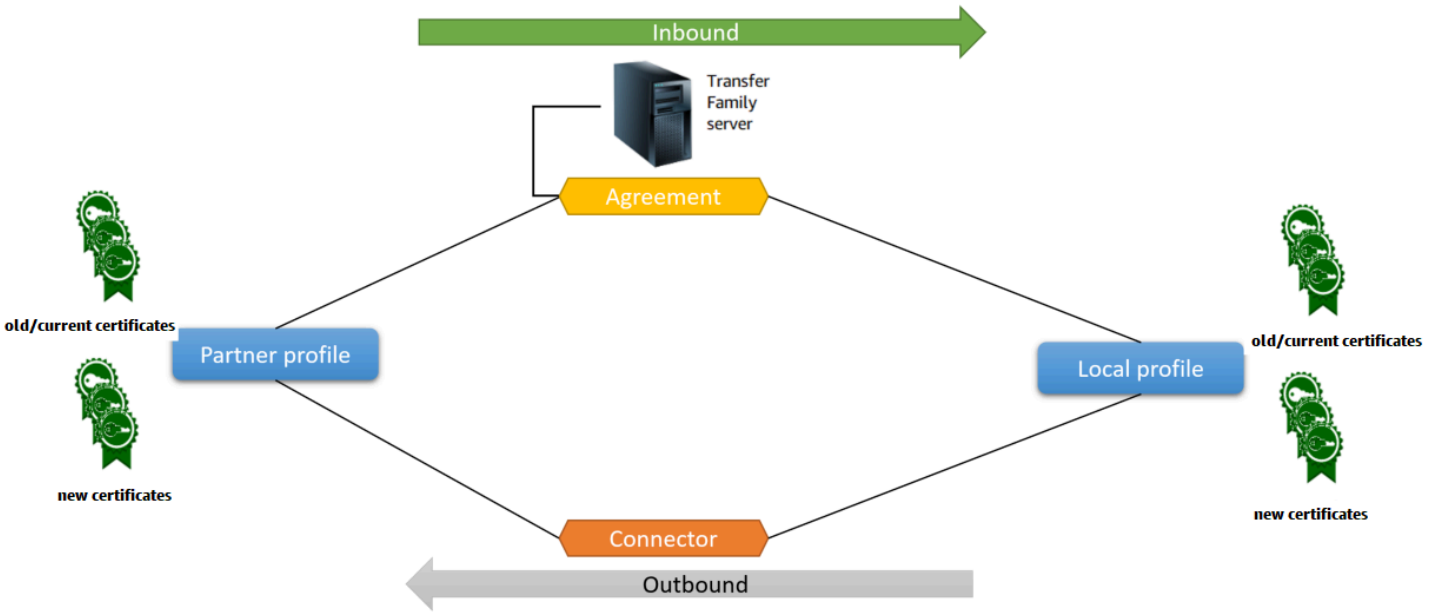
Configurazione di AS2

Per creare un server compatibile con AS2, è necessario specificare anche i seguenti componenti:

- Accordi: gli accordi bilaterali con i partner commerciali, o partnership, definiscono la relazione tra le due parti che si scambiano messaggi (file). Per definire un accordo, Transfer Family combina informazioni su server, profilo locale, profilo partner e certificato. I processi Transfer Family AS2-Inbound utilizzano accordi.
- Certificati: i certificati a chiave pubblica (X.509) vengono utilizzati nelle comunicazioni AS2 per la crittografia e la verifica dei messaggi. I certificati vengono utilizzati anche per gli endpoint dei connettori.
- Profili locali e profili partner: un profilo locale definisce l'organizzazione o il «partito» locale (server Transfer Family abilitato per AS2). Allo stesso modo, un profilo partner definisce l'organizzazione del partner remoto, esterna a Transfer Family.

Sebbene non sia richiesto per tutti i server compatibili con AS2, per i trasferimenti in uscita è necessario un connettore. Un connettore acquisisce i parametri per una connessione in uscita. Il connettore è necessario per inviare file a un server esterno, non AWS al server, del cliente.

Il diagramma seguente mostra la relazione tra gli oggetti AS2 coinvolti nei processi in entrata e in uscita.



Per un end-to-end esempio di configurazione AS2, vedere. Configurazione di una configurazione AS2

Argomenti

- Creare un server AS2 utilizzando la console Transfer Family
- Usa un modello per creare uno stack demo Transfer Family AS2
- Configurazioni e quote AS2
- Caratteristiche e funzionalità di AS2

Creare un server AS2 utilizzando la console Transfer Family

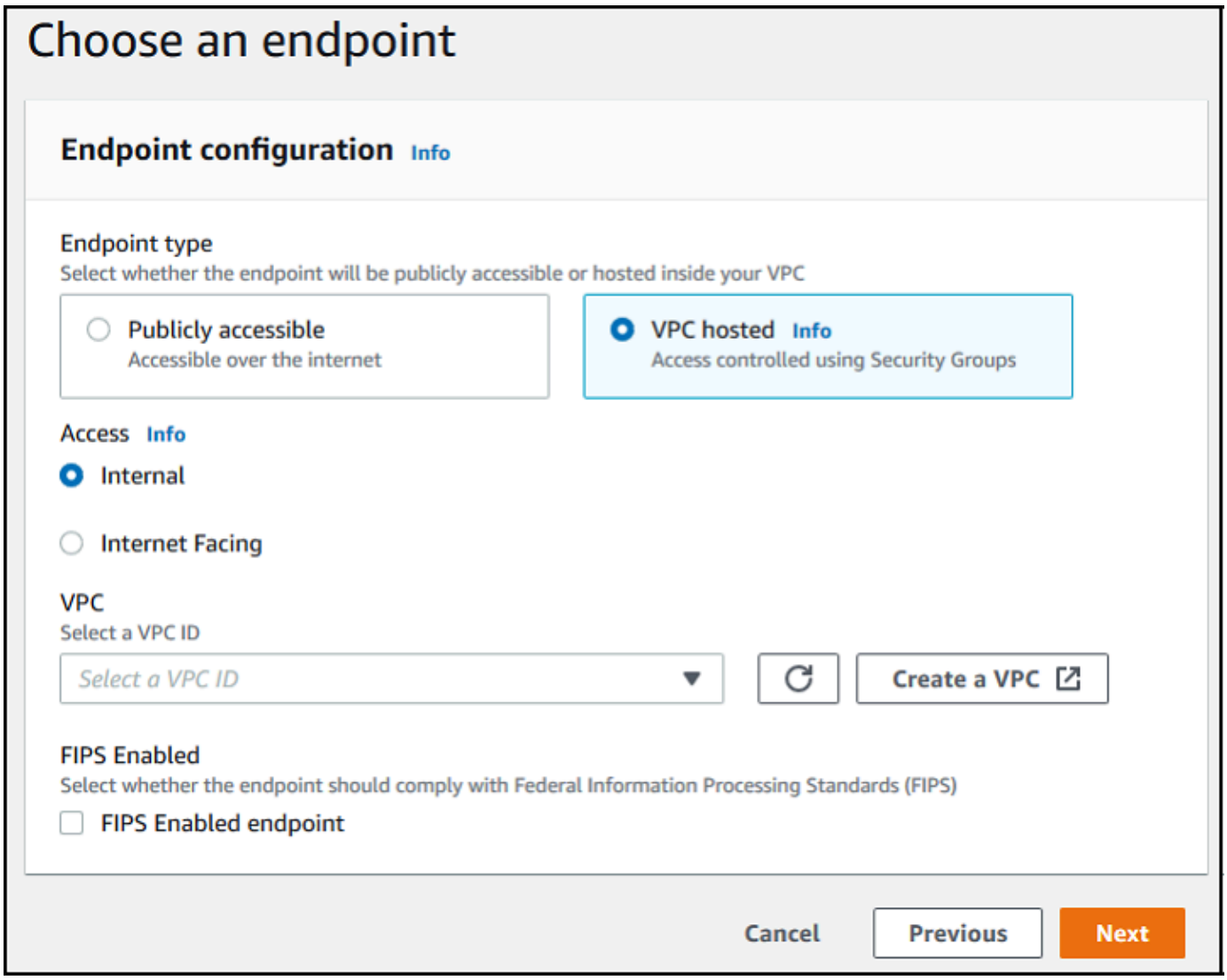
Questa procedura spiega come creare un server compatibile con AS2 utilizzando la console Transfer Family. Se AWS CLI invece desideri utilizzare il, consulta. the section called “Fase 2: Creare un server Transfer Family che utilizzi il protocollo AS2”

Per creare un server compatibile con AS2

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server, quindi scegli Crea server.
3. Nella pagina Scegli i protocolli, seleziona AS2 (Dichiarazione di applicabilità 2), quindi scegli Avanti.
4. Nella pagina Scegli un provider di identità, scegli Avanti.

> **Note**
>
> Per AS2, non puoi scegliere un provider di identità perché l'autenticazione di base non è supportata per il protocollo AS2. Al contrario, puoi controllare l'accesso tramite gruppi di sicurezza del cloud privato virtuale (VPC).

5. Nella pagina Scegli un endpoint, procedi come segue:



a. Per il tipo di endpoint, scegli VPC ospitato per ospitare l'endpoint del tuo server. Per informazioni sulla configurazione dell'endpoint ospitato da VPC, consulta. Crea un server in un cloud privato virtuale

> **Note**
>
> Gli endpoint accessibili al pubblico non sono supportati per il protocollo AS2. Per rendere il tuo endpoint VPC accessibile su Internet, scegli Internet Facing in Access, quindi fornisci i tuoi indirizzi IP elastici.

b. Per Access, scegli una delle seguenti opzioni:

- Interno: scegli questa opzione per fornire l'accesso dall'interno dei tuoi ambienti VPC e connessi a VPC, ad esempio un data center locale tramite VPN. AWS Direct Connect
- Connessione Internet: scegli questa opzione per fornire l'accesso tramite Internet e dall'interno dei tuoi ambienti VPC e connessi a VPC, come un data center locale o una VPN. AWS Direct Connect

  Se scegli Internet Facing, fornisci i tuoi indirizzi IP elastici quando richiesto.

c. Per VPC, scegli un VPC esistente o scegli Crea VPC per creare un nuovo VPC.

d. Per FIPS Enabled, mantieni deselezionata la casella di controllo FIPS Enabled endpoint.

> **Note**
>
> Gli endpoint compatibili con FIPS non sono supportati per il protocollo AS2.

e. Seleziona Successivo.

6. Nella pagina Scegli un dominio, scegli Amazon S3 per archiviare e accedere ai tuoi file come oggetti utilizzando il protocollo selezionato.

   Seleziona Successivo.

7. Nella pagina Configura dettagli aggiuntivi, scegli le impostazioni di cui hai bisogno.

> **Note**
>
> Se state configurando altri protocolli insieme ad AS2, verranno applicate tutte le impostazioni di dettaglio aggiuntive. Tuttavia, per il protocollo AS2, le uniche impostazioni applicabili sono quelle nelle sezioni di CloudWatch registrazione e Tag.

Anche se l'impostazione di un ruolo CloudWatch di registrazione è facoltativa, consigliamo vivamente di configurarla in modo da poter visualizzare lo stato dei messaggi e risolvere i problemi di configurazione.

8. Nella pagina Rivedi e crea, rivedi le tue scelte per assicurarti che siano corrette.

   - Se desideri modificare una qualsiasi delle tue impostazioni, scegli Modifica accanto al passaggio che desideri modificare.

     > **Note**
     >
     > Se modifichi un passaggio, ti consigliamo di rivedere ogni passaggio successivo a quello che hai scelto di modificare.

   - Se non hai apportato modifiche, scegli Crea server per creare il tuo server. Viene visualizzata la pagina Servers (Server), mostrata di seguito, in cui è elencato il nuovo server.

     Possono essere necessari alcuni minuti prima che lo stato del nuovo server passi a Online. A questo punto, il server può eseguire operazioni sui file per gli utenti.

Usa un modello per creare uno stack demo Transfer Family AS2

Forniamo un AWS CloudFormation modello autonomo per creare rapidamente un server Transfer Family abilitato per AS2. Il modello configura il server con un endpoint Amazon VPC pubblico, certificati, profili locali e partner, un accordo e un connettore.

Prima di utilizzare questo modello, tieni presente quanto segue:

- Se crei uno stack da questo modello, ti verranno fatturate le AWS risorse utilizzate.
- Il modello crea più certificati e li inserisce AWS Secrets Manager per archiviarli in modo sicuro. Puoi eliminare questi certificati da Secrets Manager se lo desideri, perché l'utilizzo di questo servizio ti viene addebitato. L'eliminazione di questi certificati in Secrets Manager non li elimina dal server Transfer Family. Pertanto, la funzionalità dello stack demo non è influenzata. Tuttavia, per i certificati che utilizzerai con un server AS2 di produzione, potresti voler utilizzare Secrets Manager per gestire e ruotare periodicamente i certificati archiviati.
- Ti consigliamo di utilizzare il modello solo come base e principalmente a scopo dimostrativo. Se desideri utilizzare questo stack dimostrativo in produzione, ti consigliamo di modificare il codice

YAML del modello per creare uno stack più robusto. Ad esempio, create certificati a livello di produzione e create una AWS Lambda funzione da utilizzare in produzione.

Per creare un server Transfer Family abilitato per AS2 da un modello CloudFormation

1. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
2. Nel riquadro di navigazione a sinistra, selezionare Stacks (Stack).
3. Scegliere Create stack (Crea stack), quindi scegliere Con nuove risorse (standard).
4. Nella sezione Prerequisito - Prepara il modello, scegli Il modello è pronto.
5. Copia questo link, modello demo AS2, e incollalo nel campo URL di Amazon S3.
6. Seleziona Successivo.
7. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack, quindi specifica i seguenti parametri:
   - In AS2, inserisci i valori per Local AS2 ID e Partner AS2 ID, oppure accetta i valori predefiniti e, rispettivamente. `local` `partner`
   - In Rete, inserite un valore per Security group ingress CIDR IP oppure accettate quello predefinito,. `0.0.0.0/0`

     > **Note**
     >
     > Questo valore, in formato CIDR, specifica quali indirizzi IP sono consentiti per il traffico in entrata verso il server AS2. Il valore predefinito,`0.0.0.0/0`, consente tutti gli indirizzi IP.

   - In Generale, immettete un valore per Prefisso o accettate quello predefinito,`transfer-as2`. Questo prefisso viene inserito prima dei nomi di risorse creati dallo stack. Ad esempio, se utilizzi il prefisso predefinito, il tuo bucket Amazon S3 viene denominato. `transfer-as2-`*`TransferS3BucketName`*
8. Seleziona Successivo. Nella pagina Configura le opzioni dello stack, scegli di nuovo Avanti.
9. Controlla i dettagli dello stack che stai creando, quindi scegli Crea stack.

> **Note**
>
> Nella parte inferiore della pagina, in Capacità, devi riconoscere che AWS CloudFormation potrebbe creare risorse AWS Identity and Access Management (IAM).

Dopo aver creato lo stack, puoi inviare un messaggio AS2 di prova dal server partner al tuo server Transfer Family locale utilizzando AWS Command Line Interface ()AWS CLI. Un AWS CLI comando di esempio per l'invio di un messaggio di prova viene creato insieme a tutte le altre risorse dello stack.

Per utilizzare questo comando di esempio, vai alla scheda Outputs dello stack e copia 2Command. TransferExampleAs È quindi possibile eseguire il comando utilizzando il. AWS CLI Se non l'hai già installato AWS CLI, consulta Installazione o aggiornamento della versione più recente di AWS CLI nella Guida per l'AWS Command Line Interface utente.

Il comando di esempio ha il seguente 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**
>
> La versione in uso di questo comando contiene i valori effettivi *TransferConnectorId* delle risorse *TransferS3BucketName* e dello stack.

Questo comando di esempio è costituito da due comandi separati concatenati utilizzando la && stringa.

Il primo comando crea un nuovo file di testo vuoto nel bucket:

```
aws s3api put-object --bucket TransferS3BucketName --key test.txt
```

Quindi, il secondo comando utilizza il connettore per inviare il file dal profilo partner al profilo locale. Il server Transfer Family dispone di un accordo che consente al profilo locale di accettare messaggi dal profilo partner.

```
aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId
 --send-file-paths /TransferS3BucketName/test.txt
```

Dopo aver eseguito il comando, puoi accedere al tuo bucket Amazon S3 (*TransferS3BucketName*) e visualizzarne il contenuto. Se il comando ha esito positivo, dovresti vedere i seguenti oggetti nel tuo bucket:

- `processed/`— Questa cartella contiene un file JSON che descrive il file trasferito e la risposta MDN.
- `processing/`— Questa cartella contiene temporaneamente i file durante l'elaborazione, ma una volta completato il trasferimento, questa cartella dovrebbe essere vuota.
- *server-id*`/`— Questa cartella è denominata in base all'ID del server Transfer Family. Contiene `from-`*partner* (questa cartella ha un nome dinamico, in base all'ID AS2 del partner), che a sua volta contiene `failed/processed/`, e `processing/` cartelle. La `/`*server-id*`/from-`*partner*`/processed/` cartella contiene una copia del file di testo trasferito e i corrispondenti file JSON e MDN.
- `test.txt`— Questo oggetto è il file (vuoto) che è stato trasferito.

Configurazioni e quote AS2

Questo argomento descrive le configurazioni, le caratteristiche e le funzionalità supportate per i trasferimenti che utilizzano il protocollo Applicability Statement 2 (AS2), inclusi i codici e i digest accettati. Questa sezione descrive anche i limiti e i problemi noti per i trasferimenti AS2.

Argomenti

Configurazioni supportate da AS2

Firma, crittografia, compressione, MDN

Sia per i trasferimenti in entrata che per quelli in uscita, i seguenti elementi sono obbligatori o facoltativi:

- Crittografia: obbligatoria (per il trasporto HTTP, che è l'unico metodo di trasporto attualmente supportato). I messaggi non crittografati vengono accettati solo se inoltrati da un proxy con

terminazione TLS come un Application Load Balancer (ALB) e l'intestazione è presente. `X-Forwarded-Proto: https`

- Firma: facoltativa
- Compressione: opzionale (l'unico algoritmo di compressione attualmente supportato è ZLIB)
- Avviso di disposizione dei messaggi (MDN): opzionale

Cifre

I seguenti codici sono supportati per i trasferimenti in entrata e in uscita:

- AES128_CBC
- AES192_CBC
- AES256_CBC
- 3DES (solo per compatibilità con le versioni precedenti)

Digerisce

Sono supportati i seguenti digest:

- Firma in entrata e MDN: SHA1, SHA256, SHA384, SHA512
- Firma in uscita e MDN: SHA1, SHA256, SHA384, SHA512

MDN

Per le risposte MDN, sono supportati alcuni tipi, come segue:

- Trasferimenti in entrata: sincroni e asincroni
- Trasferimenti in uscita: solo sincroni
- Simple Mail Transfer Protocol (SMTP) (email MDN) — Non supportato

Trasporti

- Trasferimenti in entrata: HTTP è l'unico trasporto attualmente supportato ed è necessario specificarlo in modo esplicito.

> **Note**
>
> Se devi utilizzare HTTPS per i trasferimenti in entrata, puoi terminare TLS su un Application Load Balancer o un Network Load Balancer. Questo è descritto in. Ricevi messaggi AS2 tramite HTTPS

- Trasferimenti in uscita: se si fornisce un URL HTTP, è necessario specificare anche un algoritmo di crittografia. Se fornisci un URL HTTPS, hai la possibilità di specificare NONE per il tuo algoritmo di crittografia.

Quote e limitazioni AS2

Questa sezione descrive le quote e le limitazioni per AS2

Argomenti

- Quote AS2
- Quote per la gestione dei segreti
- Limiti noti

Quote AS2

Le seguenti quote sono valide per i trasferimenti di file AS2. Per richiedere un aumento di una quota regolabile, consulta le Servizio AWS quote nel. Riferimenti generali di AWS

Quote AS2

Nome	Predefinita	Adattabile
Numero massimo di file in entrata ricevuti al secondo	100	No
Numero massimo di file in uscita inviati al secondo	100	No
Numero massimo di file in ingresso simultanei	400	No

Nome	Predefinita	Adattabile
Numero massimo di file in uscita simultanei	400	No
Dimensione massima del file in entrata (non compresso)	1 GB	No
Dimensione massima del file in uscita (non compresso)	1 GB	No
Numero massimo di file per richiesta in uscita	10	No
Numero massimo di richieste in uscita al secondo	100	No
Numero massimo di richieste in entrata al secondo	100	No
Larghezza di banda massima in uscita per account (le richieste SFTP e AS2 in uscita contribuiscono entrambe a questo valore)	50 MB al secondo	No
Numero massimo di accordi per server	100	Sì
Numero massimo di connettori per account (i connettori SFTP e AS2 contribuiscono entrambi a questo limite)	100	Sì
Numero massimo di certificati per profilo partner	10	No
Numero massimo di certificati per account	1000	Sì

Nome	Predefinita	Adattabile
Numero massimo di profili partner per account	1000	Sì

Quote per la gestione dei segreti

AWS Transfer Family effettua chiamate per AWS Secrets Manager conto dei clienti AS2 che utilizzano l'autenticazione di base. Inoltre Secrets Manager effettua chiamate a AWS KMS.

> **Note**
>
> Queste quote non sono specifiche per l'uso dei segreti per Transfer Family: sono condivise tra tutti i servizi di Transfer Family. Account AWS

Per Secrets Manager`GetSecretValue`, la quota che si applica è la frequenza combinata delle richieste DescribeSecret e delle GetSecretValue API, come descritto in AWS Secrets Manager quote.

Secrets Manager **`GetSecretValue`**

Nome	Valore	Descrizione
Frequenza combinata di richieste GetSecretValue API DescribeSecret e frequenza	Ogni regione supportata: 10.000 al secondo	Il numero massimo di transazioni al secondo DescribeSecret e le richieste GetSecretValue API combinate.

Infatti AWS KMS, si applicano le seguenti quote. `Decrypt` Per i dettagli, consulta Richiedere quote per ogni operazione API AWS KMS

AWS KMS **`Decrypt`**

Nome quota	Valore predefinito (richieste al secondo)
Frequenza della richiesta di operazioni crittografiche (simmetriche)	Queste quote condivise variano in base al tipo Regione AWS e al tipo di AWS KMS chiave

Nome quota	Valore predefinito (richieste al secondo)

	utilizzata nella richiesta. Ogni quota è calcolata separatamente.
	• 5.500 (condiviso)
	• 10.000 (condiviso) nelle regioni seguenti:
	  • Stati Uniti orientali (Ohio), us-east-2
	  • Asia Pacifico (Singapore), ap-southeast-1
	  • Asia Pacifico (Sydney), ap-southeast-2
	  • Asia Pacifico (Tokyo), ap-northeast-1
	  • Europa (Francoforte), eu-central-1
	  • Europa (Londra), eu-west-2
	• 50.000 (condiviso) nelle Regioni seguenti:
	  • Stati Uniti orientali (Virginia settentrionale), us-east-1
	  • Stati Uniti occidentali (Oregon), us-west-2
	  • Europa (Irlanda), eu-west-1

Quote di richiesta per l'archivio delle chiavi personalizzate **Note** Questa quota si applica solo se si utilizza un archivio di chiavi esterno.	Le quote di richieste di archiviazione chiavi personalizzate vengono calcolate separatam ente per ogni archivio chiavi personalizzato. • 1.800 (condivise) per ogni archivio di chiavi AWS CloudHSM • 1.800 (condiviso) per ogni archivio delle chiavi esterne

Limiti noti

- Il keep-alive TCP sul lato server non è supportato. La connessione scade dopo 350 secondi di inattività, a meno che il client non invii pacchetti keep-alive.
- Affinché un contratto attivo venga accettato dal servizio e venga visualizzato nei CloudWatch log di Amazon, i messaggi devono contenere intestazioni AS2 valide.

- Il server da cui riceve i messaggi AWS Transfer Family per AS2 deve supportare l'attributo di protezione dell'algoritmo Cryptographic Message Syntax (CMS) per la convalida delle firme dei messaggi, come definito nella RFC 6211. Questo attributo non è supportato in alcuni prodotti IBM Sterling precedenti.
- Gli ID di messaggio duplicati generano un messaggio elaborato/avviso: documento duplicato.
- La lunghezza della chiave per i certificati AS2 deve essere di almeno 2048 bit e al massimo di 4096.
- Quando si inviano messaggi AS2 o MDN asincroni all'endpoint HTTPS di un partner commerciale, i messaggi o gli mDNS devono utilizzare un certificato SSL valido firmato da un'autorità di certificazione (CA) pubblicamente affidabile. I certificati autofirmati sono attualmente supportati solo per i trasferimenti in uscita.
- L'endpoint deve supportare il protocollo TLS versione 1.2 e un algoritmo crittografico consentito dalla politica di sicurezza (come descritto in). Politiche di sicurezza per AWS Transfer Family i server
- Al momento non sono supportati più allegati e messaggi di scambio di certificati (CEM) di AS2 versione 1.2.
- L'autenticazione di base è attualmente supportata solo per i messaggi in uscita.

Caratteristiche e funzionalità di AS2

Le tabelle seguenti elencano le caratteristiche e le funzionalità disponibili per le risorse Transfer Family che utilizzano AS2.

Caratteristiche di AS2

Transfer Family offre le seguenti funzionalità per AS2.

Funzionalità	Supportato da AWS Transfer Family
Certificazione Drummond	Sì
AWS CloudFormation supporto	Sì
CloudWatchMetriche Amazon	Sì
Algoritmi crittografici SHA-2	Sì

Funzionalità	Supportato da AWS Transfer Family
Supporto per Amazon S3	Sì
Support per Amazon EFS	No
Messaggi pianificati	Sì [1]
AWS Transfer Family Flussi di lavoro gestiti	No
Messaggistica per lo scambio di certificati (CEM)	No
TLS reciproco (mTLS)	No
Support per certificati autofirmati	Sì

1. Messaggi pianificati in uscita disponibili tramite AWS Lambda le funzioni di pianificazione tramite Amazon EventBridge

Funzionalità di invio e ricezione AS2

La tabella seguente fornisce un elenco delle funzionalità di invio e ricezione di AWS Transfer Family AS2.

Funzionalità	In entrata: ricezione tramite server	In uscita: invio con connettore
Trasporto crittografato TLS (HTTPS)	Sì 1	Sì
Trasporto non TLS (HTTP)	Sì	Sì 2
MDN sincrono	Sì	Sì
Compressione dei messaggi	Sì	Sì
MDN asincrono	Sì	No
Indirizzo IP statico	Sì	Sì

Funzionalità	In entrata: ricezione tramite server	In uscita: invio con connettore
Porta il tuo indirizzo IP	Sì	No
Più file allegati	No	No
Autenticazione di base	No	Sì
Riavvio AS2	Non applicabile	No
Affidabilità AS2	No	No
Oggetto personalizzato per messaggio	Non applicabile	No

1. Trasporto crittografato TLS in entrata disponibile con Network Load Balancer (NLB)

2. Trasporto non TLS in uscita disponibile solo quando la crittografia è abilitata

Configura i connettori AS2

Lo scopo di un connettore è stabilire una relazione tra i partner commerciali per i trasferimenti in uscita, inviando file AS2 da un server Transfer Family a una destinazione esterna di proprietà del partner. Per il connettore, si specifica la parte locale, il partner remoto e i relativi certificati (creando profili locali e partner).

Dopo aver installato un connettore, puoi trasferire le informazioni ai tuoi partner commerciali. A ciascun server AS2 vengono assegnati tre indirizzi IP statici. I connettori AS2 utilizzano questi indirizzi IP per inviare mDNS asincroni ai partner commerciali tramite AS2.

> **Note**
>
> La dimensione del messaggio ricevuto da un partner commerciale non corrisponderà alla dimensione dell'oggetto in Amazon S3. Questa discrepanza si verifica perché il messaggio AS2 avvolge il file in una busta prima dell'invio. Pertanto, la dimensione del file potrebbe aumentare, anche se il file viene inviato con compressione. Pertanto, assicurati che la

dimensione massima del file del partner commerciale sia maggiore della dimensione del file che stai inviando.

Crea un connettore AS2

Questa procedura spiega come creare connettori AS2 utilizzando la AWS Transfer Family console. Se AWS CLI invece desideri utilizzare il, consultathe section called “Passaggio 6: crea un connettore tra te e il tuo partner”.

Per creare un connettore AS2

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Connettori, quindi scegli Crea connettore.
3. Nella sezione Configurazione del connettore, specifica le seguenti informazioni:
   - URL: immetti l'URL per le connessioni in uscita.
   - Ruolo di accesso: scegli l'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) da utilizzare. Assicurati che questo ruolo fornisca l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta. Inoltre, assicurati che il ruolo fornisca l'accesso in lettura e scrittura alla directory principale dei file con cui intendi inviare`StartFileTransfer`.

     > **Note**
     >
     > Se utilizzi l'autenticazione di base per il connettore, il ruolo di accesso richiede l'`secretsmanager:GetSecretValue`autorizzazione per il segreto. Se il segreto viene crittografato utilizzando una chiave gestita dal cliente anziché l' Chiave gestita da AWS accesso AWS Secrets Manager, il ruolo necessita anche dell'`kms:Decrypt`autorizzazione per quella chiave. Se si assegna un nome al segreto con il prefisso`aws/transfer/`, è possibile aggiungere l'autorizzazione necessaria con un carattere jolly (`*`), come mostrato nell'esempio di autorizzazione a creare segreti.

   - Ruolo di registrazione (opzionale): scegli il ruolo IAM per il connettore da utilizzare per inviare eventi ai tuoi log. CloudWatch

4. Nella sezione di configurazione AS2, scegli i profili locali e partner, gli algoritmi di crittografia e firma e se comprimere le informazioni trasferite. Tieni presente quanto segue:

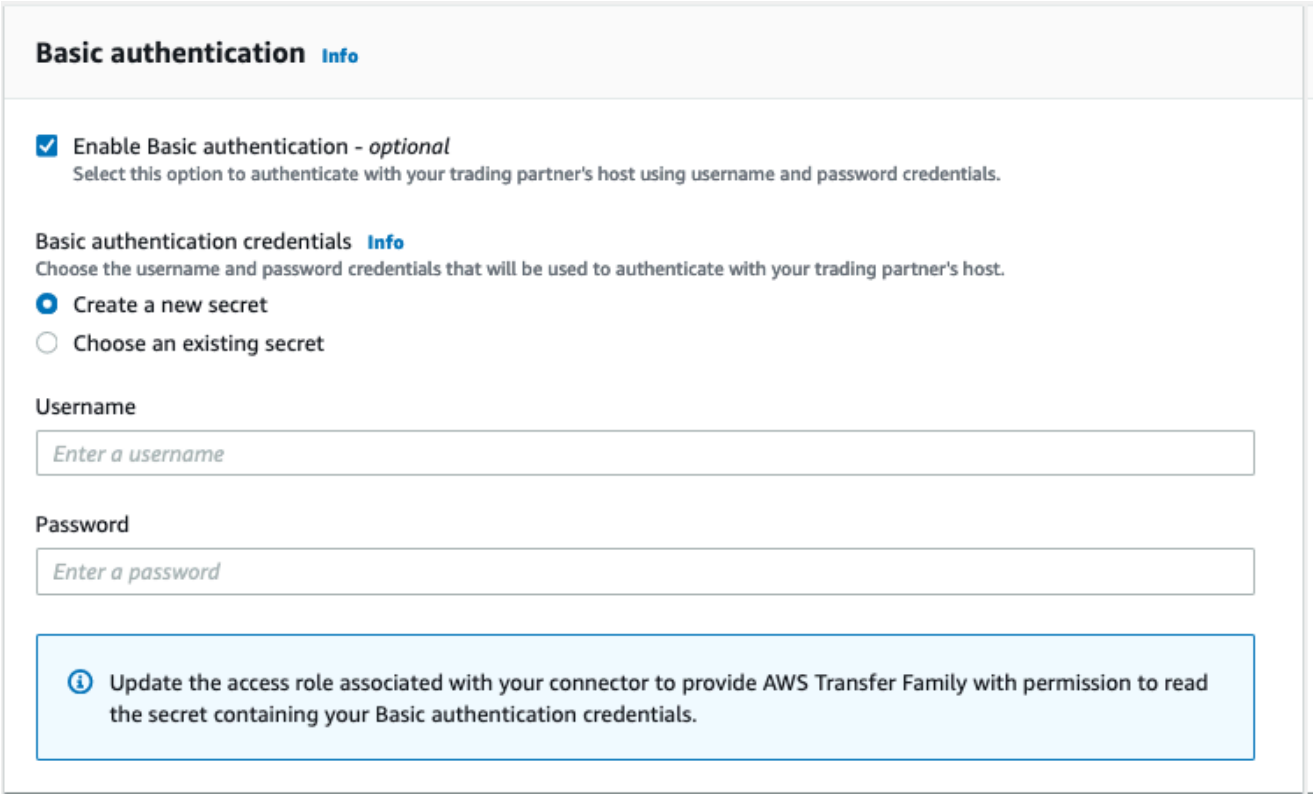
   - Per quanto riguarda l'algoritmo di crittografia, non scegliete `DES_EDE3_CBC` a meno che non dobbiate supportare un client legacy che lo richiede, in quanto si tratta di un algoritmo di crittografia debole.
   - L'oggetto viene utilizzato come attributo di intestazione `subject` HTTP nei messaggi AS2 inviati con il connettore.
   - Se scegli di creare un connettore senza un algoritmo di crittografia, devi specificare `HTTPS` come protocollo.

5. Nella sezione di configurazione MDN, specifica le seguenti informazioni:

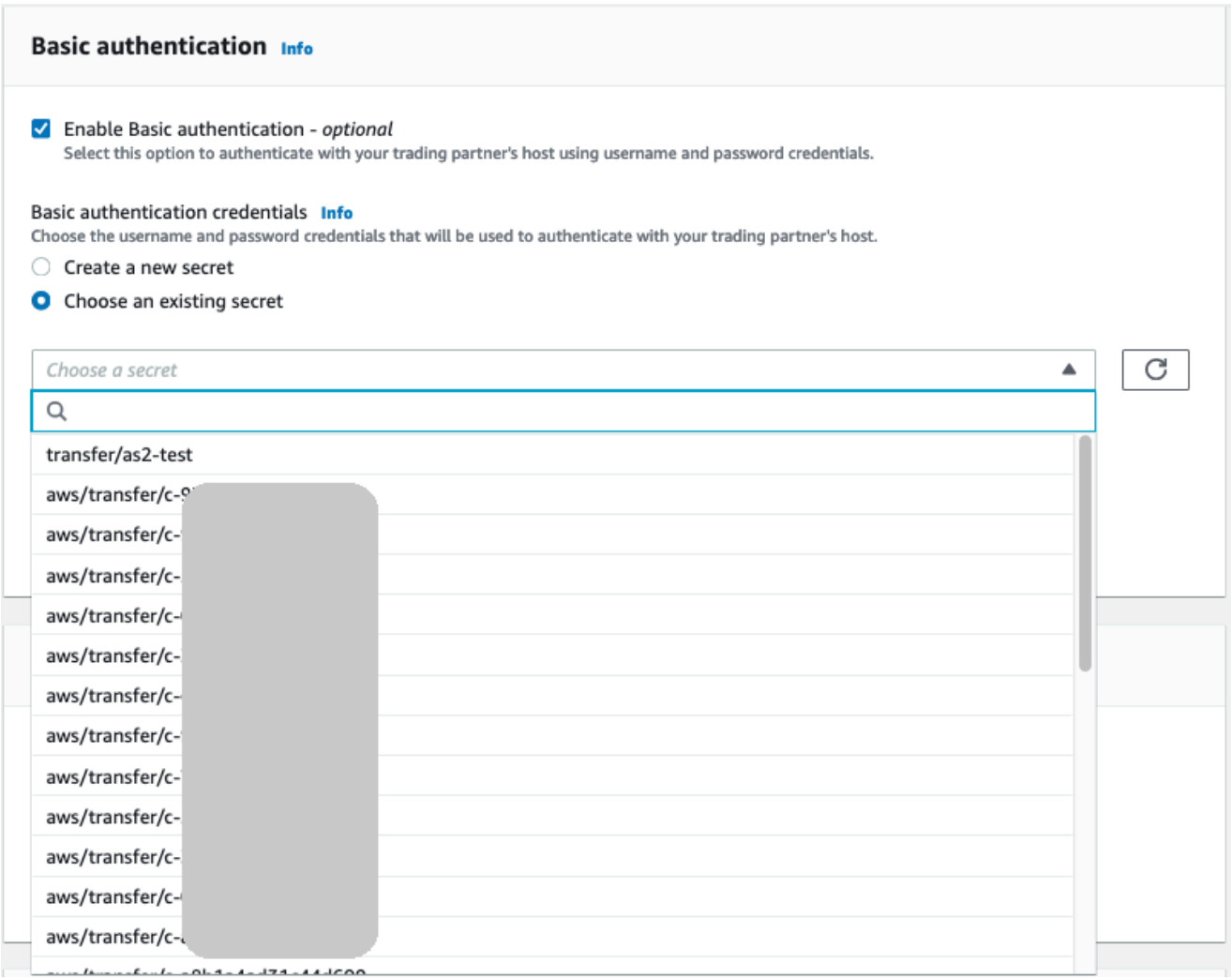
   - Richiedi MDN: hai la possibilità di richiedere al tuo partner commerciale di inviarti un MDN dopo che avrà ricevuto correttamente il tuo messaggio tramite AS2.
   - MDN firmato: hai la possibilità di richiedere la firma degli mDNS. Questa opzione è disponibile solo se hai selezionato Richiedi MDN.

6. Nella sezione Autenticazione di base, specifica le seguenti informazioni.

   - Per inviare credenziali di accesso insieme ai messaggi in uscita, seleziona Abilita l'autenticazione di base. Se non desideri inviare credenziali con messaggi in uscita, mantieni la casella di controllo Abilita autenticazione di base deselezionata.
   - Se utilizzi l'autenticazione, scegli o crea un segreto.
     - Per creare un nuovo segreto, scegli Crea un nuovo segreto, quindi inserisci un nome utente e una password. Queste credenziali devono corrispondere all'utente che si connette all'endpoint del partner.



- Per utilizzare un segreto esistente, scegli Scegli un segreto esistente, quindi scegli un segreto dal menu a discesa. Per i dettagli sulla creazione di un segreto formattato correttamente in Secrets Manager, vedereAbilita l'autenticazione di base per i connettori AS2.



7. Dopo aver confermato tutte le impostazioni, scegli Crea connettore per creare il connettore.

Viene visualizzata la pagina Connettori, con l'ID del nuovo connettore aggiunto all'elenco. Per visualizzare i dettagli dei connettori, consulta[Visualizza i dettagli del connettore AS2](#).

Algoritmi dei connettori AS2

Quando si crea un connettore AS2, al connettore vengono collegati i seguenti algoritmi di sicurezza.

Type	Algoritmo
Cifratura TLS	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Type	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

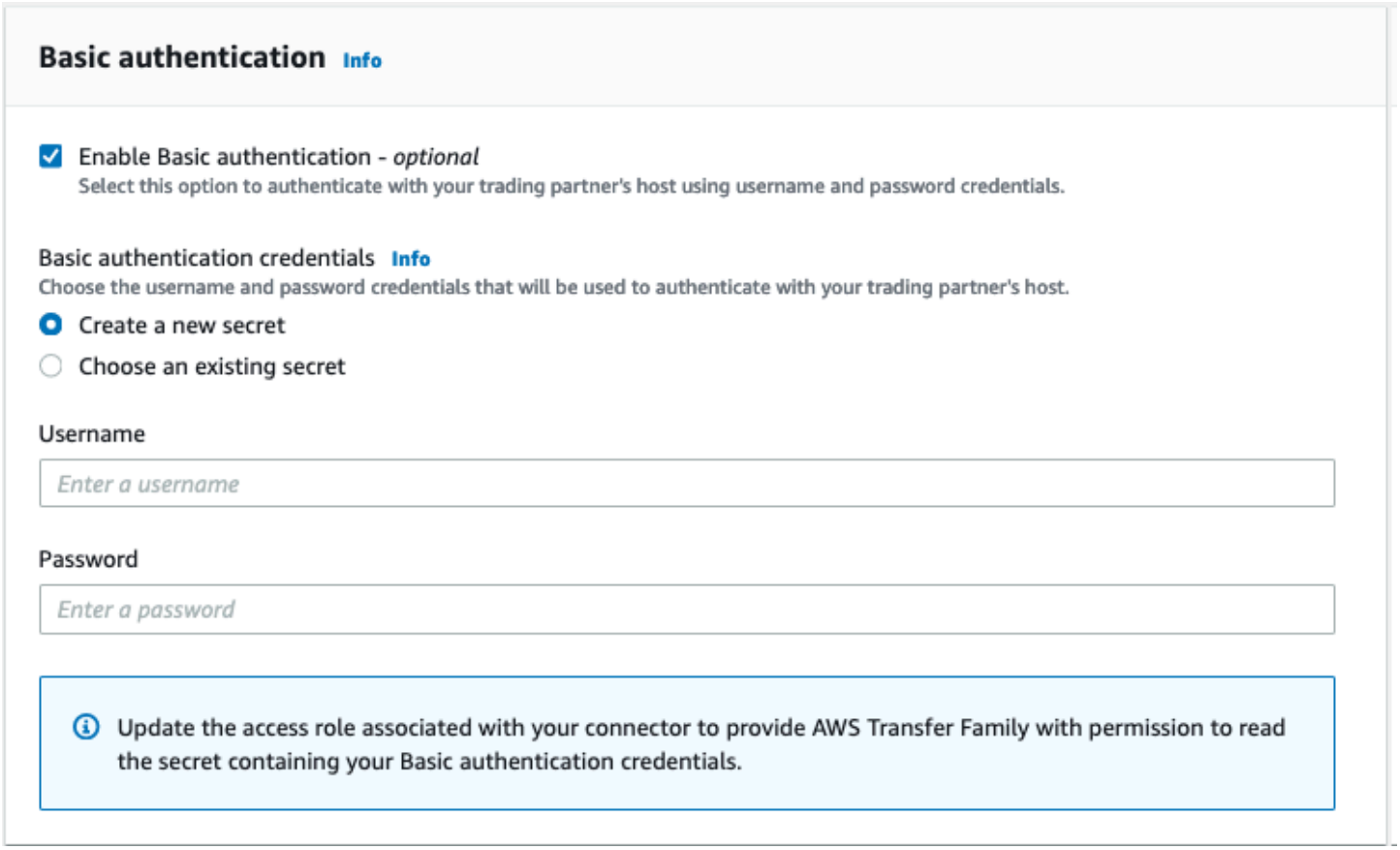
Autenticazione di base per connettori AS2

Quando crei o aggiorni un server Transfer Family che utilizza il protocollo AS2, puoi aggiungere l'autenticazione di base per i messaggi in uscita. A tale scopo, è necessario aggiungere informazioni di autenticazione a un connettore.

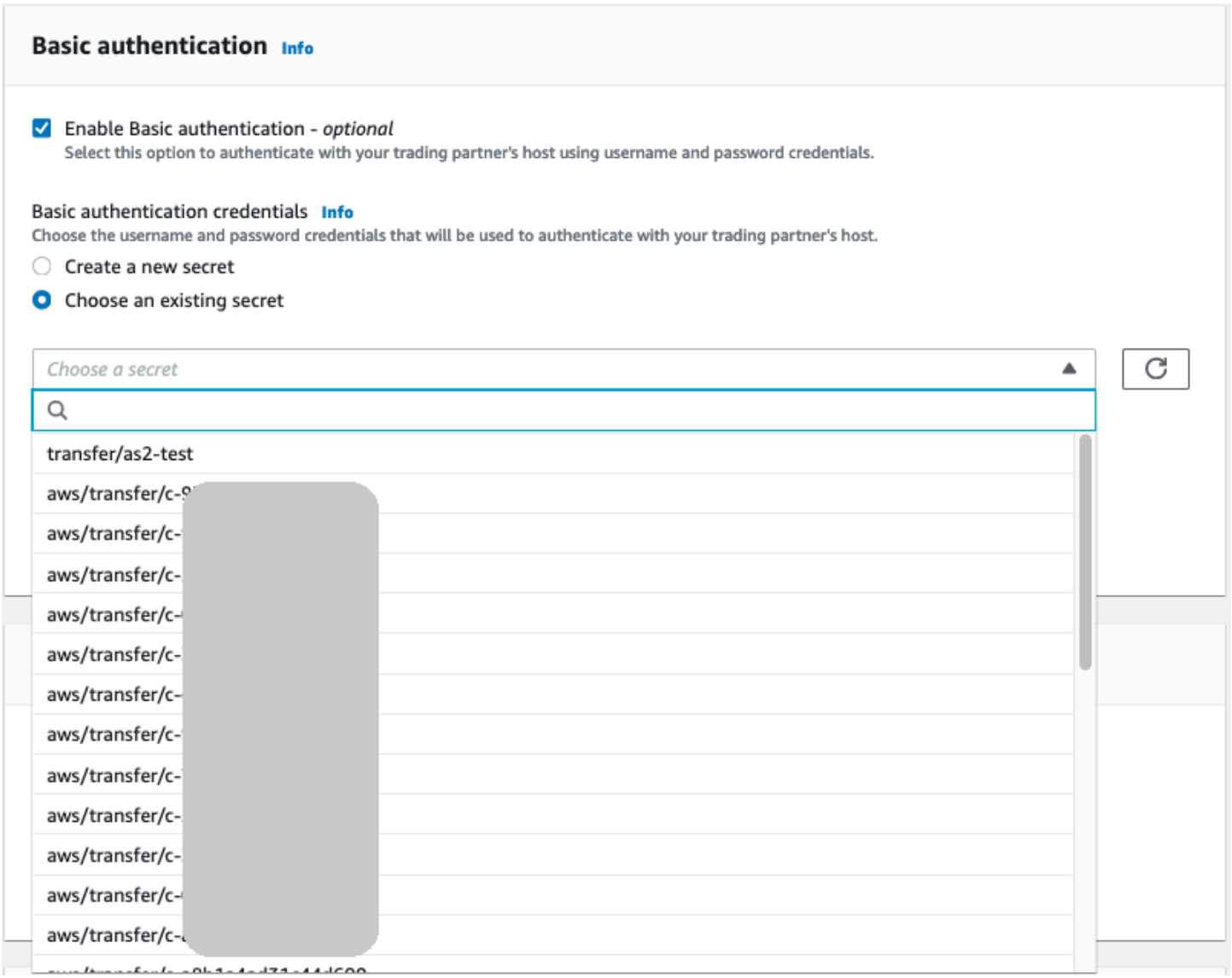
> **Note**
>
> L'autenticazione di base è disponibile solo se utilizzi HTTPS.

Per utilizzare l'autenticazione per il connettore, seleziona Abilita l'autenticazione di base nella sezione Autenticazione di base. Dopo aver abilitato l'autenticazione di base, puoi scegliere di creare un nuovo segreto o utilizzarne uno esistente. In entrambi i casi, le credenziali contenute nel segreto vengono inviate con messaggi in uscita che utilizzano questo connettore. Le credenziali devono corrispondere all'utente che sta tentando di connettersi all'endpoint remoto del partner commerciale.

La schermata seguente mostra l'opzione Abilita autenticazione di base selezionata e l'opzione Crea un nuovo segreto. Dopo aver effettuato queste scelte, puoi inserire un nome utente e una password per il segreto.



La schermata seguente mostra l'opzione Abilita l'autenticazione di base selezionata e l'opzione Scegli un segreto esistente. Il segreto deve essere nel formato corretto, come descritto in[Abilita l'autenticazione di base per i connettori AS2](#).



Abilita l'autenticazione di base per i connettori AS2

Quando abiliti l'autenticazione di base per i connettori AS2, puoi creare un nuovo segreto nella console Transfer Family oppure puoi usare un segreto creato in AWS Secrets Manager. In entrambi i casi, il tuo segreto viene archiviato in Secrets Manager.

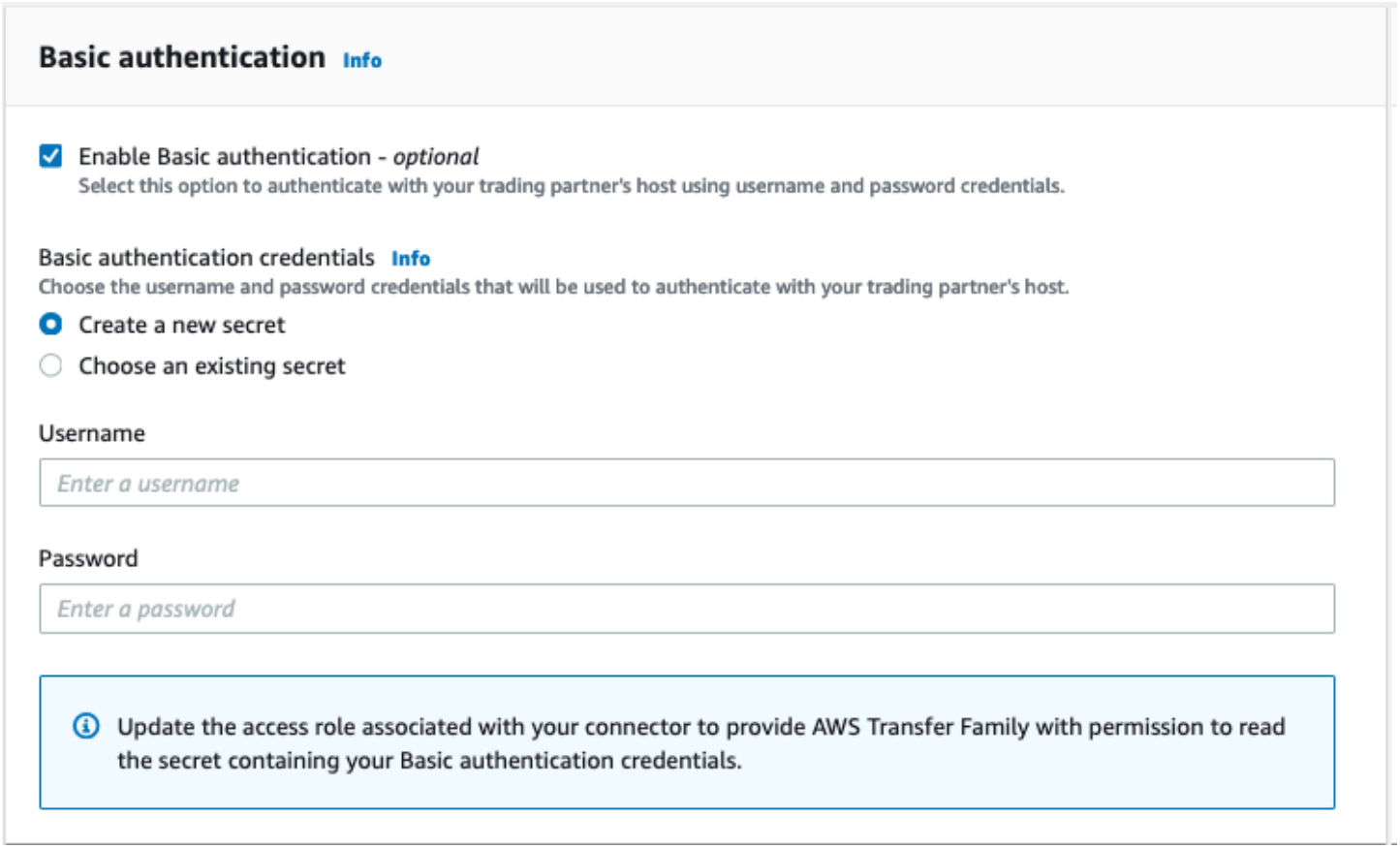
Argomenti

- Crea un nuovo segreto nella console
- Usa un segreto esistente
- Crea un segreto in AWS Secrets Manager

Crea un nuovo segreto nella console

Quando crei un connettore nella console, puoi creare un nuovo segreto.

Per creare un nuovo segreto, scegli Crea un nuovo segreto, quindi inserisci un nome utente e una password. Queste credenziali devono corrispondere all'utente che si connette all'endpoint del partner.

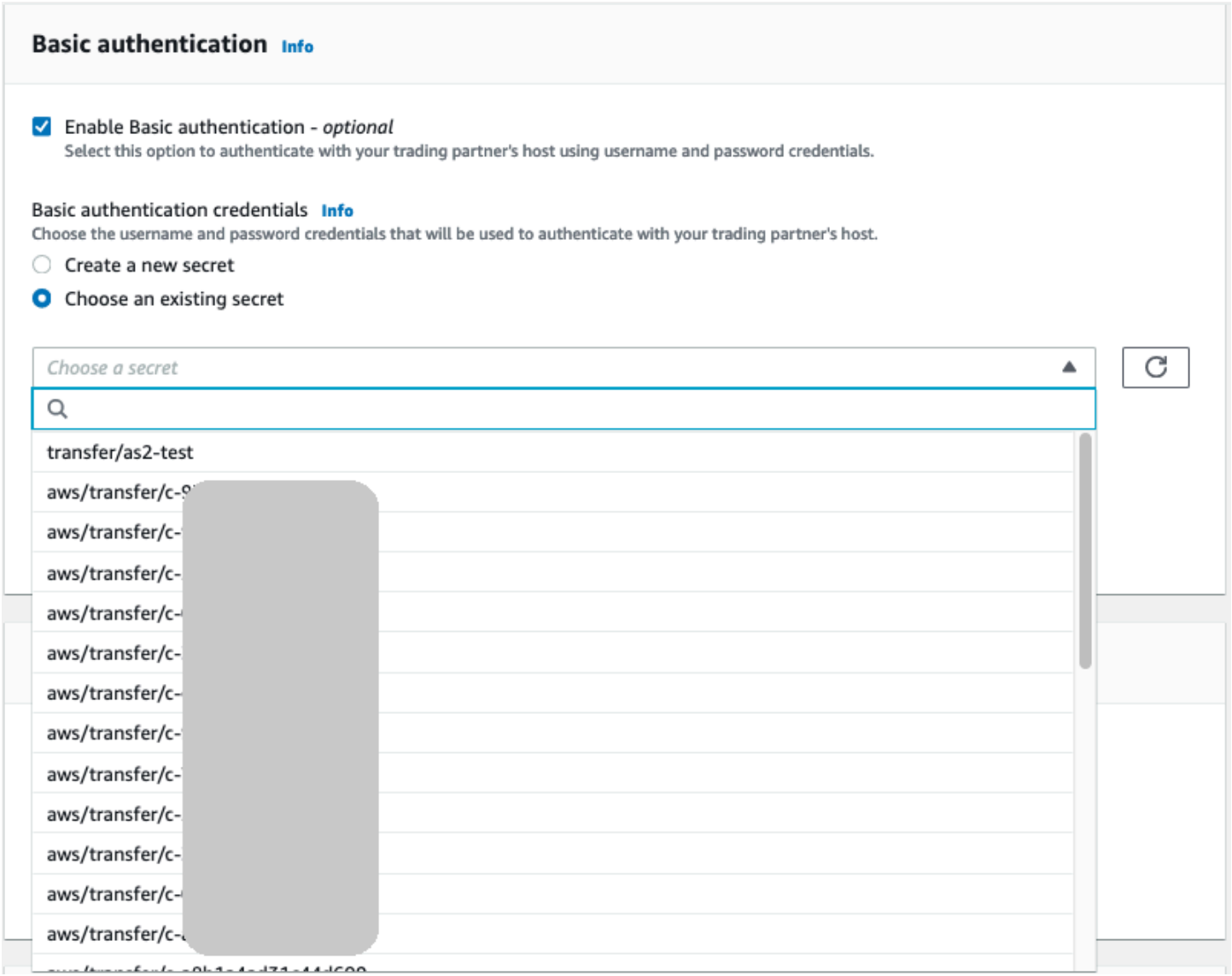


> **Note**
>
> Quando crei un nuovo segreto nella console, il nome del segreto segue questa convenzione di denominazione:**`/aws/transfer/`*`connector-id`***, dove *`connector-id`* è l'ID del connettore che stai creando. Consideralo quando cerchi di individuare il segreto in. AWS Secrets Manager

Usa un segreto esistente

Quando crei un connettore nella console, puoi specificare un segreto esistente.

Per utilizzare un segreto esistente, scegli Scegli un segreto esistente, quindi scegli un segreto dal menu a discesa. Per i dettagli sulla creazione di un segreto formattato correttamente in Secrets Manager, vedereCrea un segreto in AWS Secrets Manager.



Crea un segreto in AWS Secrets Manager

La procedura seguente descrive come creare un segreto appropriato da utilizzare con il connettore AS2.

> **Note**
>
> L'autenticazione di base è disponibile solo se utilizzi HTTPS.

Per memorizzare le credenziali utente in Secrets Manager per l'autenticazione AS2 Basic

1. Accedere AWS Management Console e aprire la AWS Secrets Manager console all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Nel pannello di navigazione a sinistra, seleziona Segreti.
3. Nella pagina Segreti, scegli Memorizza un nuovo segreto.
4. Nella pagina Scegli il tipo di segreto, per Tipo segreto, scegli Altro tipo di segreto.
5. Nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.
   - Chiave: Invio. **`Username`**
   - valore: immettere il nome dell'utente autorizzato a connettersi al server del partner.
6. Se desideri fornire una password, scegli Aggiungi riga e nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.

   Scegli Aggiungi riga e, nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.
   - Chiave: Invio. **`Password`**
   - valore: immettere la password per l'utente.
7. Se desideri fornire una chiave privata, scegli Aggiungi riga e nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.
   - Chiave: Invio. **`PrivateKey`**
   - value — Inserisci una chiave privata per l'utente. Questo valore deve essere archiviato in formato OpenSSH e deve corrispondere alla chiave pubblica archiviata per questo utente nel server remoto.
8. Seleziona Successivo.
9. Nella pagina Configura segreto, inserisci un nome e una descrizione per il tuo segreto. Ti consigliamo di utilizzare il prefisso di **`aws/transfer/`** per il nome. Ad esempio, puoi dare un nome al tuo segreto**`aws/transfer/connector-1`**.
10. Scegli Avanti, quindi accetta le impostazioni predefinite nella pagina Configura rotazione. Quindi scegli Successivo.
11. Nella pagina Revisione, scegli Store per creare e archiviare il segreto.

Dopo aver creato il segreto, puoi sceglierlo quando crei un connettore (vediConfigura i connettori AS2). Nel passaggio in cui abiliti l'autenticazione di base, scegli il segreto dall'elenco a discesa dei segreti disponibili.

Visualizza i dettagli del connettore AS2

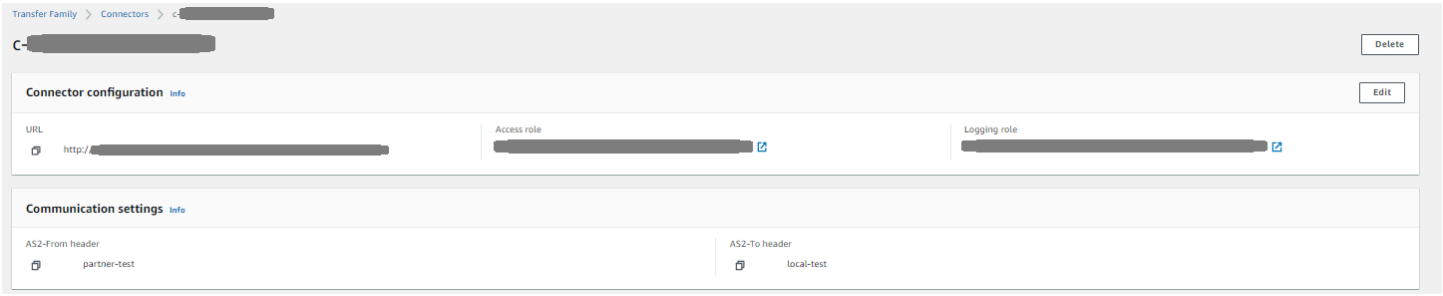
È possibile trovare un elenco di dettagli e proprietà di un AWS Transfer Family connettore AS2 nella AWS Transfer Family console. Le proprietà di un connettore AS2 includono l'URL, i ruoli, i profili, gli mDNS, i tag e le metriche di monitoraggio.

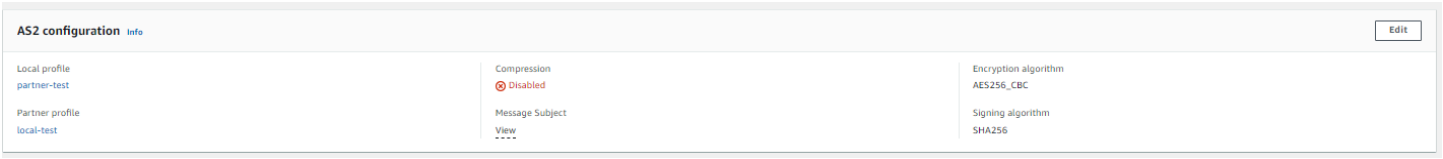
Questa è la procedura per visualizzare i dettagli del connettore.

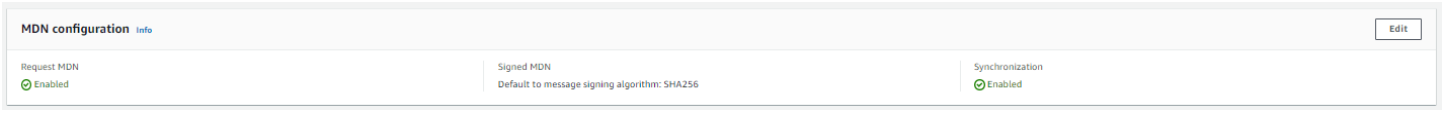
Per visualizzare i dettagli dei connettori

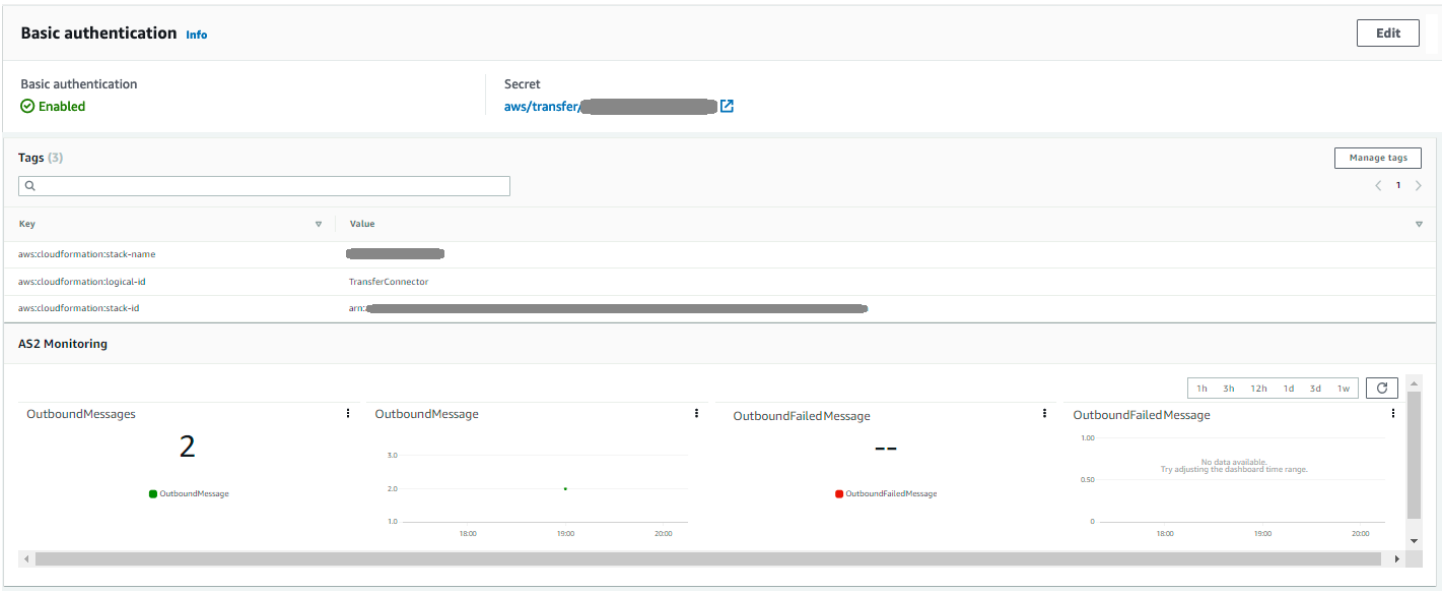
1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, selezionare Connectors (Connettori).
3. Scegli l'identificatore nella colonna Connector ID per visualizzare la pagina dei dettagli del connettore selezionato.

È possibile modificare le proprietà del connettore AS2 nella pagina dei dettagli del connettore scegliendo Modifica.









> **Note**
>
> È possibile ottenere molte di queste informazioni, anche se in un formato diverso, eseguendo il seguente comando (): AWS Command Line Interface AWS CLI
>
> ```
> aws transfer describe-connector --connector-id your-connector-id
> ```
>
> Per ulteriori informazioni, consulta il riferimento DescribeConnectorall'API.

Gestisci i partner AS2

Questo argomento illustra come gestire i certificati, i profili e gli accordi AS2.

Importa certificati AS2

Il processo Transfer Family AS2 utilizza chiavi di certificato sia per la crittografia che per la firma delle informazioni trasferite. I partner possono utilizzare la stessa chiave per entrambi gli scopi o una chiave separata per ciascuno. Se disponi di chiavi di crittografia comuni conservate in deposito da una terza parte affidabile in modo che i dati possano essere decrittografati in caso di emergenza o violazione della sicurezza, ti consigliamo di disporre di chiavi di firma separate. Utilizzando chiavi di firma separate (che non vengono affidate a garanzia), non compromettete le funzionalità di non ripudio delle vostre firme digitali.

> **Note**
>
> La lunghezza della chiave per i certificati AS2 deve essere di almeno 2048 bit e al massimo di 4096.

I seguenti punti descrivono in dettaglio come vengono utilizzati i certificati AS2 durante il processo.

- AS2 in entrata
  - Il partner commerciale invia la propria chiave pubblica per il certificato di firma e questa chiave viene importata nel profilo del partner.
  - La parte locale invia la chiave pubblica per i certificati di crittografia e firma. Il partner importa quindi la chiave o le chiavi private. La parte locale può inviare chiavi di certificato separate per la firma e la crittografia oppure può scegliere di utilizzare la stessa chiave per entrambi gli scopi.
- AS2 in uscita
  - Il partner invia la chiave pubblica per il proprio certificato di crittografia e questa chiave viene importata nel profilo del partner.
  - La parte locale invia la chiave pubblica per il certificato da firmare e importa la chiave privata del certificato per la firma.
  - Se utilizzi HTTPS, puoi importare un certificato Transport Layer Security (TLS) autofirmato.

Per informazioni dettagliate su come creare certificati, consulta. the section called “Fase 1: Creare certificati per AS2”

Questa procedura spiega come importare i certificati utilizzando la console Transfer Family. Se AWS CLI invece desideri utilizzare la, consultathe section called “Fase 3: Importazione dei certificati come risorse di certificati Transfer Family”.

Per specificare un certificato compatibile con AS2

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, sotto AS2 Trading Partners, scegli Certificati.
3. Selezionare Import certificate (Importa certificato).
4. Nella sezione Descrizione del certificato, inserisci un nome facilmente identificabile per il certificato. Assicurati di poter identificare lo scopo del certificato tramite la sua descrizione. Inoltre, scegli il ruolo per il certificato.

5. Nella sezione Contenuto del certificato, fornisci un certificato pubblico rilasciato da un partner commerciale o le chiavi pubbliche e private per un certificato locale.
6. Nella sezione Utilizzo del certificato, scegli lo scopo di questo certificato. Può essere usato per la crittografia, la firma o entrambi.

> **Note**
>
> Se scegli Crittografia e firma per l'utilizzo, Transfer Family crea due certificati identici (ognuno con il proprio ID): uno con un valore d'uso di `ENCRYPTION` e uno con un valore di utilizzo di`SIGNING`.

7. Compila la sezione Contenuto del certificato con i dettagli appropriati.
   - Se scegli Certificato autofirmato, non fornisci la catena di certificati.
   - Incolla il contenuto del certificato.
   - Se il certificato non è un certificato autofirmato, fornisci la catena di certificati.
   - Se questo certificato è un certificato locale, incollane la chiave privata.
8. Scegli Importa certificato per completare il processo e salvare i dettagli del certificato importato.

> **Note**
>
> I certificati TLS possono essere importati solo come certificato pubblico del partner. Se si seleziona Certificato pubblico di un partner e quindi si seleziona Transport Layer Security (TLS) per l'utilizzo, viene visualizzato un avviso. Inoltre, i certificati TLS devono essere autofirmati (ovvero, è necessario selezionare Certificato autofirmato per importare un certificato TLS).

Rotazione dei certificati AS2

Spesso i certificati sono validi per un periodo da sei mesi a un anno. È possibile che tu abbia impostato profili che desideri mantenere per un periodo più lungo. Per facilitare ciò, Transfer Family offre la rotazione dei certificati. È possibile specificare più certificati per un profilo, in modo da continuare a utilizzare il profilo per più anni. Transfer Family utilizza i certificati per la firma (opzionale) e la crittografia (obbligatoria). Se lo desideri, puoi specificare un singolo certificato per entrambi gli scopi.

La rotazione dei certificati è il processo di sostituzione di un vecchio certificato in scadenza con un certificato più recente. La transizione è graduale per evitare di interrompere i trasferimenti, laddove un partner dell'accordo non abbia ancora configurato un nuovo certificato per i trasferimenti in uscita o stia inviando payload firmati o crittografati con un vecchio certificato in un periodo in cui potrebbe essere in uso anche un certificato più recente. Il periodo intermedio in cui sono validi sia i vecchi che i nuovi certificati viene definito periodo di grazia.

I certificati X.509 hanno `Not Before` e date. `Not After` Tuttavia, questi parametri potrebbero non fornire un controllo sufficiente per gli amministratori. Transfer Family fornisce `Active Date` `Inactive Date` impostazioni per controllare quale certificato viene utilizzato per i payload in uscita e quale è accettato per i payload in entrata.

La selezione dei certificati in uscita utilizza il valore massimo precedente alla data del trasferimento come. `Inactive Date` I processi in entrata accettano certificati nell'intervallo di `Not Before` e `Not After` e nell'intervallo di `Active Date` e. `Inactive Date`

La tabella seguente descrive un modo possibile per configurare due certificati per un singolo profilo.

Due certificati a rotazione

Nome	NOT BEFORE(controllato dall'autorità di certificazione)	ACTIVE DATE(impostato da Transfer Family)	INACTIVE DATE(impostato da Transfer Family)	NOT AFTER(impostato dall'autorità di certificazione)
Cert1 (certificato precedente)	2019-11-01	2020-01-01	2020-12-31	2024-01-01
Cert2 (certificato più recente)	2020-11-01	2020-06-01	2021-06-01	2025-01-01

Tieni presente quanto segue:

- Quando si specifica un `Active Date` e `Inactive Date` per un certificato, l'intervallo deve essere compreso tra e. `Not Before` `Not After`
- Ti consigliamo di configurare diversi certificati per ogni profilo, assicurandoti che l'intervallo di date attivo per tutti i certificati combinati copra il periodo di tempo per il quale desideri utilizzare il profilo.

- Ti consigliamo di specificare un periodo di tolleranza tra il momento in cui il certificato precedente diventa inattivo e il momento in cui il certificato più recente diventa attivo. Nell'esempio precedente, il primo certificato non diventa inattivo fino al 31/12/2020, mentre il secondo certificato diventa attivo il 01/06/2020, garantendo un periodo di grazia di 6 mesi. Nel periodo dal 01/06/2020 al 31/12/2020, entrambi i certificati sono attivi.

Crea profili AS2

Utilizzate questa procedura per creare profili locali e di partner. Questa procedura spiega come creare profili AS2 utilizzando la console Transfer Family. Se AWS CLI invece desideri utilizzare il, consultathe section called “Fase 4: Crea profili per te e il tuo partner commerciale”.

Per creare un profilo AS2

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, sotto AS2 Trading Partners, scegli Profili, quindi scegli Crea profilo.
3. Nella sezione Configurazione del profilo, inserisci l'ID AS2 per il profilo. Questo valore viene utilizzato per le intestazioni HTTP specifiche del protocollo AS2 `as2-from` e `as2-to` per identificare la partnership commerciale, che determina i certificati da utilizzare e così via.
4. Nella sezione Tipo di profilo, scegli Profilo locale o Profilo partner.
5. Nella sezione Certificati, scegli uno o più certificati dal menu a discesa.

   > **Note**
   >
   > Se desideri importare un certificato che non è elencato nel menu a discesa, seleziona Importa un nuovo certificato. Si apre una nuova finestra del browser nella schermata Importa certificato. Per la procedura relativa all'importazione dei certificati, vedereImporta certificati AS2.

6. (Facoltativo) Nella sezione Tag, specificate una o più coppie chiave-valore per identificare questo profilo.
7. Scegli Crea profilo per completare il processo e salvare il nuovo profilo.

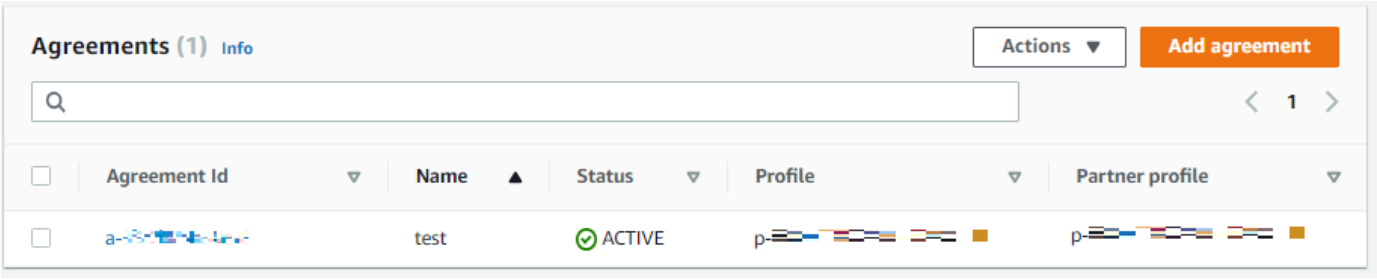
Crea accordi AS2

Gli accordi sono associati ai server Transfer Family. Specificano i dettagli per i partner commerciali che utilizzano il protocollo AS2 per scambiare messaggi o file utilizzando Transfer Family, per i trasferimenti in entrata, ovvero l'invio di file AS2 da una fonte esterna di proprietà del partner a un server Transfer Family.

Questa procedura spiega come creare accordi AS2 utilizzando la console Transfer Family. Se AWS CLI invece desideri utilizzare il, consultathe section called “Fase 5: Crea un accordo tra te e il tuo partner”.

Per creare un contratto per un server Transfer Family

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server, quindi scegli un server che utilizza il protocollo AS2.
3. Nella pagina dei dettagli del server, scorri verso il basso fino alla sezione Accordi.



4. Scegli Aggiungi accordo.
5. Compila i parametri dell'accordo, come segue:

   a. Nella sezione Configurazione dell'accordo, inserisci un nome descrittivo. Assicurati di poter identificare lo scopo dell'accordo tramite il nome. Inoltre, imposta lo stato dell'accordo: Attivo (selezionato per impostazione predefinita) o Inattivo.

   b. Nella sezione Configurazione della comunicazione, scegli un profilo locale e un profilo partner.

   c. Nella sezione di configurazione della cartella Inbox, scegli un bucket Amazon S3 per archiviare i file in entrata e un ruolo IAM che possa accedere al bucket. Facoltativamente, puoi inserire un prefisso (cartella) da utilizzare per archiviare i file nel bucket.

      Ad esempio, se inserisci **`DOC-EXAMPLE-BUCKET`** il tuo bucket e il tuo prefisso, **`incoming`** i file in arrivo vengono salvati nella cartella. `/DOC-EXAMPLE-BUCKET/incoming`

d. (Facoltativo) Aggiungi tag nella sezione Tag.

e. Dopo aver inserito tutte le informazioni per l'accordo, scegli Crea accordo.

Il nuovo accordo viene visualizzato nella sezione Accordi della pagina dei dettagli del server.

Invio e ricezione di messaggi AS2

Questa sezione descrive i processi per l'invio e la ricezione di messaggi AS2. Fornisce inoltre dettagli sui nomi dei file e sulle posizioni associati ai messaggi AS2.

La tabella seguente elenca gli algoritmi di crittografia disponibili per i messaggi AS2 e quando è possibile utilizzarli.

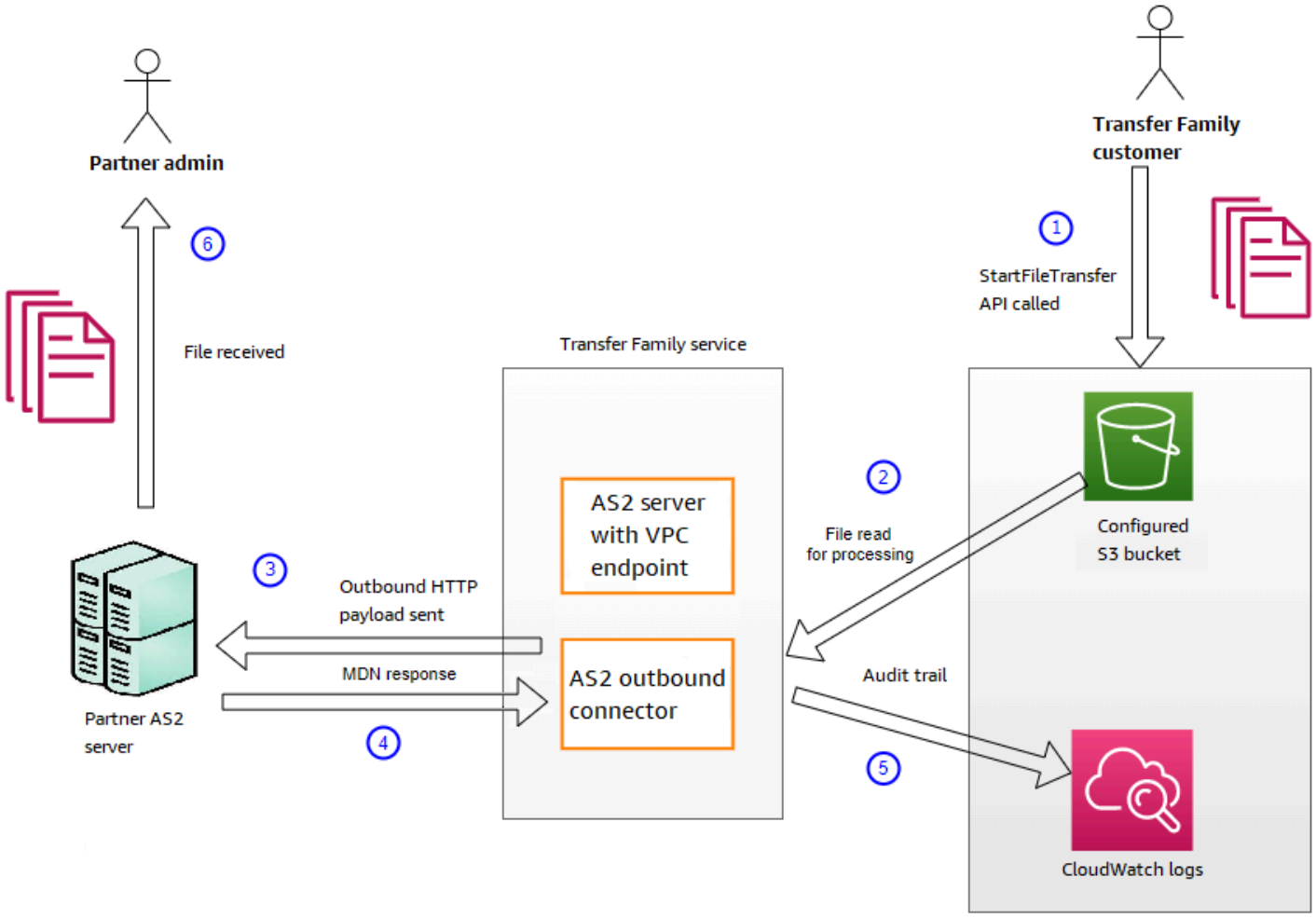
Algoritmo di crittografia	HTTP	HTTPS	Note
AES128_CBC	Sì	Sì	
AES192_CBC	Sì	Sì	
AES256_CBC	Sì	Sì	
DES_EDE3_CBC	Sì	Sì	Utilizzate questo algoritmo solo se dovete supportare un client legacy che lo richiede, poiché si tratta di un algoritmo di crittografia debole.
NONE	No	Sì	Se si inviano messaggi a un server Transfer Family, è possibile selezionare solo `NONE` se si utilizza un Application Load Balancer (ALB).

Argomenti

Processo di invio di messaggi AS2

Il processo in uscita è definito come un messaggio o un file inviato AWS a un client o servizio esterno. La sequenza per i messaggi in uscita è la seguente:

1. Un amministratore chiama il comando `start-file-transfer` AWS Command Line Interface (AWS CLI) o l'operazione `StartFileTransfer` API. Questa operazione fa riferimento a una `connector` configurazione.
2. Transfer Family rileva una nuova richiesta di file e individua il file. Il file è compresso, firmato e crittografato.
3. Un client HTTP di trasferimento esegue una richiesta HTTP POST per trasmettere il payload al server AS2 del partner.
4. Il processo restituisce la risposta MDN firmata, in linea con la risposta HTTP (MDN sincrono).
5. Man mano che il file si sposta tra le diverse fasi di trasmissione, il processo fornisce al cliente la ricevuta della risposta MDN e i dettagli di elaborazione.
6. Il server AS2 remoto mette il file decrittografato e verificato a disposizione dell'amministratore partner.



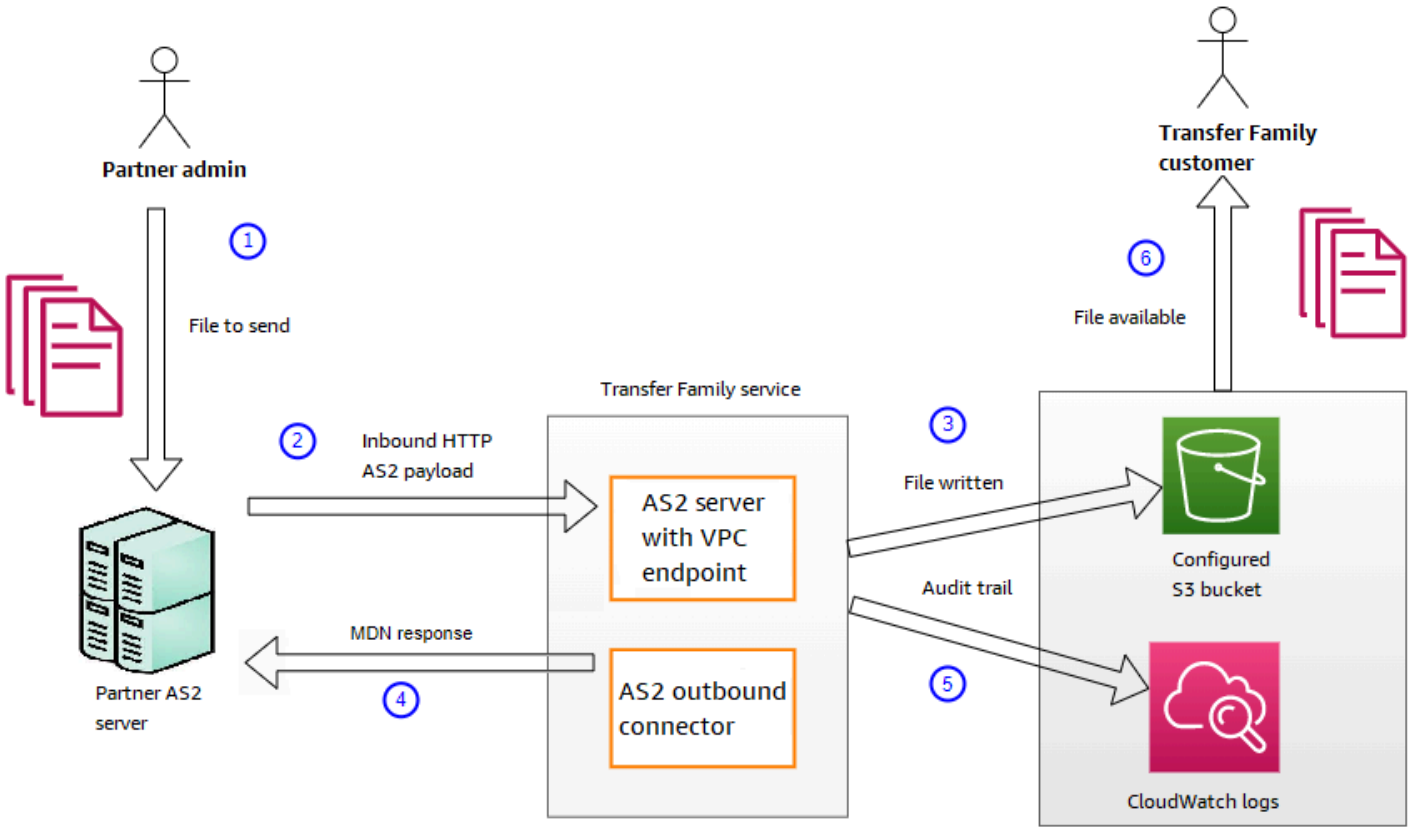
L'elaborazione AS2 supporta molti dei protocolli RFC 4130, con particolare attenzione ai casi d'uso comuni e all'integrazione con le implementazioni di server compatibili con AS2 esistenti. Per i dettagli sulle configurazioni supportate, vedere. Configurazioni supportate da AS2

Processo di ricezione dei messaggi AS2

Il processo in entrata è definito come un messaggio o un file che viene trasferito sul tuo AWS Transfer Family server. La sequenza per i messaggi in entrata è la seguente:

1. Un processo amministrativo o automatizzato avvia un trasferimento di file AS2 sul server AS2 remoto del partner.
2. Il server AS2 remoto del partner firma e crittografa il contenuto del file, quindi invia una richiesta HTTP POST a un endpoint AS2 in entrata ospitato su Transfer Family.

3. Utilizzando i valori configurati per il server, i partner, i certificati e l'accordo, Transfer Family decrittografa e verifica il payload AS2. Il contenuto del file viene archiviato nell'archivio di file Amazon S3 configurato.
4. La risposta MDN firmata viene restituita in linea con la risposta HTTP o in modo asincrono tramite una richiesta HTTP POST separata al server di origine.
5. Un audit trail viene scritto su Amazon CloudWatch con i dettagli sullo scambio.
6. Il file decrittografato è disponibile in una cartella denominata. `inbox/processed`



Invio e ricezione di messaggi AS2 tramite HTTPS

Questa sezione descrive come configurare un server Transfer Family che utilizza il protocollo AS2 per inviare e ricevere messaggi tramite HTTPS.

Argomenti

- Invia messaggi AS2 tramite HTTPS
- Ricevi messaggi AS2 tramite HTTPS

Invia messaggi AS2 tramite HTTPS

Per inviare messaggi AS2 tramite HTTPS, crea un connettore con le seguenti informazioni:

- Per l'URL, specifica un URL HTTPS
- Per l'algoritmo di crittografia, selezionare uno degli algoritmi disponibili.

> **Note**
>
> Per inviare messaggi a un server Transfer Family senza utilizzare la crittografia (ovvero, selezionando l'algoritmo `NONE` di crittografia), è necessario utilizzare un Application Load Balancer (ALB).

- Fornire i valori rimanenti per il connettore come descritto in. Configura i connettori AS2

Ricevi messaggi AS2 tramite HTTPS

AWS Transfer Family I server AS2 attualmente forniscono solo il trasporto HTTP sulla porta 5080. Tuttavia, puoi terminare TLS su un sistema di bilanciamento del carico di rete o delle applicazioni davanti all'endpoint VPC del server Transfer Family utilizzando una porta e un certificato di tua scelta. Con questo approccio, puoi fare in modo che i messaggi AS2 in arrivo utilizzino HTTPS.

Prerequisiti

- Il VPC deve trovarsi nello stesso Regione AWS server Transfer Family.
- Le sottoreti del tuo VPC devono trovarsi all'interno delle zone di disponibilità in cui desideri utilizzare il server.

> **Note**
>
> Ogni server Transfer Family può supportare fino a tre zone di disponibilità.

- Alloca fino a tre indirizzi IP elastici nella stessa regione del server. In alternativa, puoi scegliere di utilizzare il tuo intervallo di indirizzi IP (BYOIP).

> **Note**
>
> Il numero di indirizzi IP elastici deve corrispondere al numero di zone di disponibilità utilizzate con gli endpoint del server.

È possibile configurare un Network Load Balance (NLB) o un Application Load Balancer (ALB). La tabella seguente elenca i pro e i contro di ogni approccio.

La tabella seguente fornisce le differenze nelle funzionalità quando si utilizza un NLB rispetto a un ALB per terminare TLS.

Funzionalità	Network Load Balancer (NLB)	Application Load Balancer (ALB)
Latenza	Latenza inferiore in quanto opera a livello di rete.	Latenza più elevata in quanto opera a livello di applicazione.
Supporto per indirizzi IP statici	Può allegare indirizzi IP elastici che possono essere statici.	Impossibile collegare indirizzi IP elastici: fornisce un dominio i cui indirizzi IP sottostanti possono cambiare.
Routing avanzato	Non supporta il routing avanzato.	Supporta il routing avanzato. Può iniettare l'`X-Forwarded-Proto` intestazione richiesta per AS2 senza crittografia. Questa intestazione è descritta in X-Forwarded-Proto sul sito web developer.mozilla.org.
Terminazione TLS/SSL	Supporta la terminazione TLS/SSL	Supporta la terminazione TLS/SSL

Funzionalità	Network Load Balancer (NLB)	Application Load Balancer (ALB)
TLS reciproco (mTLS)	Transfer Family attualmente non supporta l'utilizzo di un NLB per MTL	Support per MTL

Configure NLB

Questa procedura descrive come configurare un Network Load Balancer (NLB) con accesso a Internet nel tuo VPC.

Per creare un Network Load Balancer e definire l'endpoint VPC del server come destinazione del load balancer

1. Apri la console Amazon Elastic Compute Cloud all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di navigazione, scegli Load Balancers, quindi scegli Create load balancer.
3. In Network Load Balancer (Sistema di bilanciamento del carico della rete), scegli Crea.
4. Nella sezione Configurazione di base, inserisci le seguenti informazioni:
   - Per Nome, inserisci un nome descrittivo per il sistema di bilanciamento del carico.
   - Per Scheme (Schema), scegliere Internet-facing.
   - Per il tipo di indirizzo IP, scegli IPv4.
5. Nella sezione Mappatura della rete, inserisci le seguenti informazioni:
   - Per VPC, scegli il cloud privato virtuale (VPC) che hai creato.
   - In Mappature, scegli le zone di disponibilità associate alle sottoreti pubbliche disponibili nello stesso VPC che usi con gli endpoint del server.
   - Per l'indirizzo IPv4 di ogni sottorete, scegli uno degli indirizzi IP elastici che hai allocato.
6. Nella sezione Listener e routing, inserite le seguenti informazioni:
   - Per Protocollo, scegli TLS.
   - Per Port (Porta), immettere **`5080`**.
   - Per Azione predefinita, scegli Crea gruppo target. Per i dettagli sulla creazione di un nuovo gruppo target, consultaPer creare un gruppo di destinazione.

Dopo aver creato un gruppo target, inserisci il suo nome nel campo di azione predefinito.

7. Nella sezione Impostazioni Secure listener, scegli il tuo certificato nell'area Certificato SSL/TLS predefinito.
8. Scegli Crea sistema di bilanciamento del carico per creare il tuo NLB.
9. (Facoltativo, ma consigliato) Attiva i log di accesso per Network Load Balancer per mantenere un audit trail completo, come descritto in Registri di accesso per il tuo Network Load Balancer.

   Consigliamo questo passaggio perché la connessione TLS viene interrotta all'NLB. Pertanto, l'indirizzo IP di origine riportato nei gruppi di CloudWatch log di Transfer Family AS2 è l'indirizzo IP privato dell'NLB, anziché l'indirizzo IP esterno del partner commerciale.

Configure ALB

Questa procedura descrive come configurare un Application Load Balancer (NLB) nel tuo VPC.

Per creare un Application Load Balancer e definire l'endpoint VPC del server come destinazione del load balancer

1. Apri la console Amazon Elastic Compute Cloud all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di navigazione, scegli Load Balancers, quindi scegli Create load balancer.
3. In Application Load Balancer, scegli Crea.
4. Nella console ALB, crea un nuovo listener HTTP sulla porta 443 (HTTPS).
5. (Facoltativo). Se desideri configurare l'autenticazione reciproca (MTL), configura le impostazioni di sicurezza e un trust store.

   a. Allega il tuo certificato SSL/TLS al listener.

   b. In Gestione dei certificati client, seleziona Autenticazione reciproca (mTLS).

   c. Scegli Verifica con trust store.

   d. In Impostazioni MTLS avanzate, scegli o crea un trust store caricando i tuoi certificati CA.
6. Crea un nuovo gruppo target e aggiungi gli indirizzi IP privati degli endpoint del server Transfer Family AS2 come destinazioni sulla porta 5080. Per i dettagli sulla creazione di un nuovo gruppo target, consulta. Per creare un gruppo di destinazione

7. Configura i controlli sanitari per il gruppo target in modo che utilizzi il protocollo TCP sulla porta 5080.
8. Crea una nuova regola per inoltrare il traffico HTTPS dal listener al gruppo di destinazione.
9. Configura il listener per utilizzare il tuo certificato SSL/TLS.

Dopo aver configurato il sistema di bilanciamento del carico, i client comunicano con il sistema di bilanciamento del carico tramite il listener di porta personalizzato. Quindi, il load balancer comunica con il server tramite la porta 5080.

Per creare un gruppo di destinazione

1. Dopo aver scelto Crea gruppo target nella procedura precedente, viene visualizzata la pagina Specificare i dettagli del gruppo per un nuovo gruppo target.
2. Nella sezione Configurazione di base, inserisci le seguenti informazioni.
   - Per Scegli un tipo di destinazione, scegli gli indirizzi IP.
   - In Nome gruppo di destinazione, immetti un nome per il gruppo di destinazione.
   - Per Protocol (Protocollo), selezionare TCP.
   - Per Port (Porta), immettere **`5080`**.
   - Per il tipo di indirizzo IP, scegli IPv4.
   - Per VPC, scegli il VPC che hai creato per il tuo server Transfer Family AS2.
3. Nella sezione Controlli sanitari, scegli TCP per il protocollo Health check.
4. Seleziona Successivo.
5. Nella pagina Registra obiettivi, inserisci le seguenti informazioni:
   - Per Network, verifica che sia specificato il VPC che hai creato per il tuo server Transfer Family AS2.
   - Per l'indirizzo IPv4, inserisci l'indirizzo IPv4 privato degli endpoint del tuo server Transfer Family AS2.

     Se hai più di un endpoint per il tuo server, scegli Aggiungi indirizzo IPv4 per aggiungere un'altra riga per l'immissione di un altro indirizzo IPv4. Ripeti questa procedura finché non avrai inserito gli indirizzi IP privati per tutti gli endpoint del server.
   - Assicurati che Ports sia impostato su. **`5080`**

- Scegli Includi come in sospeso di seguito per aggiungere i tuoi dati alla sezione Review targets.

6. Nella sezione Rivedi gli obiettivi, esamina i tuoi obiettivi IP.
7. Scegli Crea gruppo target, quindi torna alla procedura precedente per la creazione del tuo NLB e inserisci il nuovo gruppo target dove indicato.

Verifica l'accesso al server da un indirizzo IP elastico

Connettiti al server tramite la porta personalizzata utilizzando un indirizzo IP elastico o il nome DNS del Network Load Balancer.

> **Important**
>
> Gestisci l'accesso al tuo server dagli indirizzi IP dei client utilizzando gli elenchi di controllo degli accessi alla rete (ACL di rete) per le sottoreti configurate sul load balancer. Le autorizzazioni ACL di rete sono impostate a livello di sottorete, quindi le regole si applicano a tutte le risorse che utilizzano la sottorete. Non è possibile controllare l'accesso dagli indirizzi IP dei client utilizzando i gruppi di sicurezza, poiché il tipo di destinazione del sistema di bilanciamento del carico è impostato su indirizzi IP anziché su istanze. Pertanto, il load balancer non conserva gli indirizzi IP di origine. Se i controlli di integrità del Network Load Balancer falliscono, significa che il load balancer non può connettersi all'endpoint del server. Per risolvere questo problema, controlla quanto segue:
>
> - Verifica che il gruppo di sicurezza associato all'endpoint del server consenta le connessioni in entrata dalle sottoreti configurate sul load balancer. Il load balancer deve essere in grado di connettersi all'endpoint del server tramite la porta 5080.
> - Verifica che lo stato del server sia Online.

Trasferimento di file tramite un connettore AS2

I connettori AS2 stabiliscono una relazione tra i partner commerciali per il trasferimento di messaggi AS2 da un server Transfer Family a una destinazione esterna di proprietà del partner.

È possibile utilizzare Transfer Family per inviare messaggi AS2 facendo riferimento all'ID del connettore e ai percorsi dei file, come illustrato nel seguente 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"
```

Per ottenere i dettagli dei connettori, esegui il seguente comando:

```
aws transfer list-connectors
```

Il `list-connectors` comando restituisce gli ID dei connettori, gli URL e gli Amazon Resource Names (ARN) per i connettori.

Per restituire le proprietà di un particolare connettore, esegui il comando seguente con l'ID che desideri utilizzare:

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

Il `describe-connector` comando restituisce tutte le proprietà del connettore, inclusi l'URL, i ruoli, i profili, gli mDNS (Message Disposition Notices), i tag e le metriche di monitoraggio.

È possibile confermare che il partner ha ricevuto correttamente i file visualizzando i file JSON e MDN. Questi file sono denominati in base alle convenzioni descritte in. Nomi e posizioni dei file
Se hai configurato un ruolo di registrazione quando hai creato il connettore, puoi anche controllare CloudWatch nei log lo stato dei messaggi AS2.

Per visualizzare i dettagli del connettore AS2, vedere. Visualizza i dettagli del connettore AS2 Per ulteriori informazioni sulla creazione di connettori AS2, vedere. Configura i connettori AS2

Nomi e posizioni dei file

Questa sezione illustra le convenzioni di denominazione dei file per i trasferimenti AS2.

Per i trasferimenti di file in entrata, tenete presente quanto segue:

- Si specifica la directory di base in un accordo. La directory di base è il nome del bucket Amazon S3 combinato con un prefisso, se presente. Ad esempio, `/DOC-EXAMPLE-BUCKET/AS2-folder`.
- Se un file in entrata viene elaborato correttamente, il file (e il file JSON corrispondente) viene salvato nella cartella. `/processed` Ad esempio, `/DOC-EXAMPLE-BUCKET/AS2-folder/processed`.

  Il file JSON contiene i seguenti campi:

  - `agreement-id`
  - `as2-from`
  - `as2-to`
  - `as2-message-id`
  - `transfer-id`
  - `client-ip`
  - `connector-id`
  - `failure-message`
  - `file-path`
  - `message-subject`
  - `mdn-message-id`
  - `mdn-subject`
  - `requester-file-name`
  - `requester-content-type`
  - `server-id`
  - `status-code`
  - `failure-code`
  - `transfer-size`
- Se un file in entrata non può essere elaborato correttamente, il file (e il file JSON corrispondente) viene salvato nella cartella. `/failed` Ad esempio, `/DOC-EXAMPLE-BUCKET/AS2-folder/failed`.
- Il file trasferito viene archiviato nella `processed` cartella come. *`original_filename`*`.`*`messageId`*`.`*`original_extension`* Cioè, l'ID del messaggio per il trasferimento viene aggiunto al nome del file, prima dell'estensione originale.
- Un file JSON viene creato e salvato come. *`original_filename`*`.`*`messageId`*`.`*`original_extension`*`.json` Oltre all'ID del messaggio aggiunto, la stringa `.json` viene aggiunta al nome del file trasferito.
- Un file MDN (Message Disposition Notice) viene creato e salvato come. *`original_filename`*`.`*`messageId`*`.`*`original_extension`*`.mdn` Oltre all'ID del messaggio aggiunto, la stringa `.mdn` viene aggiunta al nome del file trasferito.
- Se è presente un file in entrata denominato`ExampleFileInS3Payload.dat`, vengono creati i seguenti file:

- File — `ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
- JSON — `ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
- MDN — `ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`

Per i trasferimenti in uscita, la denominazione è simile, con la differenza che non esiste un file di messaggi in entrata e inoltre, l'ID di trasferimento per il messaggio trasferito viene aggiunto al nome del file. L'ID di trasferimento viene restituito dall'operazione `StartFileTransfer` API (o quando un altro processo o script richiama questa operazione).

- `transfer-id`è un identificatore associato a un trasferimento di file. Tutte le richieste che fanno parte di una `StartFileTransfer` chiamata condividono un`transfer-id`.
- La directory di base è la stessa del percorso utilizzato per il file sorgente. In altre parole, la directory di base è il percorso specificato nell'operazione o nel `start-file-transfer` AWS CLI comando `StartFileTransfer` API. Per esempio:

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

  Se si esegue questo comando, i file MDN e JSON vengono salvati in `/DOC-EXAMPLE-BUCKET/AS2-folder/processed` (per trasferimenti riusciti) o `/DOC-EXAMPLE-BUCKET/AS2-folder/failed` (per trasferimenti non riusciti).
- Un file JSON viene creato e salvato come. *`original_filename`*`.`*`transferId`*`.`*`messageId`*`.`*`original_extension`*`.json`
- Un file MDN viene creato e salvato come. *`original_filename`*`.`*`transferId`*`.`*`messageId`*`.`*`original_extension`*`.mdn`
- Se esiste un file in uscita denominato`ExampleFileOutTestOutboundSyncMdn.dat`, vengono creati i seguenti file:
  - 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`

Puoi anche controllare CloudWatch i log per visualizzare i dettagli dei tuoi trasferimenti, compresi quelli che non sono andati a buon fine.

Codici di stato

La tabella seguente elenca tutti i codici di stato che possono essere registrati nei CloudWatch log quando tu o il tuo partner inviate un messaggio AS2. Le diverse fasi di elaborazione dei messaggi si applicano a diversi tipi di messaggi e sono destinate esclusivamente al monitoraggio. Gli stati COMPLETED e FAILED rappresentano la fase finale dell'elaborazione e sono visibili nei file JSON.

Codice	Descrizione	Elaborazione completata?
IN ELABORAZIONE	Il messaggio è in fase di conversione nel formato finale. Ad esempio, le fasi di decompressione e decrittografia hanno entrambe questo stato.	No
MDN_TRANSMITX	L'elaborazione dei messaggi consiste nell'invio di una risposta MDN.	No
MDN_RECEIVE	L'elaborazione dei messaggi sta ricevendo una risposta MDN.	No
COMPLETED	L'elaborazione dei messaggi è stata completata correttamente. Questo stato include l'invio di un MDN per un messaggio in entrata o per la verifica MDN dei messaggi in uscita.	Sì
Non riuscito	L'elaborazione dei messaggi non è riuscita. Per un	Sì

Codice	Descrizione	Elaborazione completata?
	elenco dei codici di errore, vedereCodici di errore AS2.	

File JSON di esempio

Questa sezione elenca file JSON di esempio per i trasferimenti in entrata e in uscita, inclusi file di esempio per trasferimenti riusciti e trasferimenti non riusciti.

File in uscita di esempio che è stato trasferito correttamente:

```
{
  "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"
}
```

Esempio di file in uscita trasferito senza successo:

```
{
  "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"
}
```

Esempio di file in entrata trasferito correttamente:

```
{
  "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"
}
```

Esempio di file in entrata che non è stato trasferito correttamente:

```
{
  "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"
}
```


Monitoraggio dell'utilizzo di AS2

Puoi monitorare l'attività di AS2 utilizzando Amazon CloudWatch eAWS CloudTrail. Per visualizzare altre metriche del server Transfer Family, consulta CloudWatch Registrazione Amazon per AWS Transfer Family

Metriche AS2

Parametro	Descrizione
`InboundMessage`	Il numero totale di messaggi AS2 ricevuti con successo da un partner commerciale. Unità: numero Periodo: 5 minuti
`InboundFailedMessage`	Il numero totale di messaggi AS2 ricevuti senza successo da un partner commerciale. Cioè, un partner commerciale ha inviato un messaggio , ma il server Transfer Family non è stato in grado di elaborarlo correttamente. Unità: numero Periodo: 5 minuti

Parametro	Descrizione
`OutboundMessage`	Il numero totale di messaggi AS2 inviati con successo dal server Transfer Family a un partner commerciale. Unità: numero Periodo: 5 minuti
`OutboundFailedMessage`	Il numero totale di messaggi AS2 che sono stati inviati senza successo a un partner commercia le. Cioè, sono stati inviati dal server Transfer Family, ma non sono stati ricevuti con successo dal partner commerciale. Unità: numero Periodo: 5 minuti

Codici di stato AS2

La tabella seguente elenca tutti i codici di stato che possono essere registrati nei CloudWatch registri quando tu o il tuo partner inviate un messaggio AS2. Le diverse fasi di elaborazione dei messaggi si applicano a diversi tipi di messaggi e sono destinate esclusivamente al monitoraggio. Gli stati COMPLETED e FAILED rappresentano la fase finale dell'elaborazione e sono visibili nei file JSON.

Codice	Descrizione	Elaborazione completata?
IN ELABORAZIONE	Il messaggio è in fase di conversione nel formato finale. Ad esempio, le fasi di decompressione e decrittog rafia hanno entrambe questo stato.	No

Codice	Descrizione	Elaborazione completata?
MDN_TRANSMITX	L'elaborazione dei messaggi consiste nell'invio di una risposta MDN.	No
MDN_RECEIVE	L'elaborazione dei messaggi sta ricevendo una risposta MDN.	No
COMPLETED	L'elaborazione dei messaggi è stata completata correttamente. Questo stato include l'invio di un MDN per un messaggio in entrata o per la verifica MDN dei messaggi in uscita.	Sì
Non riuscito	L'elaborazione dei messaggi non è riuscita. Per un elenco dei codici di errore, vedereCodici di errore AS2.	Sì

Codici di errore AS2

La tabella seguente elenca e descrive i codici di errore che potreste ricevere dai trasferimenti di file AS2.

Codici di errore AS2

Codice	Errore	Descrizione e risoluzione
`ACCESS_DENIED`	• Accesso negato. Verifica se il tuo ruolo di accesso dispone delle autorizzazioni necessarie. • Percorso del file non valido *`send-file-path`*	Si verifica quando si gestisce una `StartFileTransfer` richiesta in cui nessuna delle due non è valida o `SendFilePaths` non è valida. Cioè, nel percorso

Codice	Errore	Descrizione e risoluzione
	• *Impossibile ottenere le credenziali con ErrorCode: error-code*	manca il nome del bucket Amazon S3 oppure il percorso include caratteri non validi. Si verifica anche se Transfer Family non riesce ad assumere il ruolo di accesso o il ruolo di registrazione. Assicurati che il percorso contenga un nome di bucket Amazon S3 e un nome chiave validi.
AGREEMENT_NOT_FOUND	L'accordo non è stato trovato.	L'accordo non è stato trovato o l'accordo è associato a un profilo inattivo. Aggiorna l'accordo all'interno del server Transfer Family per includere i profili attivi.
CONNECTOR_NOT_FOUND	Il connettore o la configurazione correlata non sono stati trovati.	Il connettore non è stato trovato oppure il connettore è associato a un profilo inattivo. Aggiorna il connettore per includere i profili attivi.

Codice	Errore	Descrizione e risoluzione
`CREDENTIALS_RETRIEVAL_FAILED`	1. Segreto non trovato in Secrets Manager. 2. Impossibile accedere a Secrets Manager. 3. Impossibile decifrare il segreto in Secrets Manager. 4. Impossibile ottenere un valore segreto a causa della limitazione.	Per l'autenticazione AS2 Basic, il segreto deve essere formattato correttamente. Le seguenti risoluzioni corrispondono agli errori elencati nella colonna precedente. 1. Assicurati che l'ID segreto sia corretto. 2. Assicurati che il ruolo di accesso disponga delle autorizzazioni appropriate per leggere il segreto. Il ruolo di accesso deve fornire l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta. Inoltre, assicurati che il ruolo fornisca l'accesso in lettura e scrittura alla directory principale dei file con cui intendi inviare`StartFileTransfer` . 3. Se per il segreto viene utilizzata una chiave gestita dal cliente, assicurati che il ruolo di accesso disponga delle autorizzazioni per la chiave AWS Key Management Service (AWS KMS).

Codice	Errore	Descrizione e risoluzione
		4. Per le quote applicabili, consulta. Quote per la gestione dei segreti
DECOMPRESSION_FAILED	Decompressione del messaggio non riuscita.	Il file inviato è danneggiato o l'algoritmo di compressione non è valido. Invia nuovamente il messaggio e verifica che venga utilizzata la compressione ZLIB oppure invia nuovamente il messaggio senza la compressione abilitata.
DECRYPT_FAILED	*Impossibile decifrare l'ID del messaggio Message-ID.* Assicurati che il partner disponga della chiave di crittografia pubblica corretta.	Decrittografia non riuscita. Verifica che il partner abbia inviato un payload utilizzando un certificato valido e che la crittografia sia stata eseguita utilizzando un algoritmo di crittografia valido.
DECRYPT_FAILED_INVALID_SMIME_FORMAT	Impossibile analizzare MimePart con busta.	Il payload MIME è danneggiato o è in un formato SMIME non supportato. Il mittente deve assicurarsi che il formato che sta utilizzando sia supportato, quindi inviare nuovamente il payload.

Codice	Errore	Descrizione e risoluzione
`DECRYPT_FAILED_NO_DECRYPTION_KEY_FOUND`	Non è stata trovata alcuna chiave di decrittografia corrispondente.	Al profilo partner non era assegnato un certificato corrispondente al messaggio oppure i certificati corrispondenti al messaggio sono ora scaduti o non più validi. È necessario aggiornare il profilo partner e assicurarsi che contenga un certificato valido.
`DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG`	*Decrittografia del payload SMIME richiesta utilizzando un algoritmo non supportato con ID: Encryption-ID.*	Il mittente remoto ha inviato un payload AS2 con un algoritmo di crittografia non supportato. Il mittente deve scegliere un algoritmo di crittografia supportato da. AWS Transfer Family
`DUPLICATE_MESSAGE`	Fase di elaborazione duplicata o doppia.	Il payload ha una fase di elaborazione duplicata. Ad esempio, esistono due fasi di crittografia. Invia nuovamente il messaggio con un solo passaggio per la firma, la compressione e la crittografia.

Codice	Errore	Descrizione e risoluzione
`ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND`	*Nessun certificato di crittografia pubblico valido trovato nel profilo: local-profile-ID*	Transfer Family sta tentando di crittografare un messaggio in uscita, ma non è stato trovato alcun certificato di crittografia per il profilo locale. Opzioni di risoluzione: • Assicurati che al profilo locale siano allegati un certificato e una chiave privata per la crittografia. • Assicurati che il certificato di crittografia sia attualmente attivo.
`ENCRYPTION_FAILED`	Impossibile crittografare il *nome* del file.	Il file da inviare non è disponibile per la crittografia. Verificate che il file si trovi nella posizione AS2 prevista e che AWS Transfer Family disponga dell'autorizzazione per leggerlo.
`FILE_SIZE_TOO_LARGE`	La dimensione del file è troppo grande.	Ciò si verifica quando si invia o si riceve un file che supera il limite di dimensione del file.

Codice	Errore	Descrizione e risoluzione
`HTTP_ERROR_RESPONSE_FROM_PARTNER`	*`Partner-URL ha restituito lo stato 400 per il messaggio con ID= Message-ID.`*	La comunicazione con il server AS2 del partner ha restituito un codice di risposta HTTP imprevisto. Il partner potrebbe essere in grado di fornire ulteriori diagnosi dai registri del server AS2.
`INSUFFICENT_MESSAGE_SECURITY_UNENCRYPTED`	È richiesta la crittografia.	Il partner ha inviato un messaggio non crittografato a Transfer Family, che non è supportato. Il mittente deve utilizzare un payload crittografato.
`INVALID_ENDPOINT_PROTOCOL`	Sono supportati solo HTTP e HTTPS.	È necessario specificare HTTP o HTTPS come protocollo nella configurazione del connettore AS2.

Codice	Errore	Descrizione e risoluzione
`INVALID_REQUEST`	1. C'è un problema con l'intestazione di un messaggio. 2. Impossibile analizzare il codice JSON segreto. Il formato JSON segreto non corrisponde al formato previsto. 3. Il segreto deve essere una stringa JSON. 4. Il nome utente non deve contenere i due punti. Il nome utente non deve contenere caratteri di controllo. Il nome utente deve contenere solo caratteri ASCII. La password non deve contenere caratteri di controllo. La password deve contenere solo caratteri ASCII.	Questo errore ha diverse cause. Le seguenti risoluzio ni corrispondono agli errori elencati nella colonna precedente. 1. Controlla i `as2-to` campi `as2-from` e. Assicurati che l'ID del messaggio originale sia corretto per il formato MDN. Assicurati inoltre che nel formato dell'ID del messaggio non manchi alcuna intestazione AS2. 2. Assicurati che il valore segreto corrisponda al formato documentato, come descritto in. Abilita l'autenticazione di base per i connettori AS2 3. Assicuratevi che il segreto sia fornito come stringa e non come file binario. 4. Apporta la correzione necessaria al nome utente o alla password.

Codice	Errore	Descrizione e risoluzione
INVALID_URL_FORMAT	*Formato URL non valido: URL*	Ciò si verifica quando si invia un messaggio in uscita utilizzando un connettore configurato con un URL non valido. Assicurati che il connettore sia configurato con un URL HTTP o HTTPS valido.
MDN_RESPONSE_INDICATES_AUTHENTICATION_FAILED	Non applicabile	Il destinatario non può autenticare il mittente. Il partner commerciale restituisce un MDN a Transfer Family con il modificatore di disposizione Error: authentication-failed.
MDN_RESPONSE_INDICATES_DECOMPRESSION_FAILED	Non applicabile	Ciò si verifica quando il destinatario non è in grado di decomprimere il contenuto del messaggio. Il partner commerciale restituisce un MDN a Transfer Family con il modificatore di disposizione Error: decompression-failed.
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	Non applicabile	Il destinatario non può decriptare il contenuto del messaggio. Il partner commerciale restituisce un MDN a Transfer Family con il modificatore di disposizione Error: authentication-failed.

Codice	Errore	Descrizione e risoluzione
`MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY`	Non applicabile	Il destinatario si aspetta che il messaggio sia firmato o crittografato, ma non è così. Il partner commerciale restituisce un MDN a Transfer Family con il modificatore di disposizione Error:. insufficient-message-security Abilita la firma e/o la crittografia sul connettore per soddisfare le aspettative del partner commerciale.
`MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED`	Non applicabile	Il ricevitore non può verificare l'integrità del contenuto. Il partner commerciale restituisce un MDN a Transfer Family con il modificatore di disposizione Error:. integrity-check-failed
`PATH_NOT_FOUND`	*`Impossibile creare il percorso del file di directory.`* Il percorso principale non è stato trovato.	Transfer Family sta tentando di creare una directory nel bucket Amazon S3 del cliente, ma il bucket non viene trovato. Assicurati che ogni percorso menzionato nel `StartFileTransfer` comando contenga il nome di un bucket esistente.

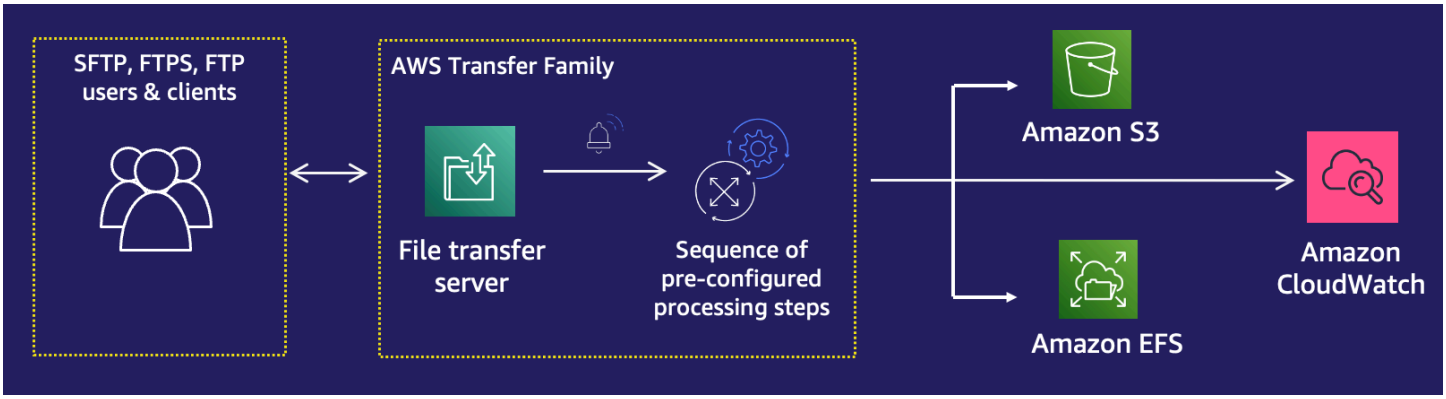
Codice	Errore	Descrizione e risoluzione
SEND_FILE_NOT_FOUND	Percorso del file *file-path* non trovato.	Transfer Family non riesce a localizzare il file durante l'operazione di invio del file. Verifica che la home directory e il percorso configurati siano validi e che Transfer Family disponga dei permessi di lettura per il file.
SERVER_NOT_FOUND	Impossibile trovare il server associato al messaggio.	Transfer Family non è riuscito a trovare il server quando ha ricevuto un messaggio. Questo può accadere se il server viene eliminato durante l'elaborazione di un messaggio in arrivo.
SERVER_NOT_ONLINE	Server *Server-ID non è online*.	Il server Transfer Family è offline. Avvia il server in modo che possa ricevere ed elaborare i messaggi.
SIGNING_FAILED	Impossibile firmare il file.	Il file da inviare non è disponibi le per la firma oppure non è stato possibile eseguire la firma. Verifica che il file si trovi nella posizione AS2 prevista e che AWS Transfer Family disponga dell'autorizzazione per leggerlo.

Codice	Errore	Descrizione e risoluzione
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	Nessun certificato trovato per il profilo: *local-profile-ID*.	Sto tentando di firmare un messaggio in uscita, ma non è stato trovato alcun certificato di firma per il profilo locale. Opzioni di risoluzione: • Assicurati che al profilo locale siano allegati un certificato e una chiave privata per la firma. • Assicurati che il certificato di firma sia attualmente attivo.
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	Impossibile convertire il nome host in indirizzi IP.	Transfer Family non è in grado di eseguire la risoluzione da DNS a indirizzo IP sul server DNS pubblico configurato nel connettore AS2. Aggiorna il connettore in modo che punti a un URL partner valido.
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	La connessione all'endpoint è scaduta.	Transfer Family non è in grado di stabilire una connessione socket al server AS2 del partner configurato. Verificate che il server AS2 del partner sia disponibile all'indirizzo IP configurato.

Codice	Errore	Descrizione e risoluzione
UNABLE_TO_RESOLVE_HOSTNAME	*Impossibile risolvere il nome host e il nome host.*	Il server Transfer Family non è riuscito a risolvere il nome host del partner utilizzando un server DNS pubblico. Verifica che l'host configurato sia registrato e che il record DNS abbia avuto il tempo di pubblicazione.
VERIFICATION_FAILED	La verifica della firma non è riuscita per il messaggio AS2 *Message-ID* o il codice MIC non corrisponde.	Verifica che il certificato di firma del mittente corrisponda ai certificati di firma del profilo remoto. Verifica anche che gli algoritmi MIC siano compatibili con. AWS Transfer Family
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	• Nel profilo: *Partner-Profile-ID* non è stato trovato alcun certificato pubblico corrispondente alla firma del messaggio. • *Impossibile ottenere certificati per il profilo inesistente: Partner-Profile-ID.* • *Nessun certificato valido è stato trovato nel profilo: Partner-Profile-ID.*	AWS Transfer Familysta tentando di verificare la firma di un messaggio ricevuto, ma non è stato trovato alcun certificato di firma corrispondente per il profilo partner. Opzioni di risoluzione: • Assicurati che al profilo del partner sia allegato un certificato di firma. • Assicurati che il certificato sia attualmente attivo. • Assicurati che il certificato di firma sia il certificato di firma corretto per il partner.

AWS Transfer Family flussi di lavoro gestiti

AWS Transfer Family supporta flussi di lavoro gestiti per l'elaborazione dei file. Con i flussi di lavoro gestiti, è possibile avviare un flusso di lavoro dopo che un file è stato trasferito tramite SFTP, FTPS o FTP. Utilizzando questa funzionalità, è possibile soddisfare in modo sicuro ed economico i requisiti di conformità per gli scambi di file business-to-business (B2B) coordinando tutti i passaggi necessari per l'elaborazione dei file. Inoltre, beneficiate del end-to-end controllo e della visibilità.



Orchestrando le attività di elaborazione dei file, i flussi di lavoro gestiti consentono di preelaborare i dati prima che vengano utilizzati dalle applicazioni downstream. Tali attività di elaborazione dei file potrebbero includere:

- Spostamento di file in cartelle specifiche dell'utente.
- Decrittografia dei file come parte di un flusso di lavoro.
- Etichettatura dei file.
- Esecuzione di un'elaborazione personalizzata creando e associando una AWS Lambda funzione a un flusso di lavoro.
- Invio di notifiche quando un file è stato trasferito con successo. (Per un post sul blog che descrive in dettaglio questo caso d'uso, consulta Personalizzare le notifiche di consegna dei file utilizzando flussi di lavoro AWS Transfer Family gestiti.)

Per replicare e standardizzare rapidamente le comuni attività di elaborazione dei file post-caricamento che coinvolgono più unità aziendali dell'organizzazione, è possibile implementare flussi di lavoro utilizzando l'infrastruttura come codice (IaC). È possibile specificare un flusso di lavoro gestito da avviare sui file caricati per intero. È inoltre possibile specificare un flusso di lavoro gestito diverso da avviare sui file caricati solo parzialmente a causa di una disconnessione prematura della sessione. La gestione integrata delle eccezioni consente di reagire rapidamente ai risultati

dell'elaborazione dei file, offrendo al contempo il controllo sulla gestione degli errori. Inoltre, ogni fase del flusso di lavoro produce registri dettagliati, che è possibile controllare per tracciare la derivazione dei dati.

Per iniziare, esegui le seguenti attività:

1. Configura il flusso di lavoro in modo che contenga azioni di preelaborazione, come copia, etichettatura e altri passaggi in base alle tue esigenze. Per informazioni dettagliate, vedi Crea un flusso di lavoro.
2. Configura un ruolo di esecuzione, che Transfer Family utilizza per eseguire il flusso di lavoro. Per informazioni dettagliate, vedi Politiche IAM per i flussi di lavoro.
3. Mappa il flusso di lavoro su un server, in modo che all'arrivo del file, le azioni specificate in questo flusso di lavoro vengano valutate e avviate in tempo reale. Per informazioni dettagliate, vedi Configura ed esegui un flusso di lavoro.

Informazioni correlate

- Per monitorare le esecuzioni del flusso di lavoro, consulta. Utilizzo delle CloudWatch metriche per Transfer Family
- Per i registri di esecuzione dettagliati e le informazioni sulla risoluzione dei problemi, vedere. Risolvi gli errori relativi al flusso di lavoro utilizzando Amazon CloudWatch
- Transfer Family offre un post sul blog e un workshop che ti guidano nella creazione di una soluzione per il trasferimento di file. Questa soluzione sfrutta gli endpoint SFTP/FTPS gestiti e Amazon Cognito e DynamoDB AWS Transfer Family per la gestione degli utenti.

  Il post del blog è disponibile in Utilizzo di Amazon Cognito come provider di identità con AWS Transfer Family Amazon S3. Puoi visualizzare i dettagli del workshop qui.
- Visualizza AWS Transfer Family Managed Workflows per una breve introduzione ai flussi di lavoro Transfer Family.

Argomenti

- Crea un flusso di lavoro
- Utilizza passaggi predefiniti
- Utilizza passaggi di elaborazione dei file personalizzati
- Politiche IAM per i flussi di lavoro

- Gestione delle eccezioni per un flusso di lavoro
- Monitora l'esecuzione del workflow
- Creare un flusso di lavoro a partire da un modello
- Rimuovere un flusso di lavoro da un server Transfer Family
- Restrizioni e limitazioni dei flussi di lavoro gestiti

Per ulteriori informazioni su come iniziare a utilizzare i flussi di lavoro gestiti, consulta le seguenti risorse:

- AWS Transfer Family video dimostrativo sui flussi di lavoro gestiti
- Creazione di una piattaforma di trasferimento file nativa per il cloud utilizzando AWS Transfer Family i flussi di lavoro (post sul blog)

Crea un flusso di lavoro

È possibile creare un flusso di lavoro gestito utilizzando AWS Management Console, come descritto in questo argomento. Per rendere il processo di creazione del flusso di lavoro il più semplice possibile, sono disponibili pannelli di aiuto contestuali per la maggior parte delle sezioni della console.

Un flusso di lavoro prevede due tipi di passaggi:

- Passaggi nominali: i passaggi nominali sono passaggi di elaborazione dei file che si desidera applicare ai file in entrata. Se si seleziona più di un passaggio nominale, ogni passaggio viene elaborato in una sequenza lineare.
- Fasi di gestione delle eccezioni: i gestori delle eccezioni sono fasi di elaborazione dei file che vengono AWS Transfer Family eseguite nel caso in cui alcuni passaggi nominali falliscano o causino errori di convalida.

Crea un flusso di lavoro

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Flussi di lavoro.
3. Nella pagina Flussi di lavoro, scegli Crea flusso di lavoro.
4. Nella pagina Crea flusso di lavoro, inserisci una descrizione. Questa descrizione viene visualizzata nella pagina Flussi di lavoro.

5. Nella sezione Passaggi nominali, scegli Aggiungi passaggio. Aggiungi uno o più passaggi.

    a. Scegli un tipo di passaggio tra le opzioni disponibili. Per ulteriori informazioni sui vari tipi di fasi, vederethe section called “Utilizza passaggi predefiniti”.

    b. Scegli Avanti, quindi configura i parametri per la fase.

    c. Scegli Avanti, quindi esamina i dettagli del passaggio.

    d. Scegli Crea passaggio per aggiungere il passaggio e continuare.

    e. Continua ad aggiungere i passaggi secondo necessità. Il numero massimo di passaggi in un flusso di lavoro è 8.

    f. Dopo aver aggiunto tutti i passaggi nominali necessari, scorri verso il basso fino alla sezione Gestori delle eccezioni — opzionale e scegli Aggiungi passaggio.

    > **Note**
    >
    > Per essere informati degli errori in tempo reale, ti consigliamo di configurare i gestori delle eccezioni e i passaggi da eseguire in caso di errore del flusso di lavoro.

6. Per configurare i gestori delle eccezioni, aggiungi i passaggi nello stesso modo descritto in precedenza. Se un file fa sì che un passaggio generi un'eccezione, i gestori delle eccezioni vengono richiamati uno per uno.
7. (Facoltativo) Scorri verso il basso fino alla sezione Tag e aggiungi tag per il tuo flusso di lavoro.
8. Controlla la configurazione e scegli Crea flusso di lavoro.

> **Important**
>
> Dopo aver creato un flusso di lavoro, non puoi modificarlo, quindi assicurati di rivedere attentamente la configurazione.

Configura ed esegui un flusso di lavoro

Prima di poter eseguire un flusso di lavoro, è necessario associarlo a un server Transfer Family.

Per configurare Transfer Family per eseguire un flusso di lavoro sui file caricati

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server.

- Per aggiungere il flusso di lavoro a un server esistente, scegli il server che desideri utilizzare per il flusso di lavoro.
- In alternativa, crea un nuovo server e aggiungici il flusso di lavoro. Per ulteriori informazioni, consulta Configurazione di un endpoint server SFTP, FTPS o FTP.

3. Nella pagina dei dettagli del server, scorri verso il basso fino alla sezione Dettagli aggiuntivi, quindi scegli Modifica.

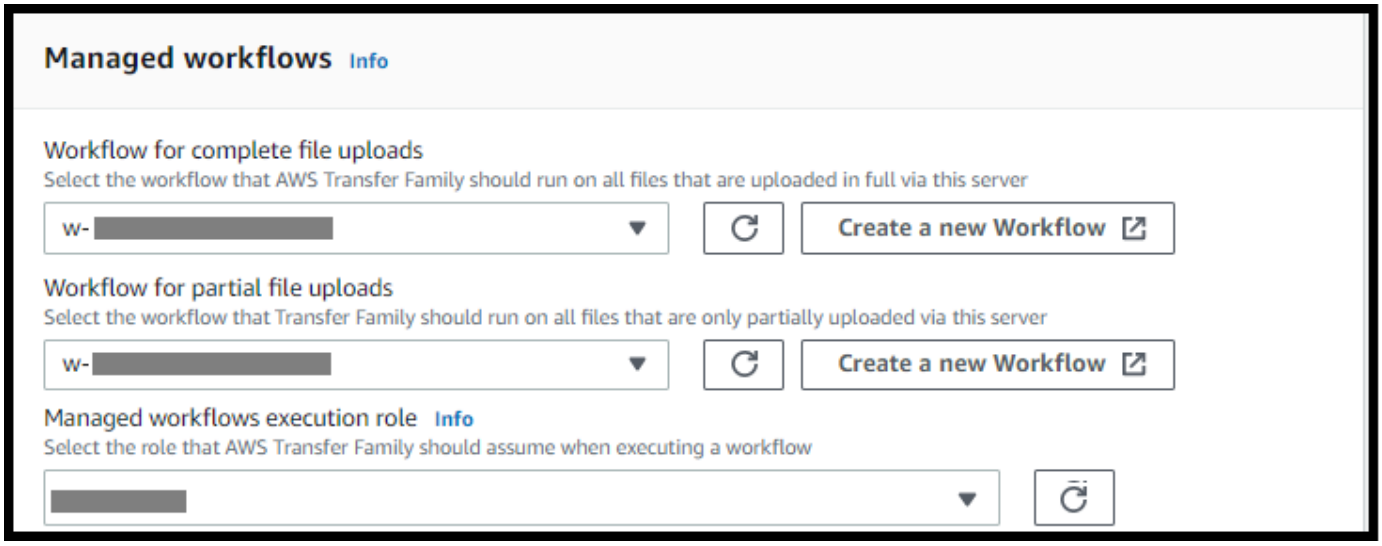
> **Note**
>
> Per impostazione predefinita, ai server non è associato alcun flusso di lavoro. La sezione Dettagli aggiuntivi viene utilizzata per associare un flusso di lavoro al server selezionato.

4. Nella pagina Modifica dettagli aggiuntivi, nella sezione Flussi di lavoro gestiti, seleziona un flusso di lavoro da eseguire su tutti i caricamenti.

> **Note**
>
> Se non disponi già di un flusso di lavoro, scegli Crea un nuovo flusso di lavoro per crearne uno.

   a. Scegli l'ID del flusso di lavoro da utilizzare.

   b. Scegli un ruolo di esecuzione. Questo è il ruolo che Transfer Family assume durante l'esecuzione dei passaggi del flusso di lavoro. Per ulteriori informazioni, consulta Politiche IAM per i flussi di lavoro. Seleziona Save (Salva.



> **Note**
>
> Se non desideri più associare un flusso di lavoro al server, puoi rimuovere l'associazione. Per informazioni dettagliate, vedi Rimuovere un flusso di lavoro da un server Transfer Family.

Per eseguire un flusso di lavoro

Per eseguire un flusso di lavoro, carichi un file su un server Transfer Family configurato con un flusso di lavoro associato.

> **Note**
>
> Ogni volta che rimuovi un flusso di lavoro da un server e lo sostituisci con uno nuovo o aggiorni la configurazione del server (che influisce sul ruolo di esecuzione di un flusso di lavoro), devi attendere circa 10 minuti prima di eseguire il nuovo flusso di lavoro. Il server Transfer Family memorizza nella cache i dettagli del flusso di lavoro e il server impiega 10 minuti per aggiornare la cache.
> Inoltre, è necessario disconnettersi da tutte le sessioni SFTP attive e quindi riconnettersi dopo il periodo di attesa di 10 minuti per visualizzare le modifiche.

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
>
```

Dopo che il file è stato caricato, l'azione definita viene eseguita sul file. Ad esempio, se il flusso di lavoro contiene una fase di copia, il file viene copiato nella posizione definita in quel passaggio. Puoi utilizzare Amazon CloudWatch Logs per tenere traccia dei passaggi eseguiti e del loro stato di esecuzione.

Visualizza i dettagli del flusso di lavoro

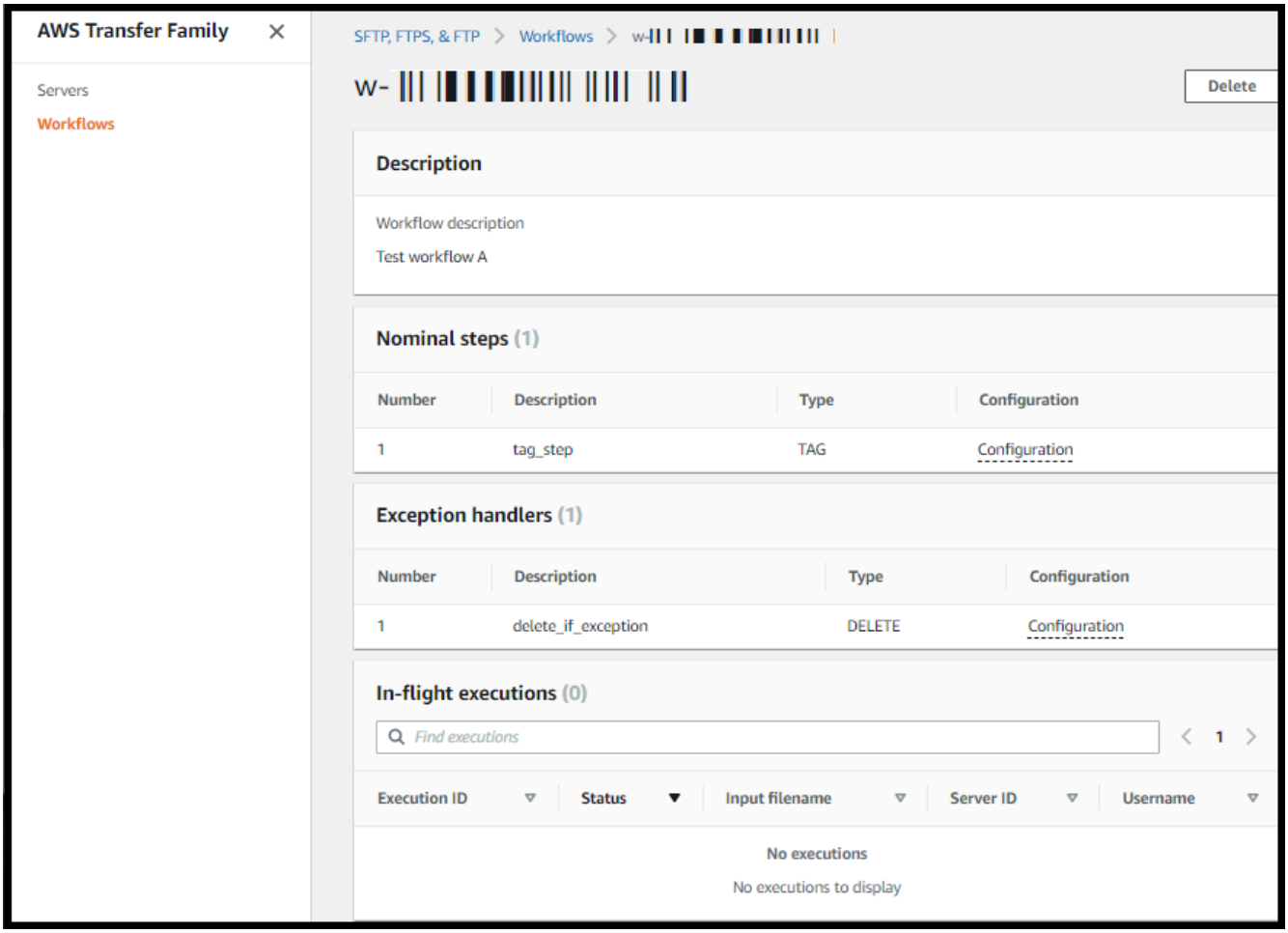
È possibile visualizzare i dettagli sui flussi di lavoro creati in precedenza o sulle esecuzioni dei flussi di lavoro. Per visualizzare questi dettagli, è possibile utilizzare la console o il pulsante AWS Command Line Interface ()AWS CLI.

Console

Visualizza i dettagli del flusso di lavoro

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Flussi di lavoro.
3. Nella pagina Flussi di lavoro, scegli un flusso di lavoro.

   Viene visualizzata la pagina dei dettagli del flusso di lavoro.



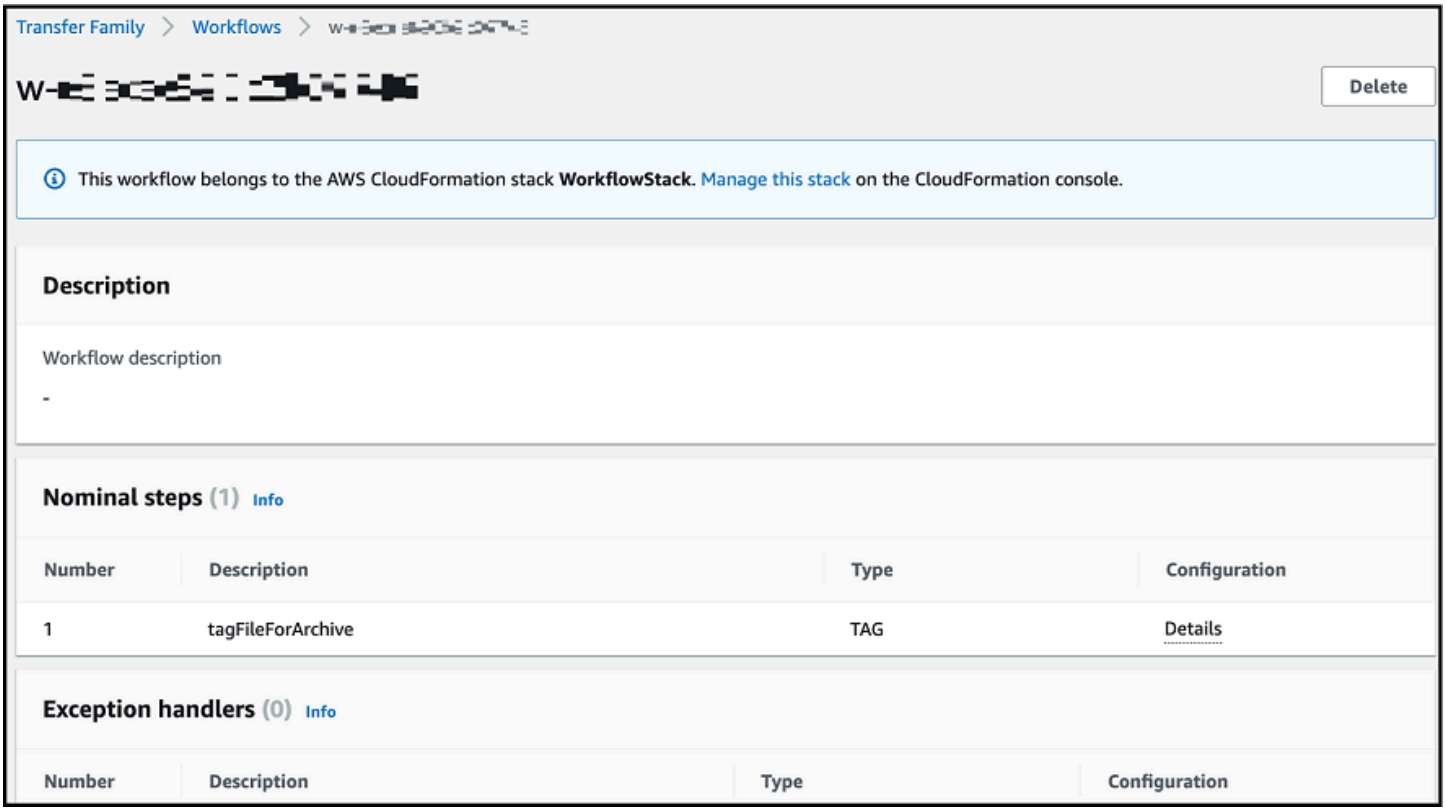
CLI

Per visualizzare i dettagli del flusso di lavoro, utilizzate il comando `describe-workflow` CLI, come illustrato nell'esempio seguente. Sostituisci l'ID del flusso di lavoro *w-1234567890abcdef0* con il tuo valore. Per ulteriori informazioni, consulta describe-workflow nel Command Reference.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": {}
    }
}
```

Se il flusso di lavoro è stato creato come parte di uno AWS CloudFormation stack, puoi gestirlo utilizzando la AWS CloudFormation console (https://console.aws.amazon.com/cloudformation).



Utilizza passaggi predefiniti

Quando crei un flusso di lavoro, puoi scegliere di aggiungere uno dei seguenti passaggi predefiniti descritti in questo argomento. Puoi anche scegliere di aggiungere fasi personalizzate di elaborazione dei file. Per ulteriori informazioni, consulta the section called “Utilizza passaggi di elaborazione dei file personalizzati”.

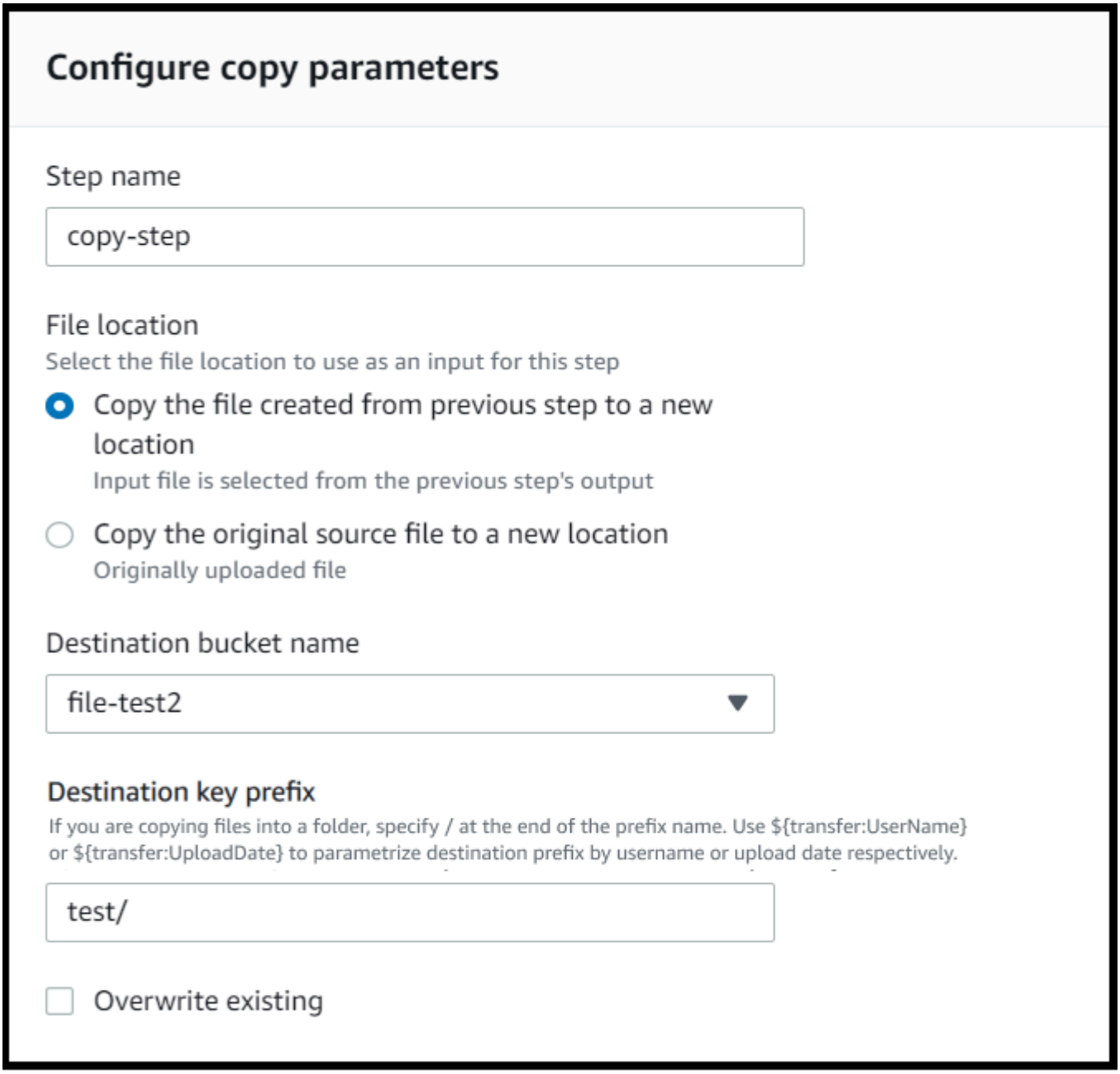
Argomenti

Copia il file

Una fase di copia del file crea una copia del file caricato in una nuova posizione Amazon S3. Attualmente, puoi utilizzare una fase di copia del file solo con Amazon S3.

La seguente fase di copia del file copia i file nella `test` cartella nel bucket di `file-test` destinazione.

Se la fase di copia del file non è la prima fase del flusso di lavoro, puoi specificare la posizione del file. Specificando la posizione del file, è possibile copiare il file utilizzato nel passaggio precedente o il file originale caricato. È possibile utilizzare questa funzione per creare più copie del file originale mantenendo intatto il file di origine per l'archiviazione dei file e la conservazione dei record. Per vedere un esempio, consulta Esempio di flusso di lavoro di etichettatura ed eliminazione.



Fornisci il bucket e i dettagli chiave

È necessario fornire il nome del bucket e una chiave per la destinazione della fase di copia del file. La chiave può essere un nome di percorso o un nome di file. Il fatto che la chiave venga considerata come un nome di percorso o un nome di file dipende dal fatto che terminiate la chiave con il carattere forward slash (/).

Se il carattere finale è/, il file viene copiato nella cartella e il suo nome non cambia. Se il carattere finale è alfanumerico, il file caricato viene rinominato con il valore chiave. In questo caso, se esiste

già un file con quel nome, il comportamento dipende dall'impostazione del campo Sovrascrivi esistente.

- Se è selezionato Sovrascrivi esistente, il file esistente viene sostituito con il file in fase di elaborazione.
- Se l'opzione Sovrascrivi esistente non è selezionata, non succede nulla e l'elaborazione del flusso di lavoro si interrompe.

> **Tip**
>
> Se le scritture simultanee vengono eseguite sullo stesso percorso del file, è possibile che si verifichi un comportamento imprevisto durante la sovrascrittura dei file.

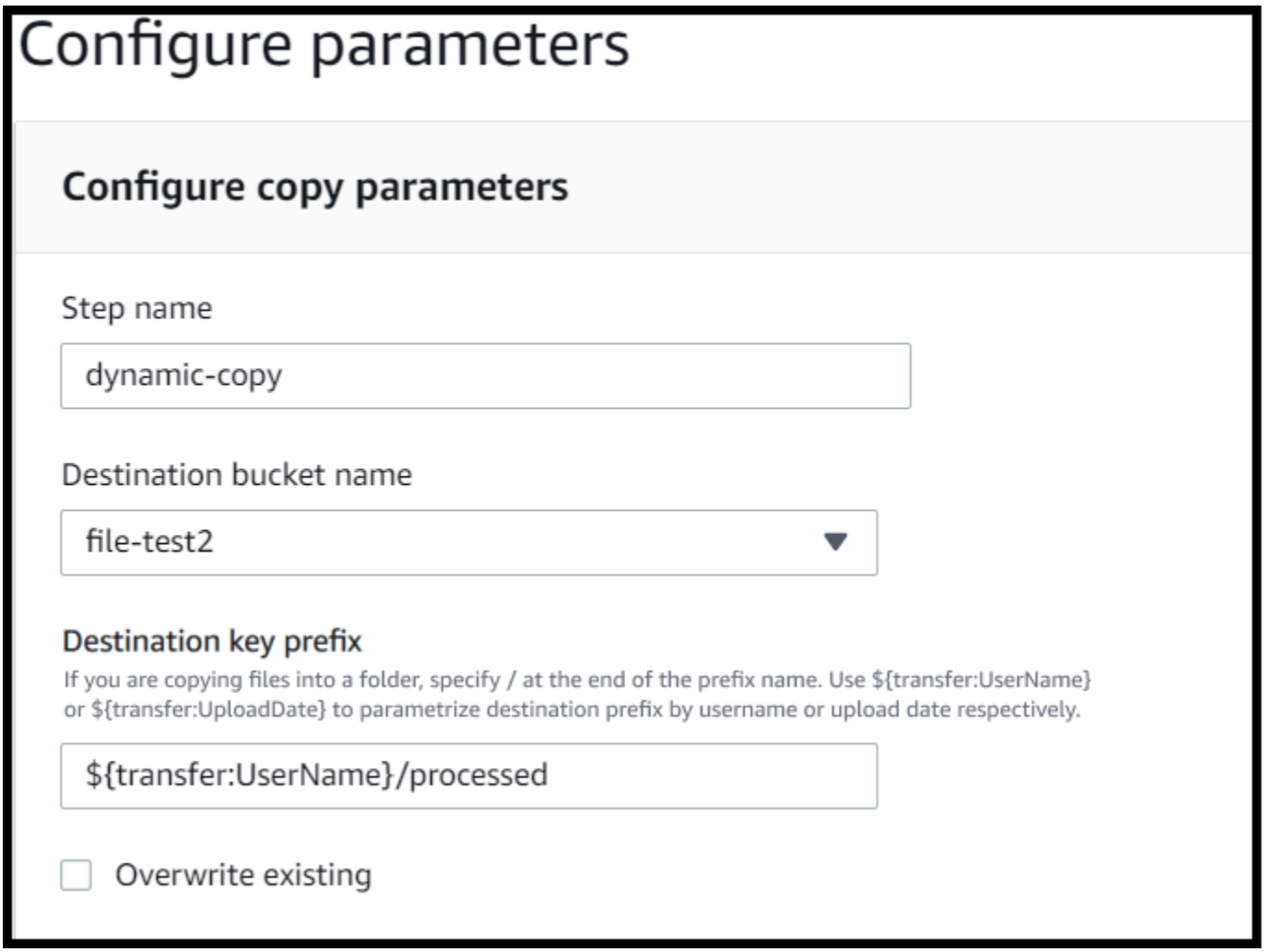
Ad esempio, se il valore chiave è`test/`, i file caricati vengono copiati nella cartella. `test` Se il valore della chiave è`test/today`, (e l'opzione Sovrascrivi esistente è selezionata) ogni file caricato viene copiato in un file denominato `today` nella `test` cartella e ogni file successivo sovrascrive quello precedente.

> **Note**
>
> Amazon S3 supporta i bucket e gli oggetti e non sono presenti gerarchie. Tuttavia, puoi utilizzare prefissi e delimitatori nei nomi delle chiavi degli oggetti per creare una gerarchia e organizzare i dati in modo simile alle cartelle.

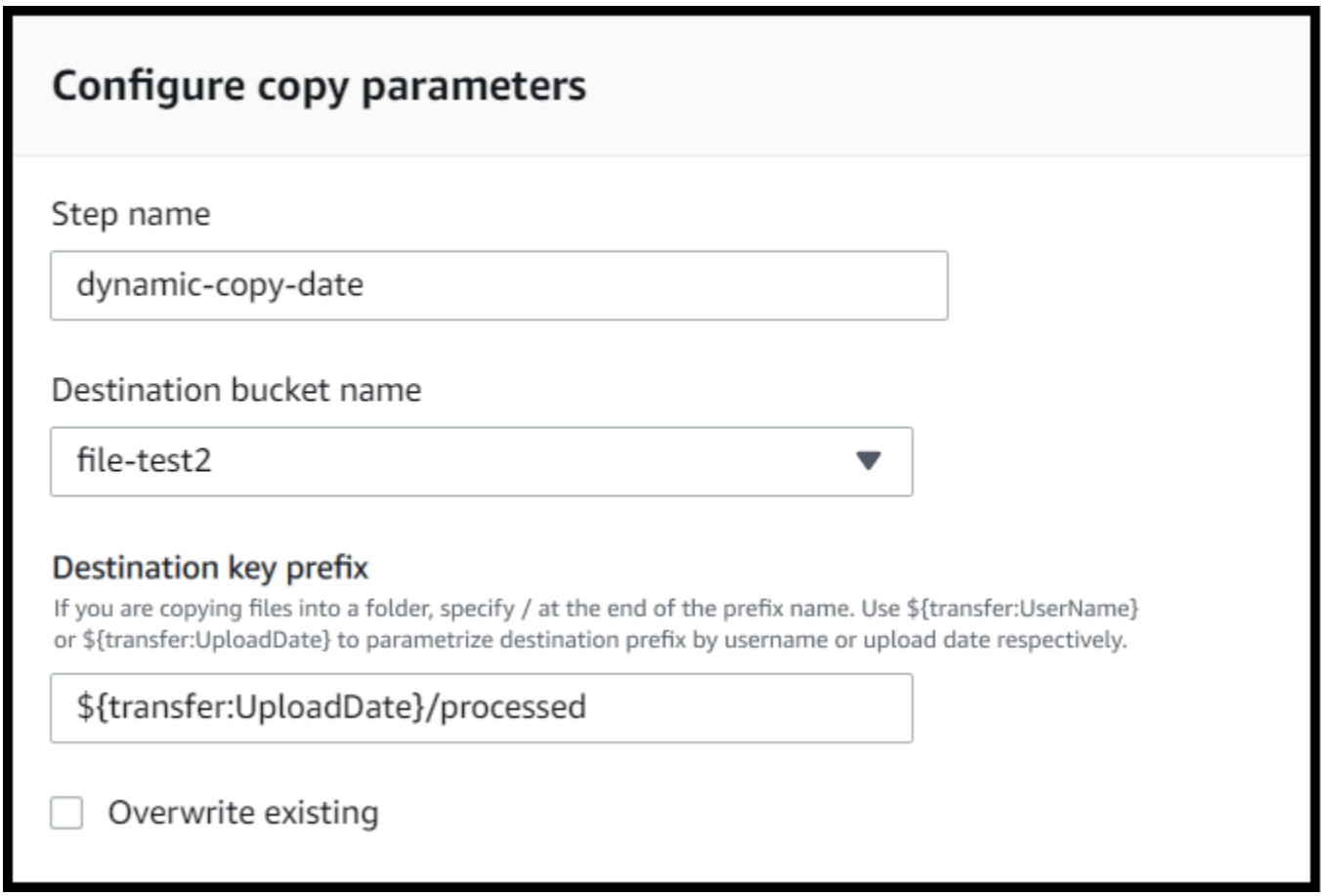
Utilizzate una variabile denominata in una fase di copia del file

In una fase di copia del file, è possibile utilizzare una variabile per copiare dinamicamente i file in cartelle specifiche dell'utente. Attualmente, puoi utilizzare `${transfer:UserName}` or `${transfer:UploadDate}` come variabile per copiare i file in una posizione di destinazione per un determinato utente che sta caricando i file o in base alla data corrente.

Nell'esempio seguente, se l'utente `richard-roe` carica un file, questo viene copiato nella cartella. `file-test2/richard-roe/processed/` Se l'utente `mary-major` carica un file, questo viene copiato nella cartella. `file-test2/mary-major/processed/`



Allo stesso modo, è possibile utilizzarli `${transfer:UploadDate}` come variabile per copiare i file in una posizione di destinazione denominata in base alla data corrente. Nell'esempio seguente, se impostate la destinazione `${transfer:UploadDate}/processed` sul 1° febbraio 2022, i file caricati vengono copiati nella `file-test2/2022-02-01/processed/` cartella.



È inoltre possibile utilizzare entrambe queste variabili insieme, combinando le loro funzionalità. Per esempio:

- È possibile impostare il prefisso della chiave di destinazione su**`folder/${transfer:UserName}/${transfer:UploadDate}/`**, ad esempio per creare cartelle annidate. `folder/marymajor/2023-01-05/`
- È possibile impostare il prefisso della chiave di destinazione su**`folder/${transfer:UserName}-${transfer:UploadDate}/`**, ad esempio per concatenare le due variabili. `folder/marymajor-2023-01-05/`

Autorizzazioni IAM per la fase di copia

Per consentire il completamento di una fase di copia, assicurati che il ruolo di esecuzione per il tuo flusso di lavoro contenga le seguenti autorizzazioni.

```
{
            "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**
>
> L'`s3:ListBucket`autorizzazione è necessaria solo se non si seleziona Sovrascrivi esistente. Questa autorizzazione controlla il tuo bucket per vedere se esiste già un file con lo stesso nome. Se hai selezionato Sovrascrivi esistente, non è necessario che il flusso di lavoro verifichi la presenza del file e può semplicemente scriverlo.
> Se i tuoi file Amazon S3 hanno tag, devi aggiungere una o due autorizzazioni alla tua policy IAM.
>
> - Aggiungi `s3:GetObjectTagging` per un file Amazon S3 senza versione.
> - Aggiungi `s3:GetObjectVersionTagging` per un file Amazon S3 con versione.

Decrittografa il file

Il blog AWS sullo storage ha un post che descrive come decrittografare semplicemente i file senza scrivere alcun codice utilizzando i flussi di lavoro Transfer Family Managed, crittografare e decrittografare i file con PGP e. AWS Transfer Family

Usa la decrittografia PGP nel tuo flusso di lavoro

Transfer Family ha il supporto integrato per la decrittografia Pretty Good Privacy (PGP). Puoi utilizzare la decrittografia PGP su file caricati tramite SFTP, FTPS o FTP su Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS).

Per utilizzare la decrittografia PGP, devi creare e archiviare le chiavi private PGP che verranno utilizzate per la decrittografia dei tuoi file. I tuoi utenti possono quindi crittografare i file utilizzando le chiavi di crittografia PGP corrispondenti prima di caricare i file sul server Transfer Family. Dopo aver ricevuto i file crittografati, puoi decrittografarli nel tuo flusso di lavoro. Per un tutorial dettagliato, consulta Configurazione di un flusso di lavoro gestito per la decrittografia di un file.

Per utilizzare la decrittografia PGP nel flusso di lavoro

1. Identifica un server Transfer Family per ospitare il tuo flusso di lavoro o creane uno nuovo. È necessario disporre dell'ID del server prima di poter memorizzare le chiavi PGP AWS Secrets Manager con il nome segreto corretto.
2. Memorizza la tua chiave PGP AWS Secrets Manager con il nome segreto richiesto. Per informazioni dettagliate, vedi Gestire le chiavi PGP. I flussi di lavoro possono individuare automaticamente la chiave PGP corretta da utilizzare per la decrittografia in base al nome segreto in Secrets Manager.

   > **Note**
   >
   > Quando memorizzi segreti in Secrets Manager, ti vengono Account AWS addebitati dei costi. Per informazioni sui prezzi, consulta Prezzi di AWS Secrets Manager.

3. Crittografa un file usando la tua coppia di chiavi PGP. (Per un elenco dei client supportati, consulta.) Client PGP supportati Se stai usando la riga di comando, esegui il comando seguente. Per usare questo comando, sostituiscilo *username@example.com* con l'indirizzo email che hai usato per creare la coppia di key pair PGP. Sostituisci *testfile.txt* con il nome del file che desideri crittografare.

   ```
   gpg -e -r username@example.com testfile.txt
   ```

4. Carica il file crittografato sul tuo server Transfer Family.
5. Configura una fase di decrittografia nel tuo flusso di lavoro. Per ulteriori informazioni, consulta Aggiungi una fase di decrittografia.

Aggiungi una fase di decrittografia

Una fase di decrittografia decrittografa un file crittografato che è stato caricato su Amazon S3 o Amazon EFS come parte del tuo flusso di lavoro. Per dettagli sulla configurazione della decrittografia, consulta. Usa la decrittografia PGP nel tuo flusso di lavoro

Quando si crea la fase di decrittografia per un flusso di lavoro, è necessario specificare la destinazione dei file decrittografati. È inoltre necessario selezionare se sovrascrivere i file esistenti se un file esiste già nella posizione di destinazione. Puoi monitorare i risultati del flusso di lavoro di decrittografia e ottenere log di controllo per ogni file in tempo reale utilizzando Amazon Logs. CloudWatch

Dopo aver scelto il tipo di file Decrypt per il passaggio, viene visualizzata la pagina Configura parametri. Inserisci i valori per la sezione Configura i parametri di decrittografia PGP.

Le opzioni disponibili sono le seguenti:

- Nome della fase: immettere un nome descrittivo per la fase.
- Posizione del file: specificando la posizione del file, è possibile decrittografare il file utilizzato nel passaggio precedente o il file originale caricato.

  > **Note**
  >
  > Questo parametro non è disponibile se questo passaggio è il primo passaggio del flusso di lavoro.

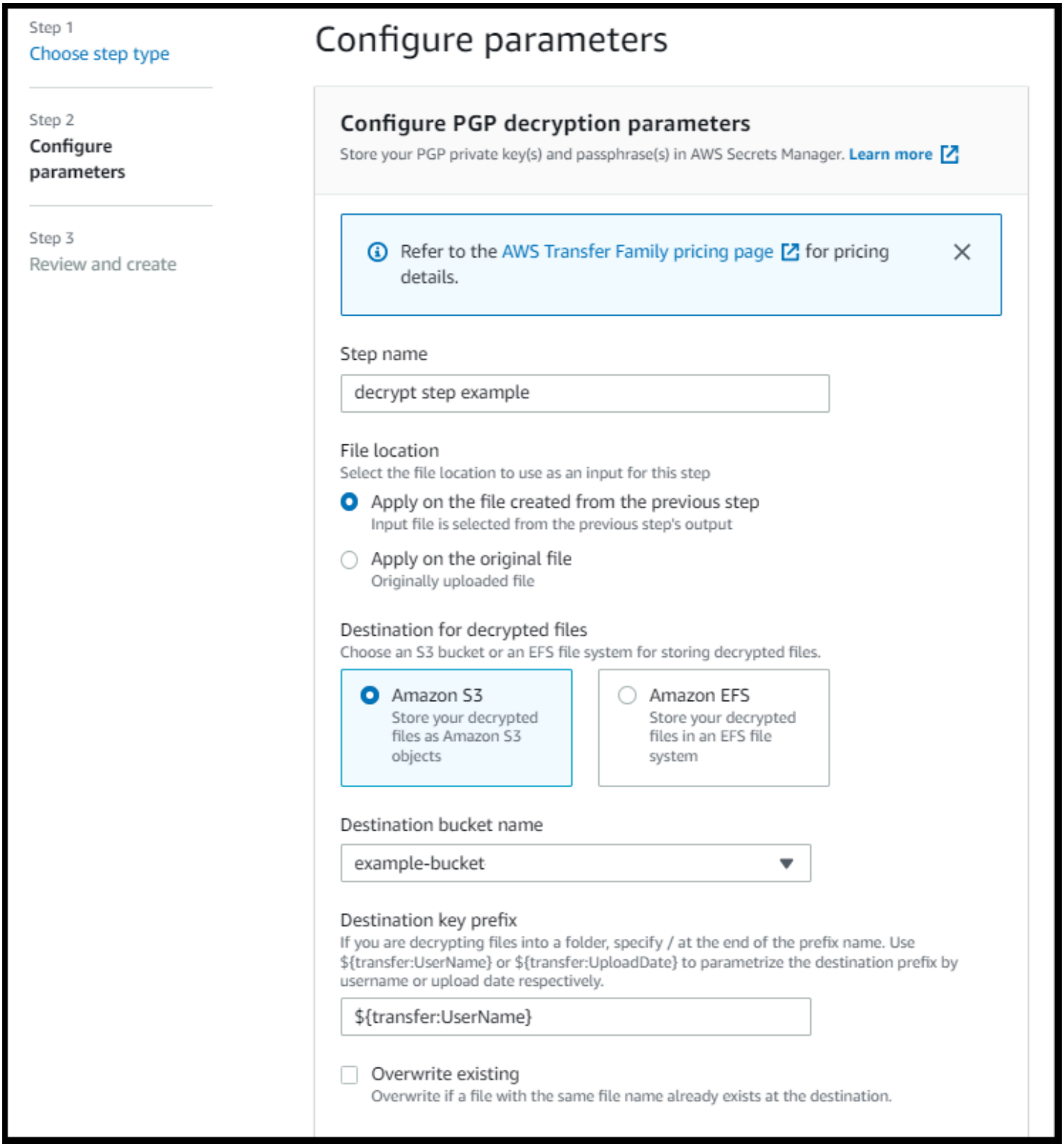
- Destinazione per i file decrittografati: scegli un bucket Amazon S3 o un file system Amazon EFS come destinazione per il file decrittografato.
  - Se scegli Amazon S3, devi fornire un nome del bucket di destinazione e un prefisso della chiave di destinazione. Per parametrizzare il prefisso della chiave di destinazione in base al nome utente, **`${transfer:UserName}`** immettete Destination key prefix. Analogamente, per parametrizzare il prefisso della chiave di destinazione in base alla data di caricamento, **`${Transfer:UploadDate}`** immettete Destination key prefix.
  - Se scegli Amazon EFS, devi fornire un file system e un percorso di destinazione.

> **Note**
>
> L'opzione di archiviazione scelta qui deve corrispondere al sistema di storage utilizzato dal server Transfer Family a cui è associato questo flusso di lavoro. In caso contrario, riceverai un errore quando tenterai di eseguire questo flusso di lavoro.

- Sovrascrivi file esistenti: se carichi un file e nella destinazione esiste già un file con lo stesso nome, il comportamento dipende dall'impostazione di questo parametro:
  - Se si seleziona Sovrascrivi esistente, il file esistente viene sostituito con il file in fase di elaborazione.
  - Se l'opzione Sovrascrivi esistente non è selezionata, non succede nulla e l'elaborazione del flusso di lavoro si interrompe.

> **Tip**
>
> Se le scritture simultanee vengono eseguite sullo stesso percorso del file, è possibile che si verifichi un comportamento imprevisto durante la sovrascrittura dei file.

La schermata seguente mostra un esempio delle opzioni che è possibile scegliere per la fase di decrittografia del file.


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.

Autorizzazioni IAM per la fase di decrittografia

Per consentire il successo di una fase di decrittografia, assicurati che il ruolo di esecuzione per il tuo flusso di lavoro contenga le seguenti autorizzazioni.

```
{
            "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**
>
> L'**`s3:ListBucket`**autorizzazione è necessaria solo se non si seleziona Sovrascrivi esistente. Questa autorizzazione controlla il tuo bucket per vedere se esiste già un file con lo stesso nome. Se hai selezionato Sovrascrivi esistente, non è necessario che il flusso di lavoro verifichi la presenza del file e può semplicemente scriverlo.

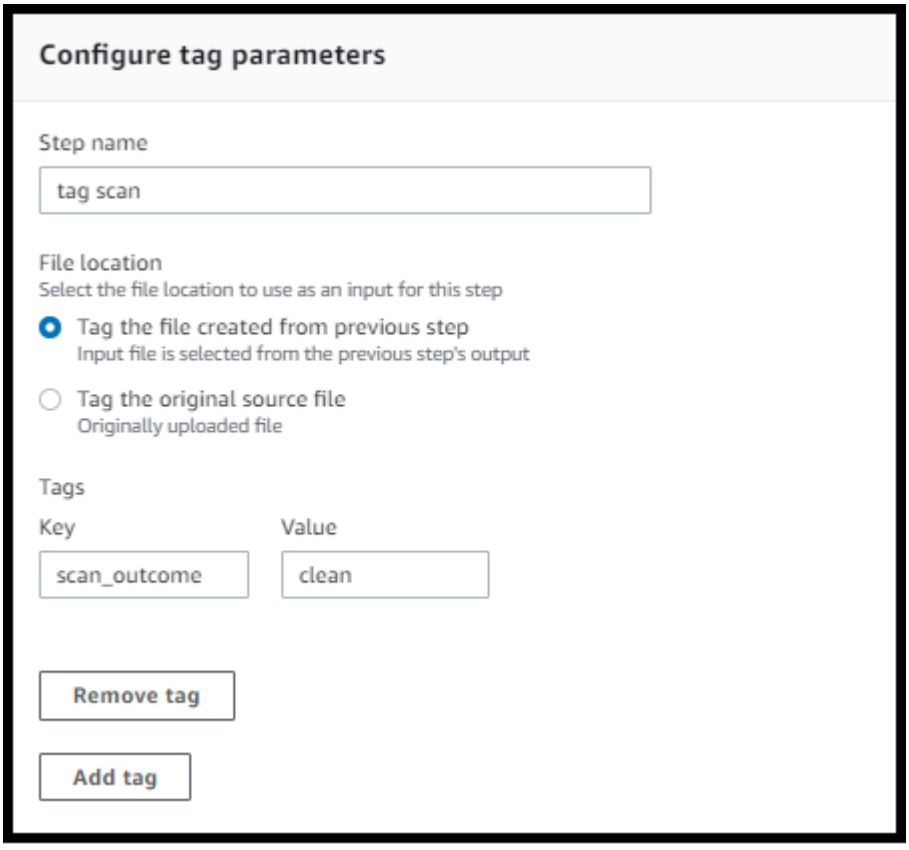
Se i tuoi file Amazon S3 hanno tag, devi aggiungere una o due autorizzazioni alla tua policy IAM.

- Aggiungi `s3:GetObjectTagging` per un file Amazon S3 senza versione.
- Aggiungi `s3:GetObjectVersionTagging` per un file Amazon S3 con versione.

Tag: file

Per etichettare i file in arrivo per un'ulteriore elaborazione a valle, utilizzate un passaggio di tag. Immettete il valore del tag che desiderate assegnare ai file in arrivo. Attualmente, l'operazione di tag è supportata solo se utilizzi Amazon S3 per lo storage del server Transfer Family.

Il seguente esempio di tag step assegna `scan_outcome` e `clean` come tag, rispettivamente, la chiave e il valore.



Per consentire il completamento di una fase di tag, assicurati che il ruolo di esecuzione per il tuo flusso di lavoro contenga le seguenti autorizzazioni.

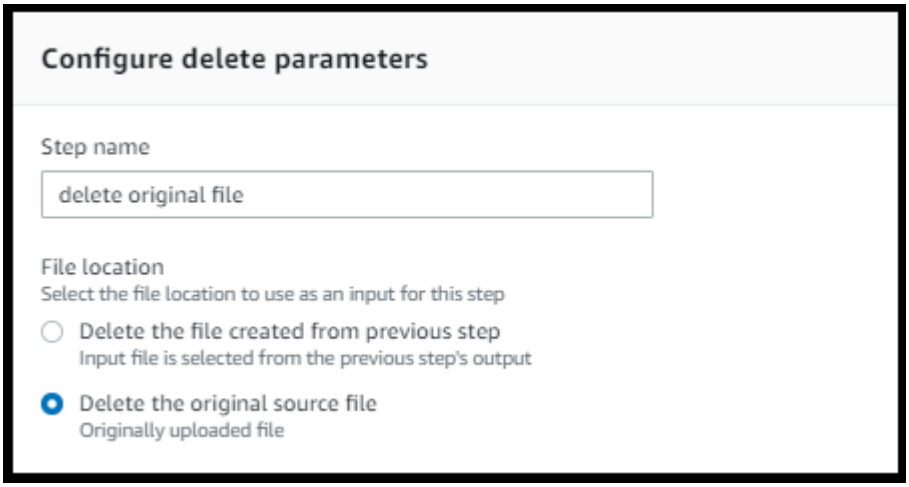
```
{
```

```
            "Sid": "Tag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
}
```

> **Note**
>
> Se il flusso di lavoro contiene un'istruzione di tag che viene eseguita prima di una fase di copia o decrittografia, devi aggiungere una o due autorizzazioni alla tua policy IAM.
>
> - Aggiungi `s3:GetObjectTagging` per un file Amazon S3 senza versione.
> - Aggiungi `s3:GetObjectVersionTagging` per un file Amazon S3 con versione.

Eliminare il file

Per eliminare un file elaborato da una fase precedente del flusso di lavoro o per eliminare il file originariamente caricato, utilizzate un passaggio di eliminazione del file.



Per consentire il completamento di un passaggio di eliminazione, assicurati che il ruolo di esecuzione per il tuo flusso di lavoro contenga le seguenti autorizzazioni.

```
{
```

```
            "Sid": "Delete",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
*"
        }
```

Variabili denominate per i flussi di lavoro

Per le fasi di copia e decrittografia, puoi utilizzare una variabile per eseguire azioni in modo dinamico. Attualmente, AWS Transfer Family supporta le seguenti variabili denominate.

- Consente `${transfer:UserName}` di copiare o decrittografare i file in una destinazione in base all'utente che carica i file.
- `${transfer:UploadDate}`Da utilizzare per copiare o decrittografare i file in una posizione di destinazione in base alla data corrente.

Esempio di flusso di lavoro di etichettatura ed eliminazione

L'esempio seguente illustra un flusso di lavoro che contrassegna i file in entrata che devono essere elaborati da un'applicazione a valle, ad esempio una piattaforma di analisi dei dati. Dopo aver taggato il file in arrivo, il flusso di lavoro elimina quindi il file originariamente caricato per risparmiare sui costi di archiviazione.

Console

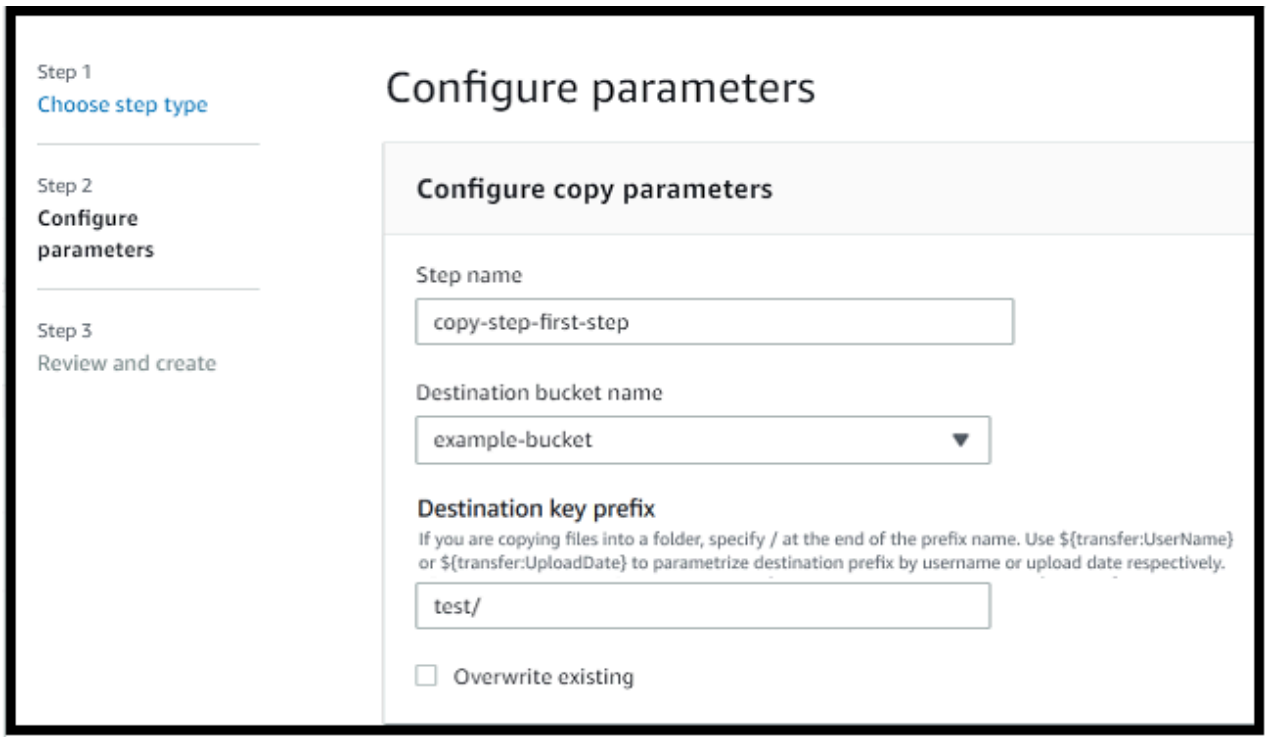
Esempio di flusso di lavoro con tag e spostamento

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Flussi di lavoro.
3. Nella pagina Flussi di lavoro, scegli Crea flusso di lavoro.
4. Nella pagina Crea flusso di lavoro, inserisci una descrizione. Questa descrizione viene visualizzata nella pagina Flussi di lavoro.
5. Aggiungi il primo passaggio (copia).

    a. Nella sezione Passaggi nominali, scegli Aggiungi passaggio.

b. Scegli Copia file, quindi scegli Avanti.

c. Inserisci un nome per la fase, quindi seleziona un bucket di destinazione e un key prefix.



d. Scegli Avanti, quindi esamina i dettagli del passaggio.

e. Scegli Crea passaggio per aggiungere il passaggio e continuare.

6. Aggiungi il secondo passaggio (tag).

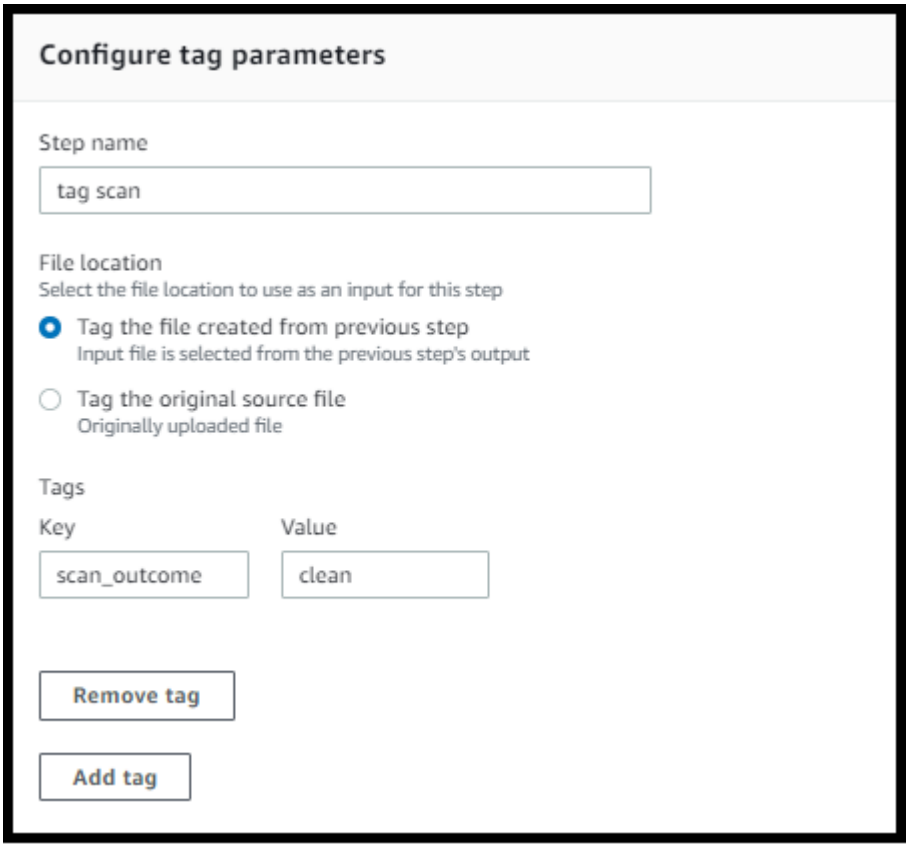
a. Nella sezione Passaggi nominali, scegli Aggiungi passaggio.

b. Scegli Tag file, quindi scegli Avanti.

c. Inserisci un nome per la fase.

d. In Posizione del file, seleziona Etichetta il file creato nel passaggio precedente.

e. Inserisci una Key (chiave) e un Value (valore).



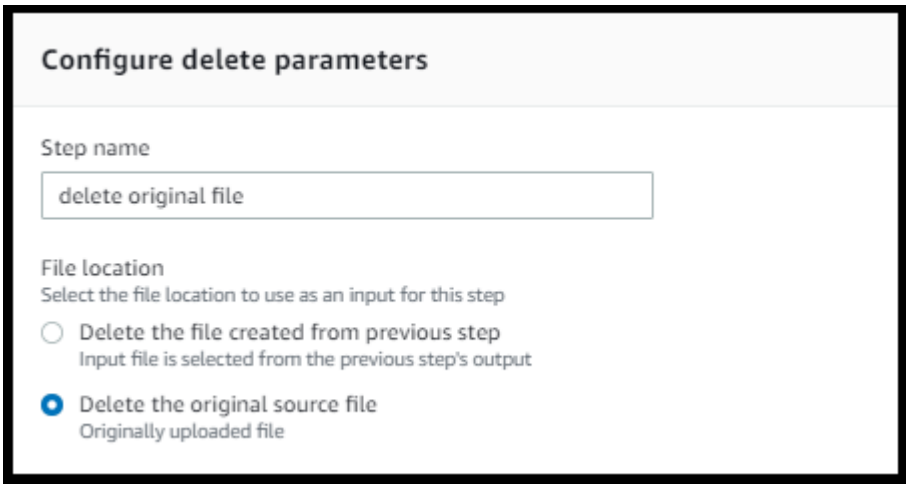
f. Scegli Avanti, quindi esamina i dettagli del passaggio.

g. Scegli Crea passaggio per aggiungere il passaggio e continuare.

7. Aggiungi il terzo passaggio (elimina).

a. Nella sezione Passaggi nominali, scegli Aggiungi passaggio.

b. Scegli Elimina file, quindi scegli Avanti.



c. Immettete il nome di una fase.

d. Per Posizione del file, seleziona Elimina il file sorgente originale.

e. Scegli Avanti, quindi esamina i dettagli del passaggio.

f. Scegli Crea passaggio per aggiungere il passaggio e continuare.

8. Controlla la configurazione del flusso di lavoro, quindi scegli Crea flusso di lavoro.

CLI

Esempio di workflow di tag e spostamento

1. Salva il codice seguente in un file; ad esempio,`tagAndMoveWorkflow.json`. Sostituisci ogni *`user input placeholder`* con le tue informazioni.

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

Il primo passaggio copia il file caricato in una nuova posizione Amazon S3. Il secondo passaggio aggiunge un tag (coppia chiave-valore) al file (`previous.file`) che è stato copiato nella nuova posizione. Infine, il terzo passaggio elimina il file originale (). `original.file`

2. Crea un flusso di lavoro dal file salvato. Sostituisci ogni *`user input placeholder`* con le tue informazioni.

```
aws transfer create-workflow --description "short-description" --steps
 file://path-to-file --region region-ID
```

Per esempio:

```
aws transfer create-workflow --description "copy-tag-delete workflow" --steps
 file://tagAndMoveWorkflow.json --region us-east-1
```

> **Note**
>
> Per maggiori dettagli sull'utilizzo dei file per caricare i parametri, vedete Come caricare i parametri da un file.

3. Aggiorna un server esistente.

> **Note**
>
> Questo passaggio presuppone che tu disponga già di un server Transfer Family e desideri associarvi un flusso di lavoro. In caso contrario, vediConfigurazione di un endpoint server SFTP, FTPS o FTP. Sostituisci ogni *`user input placeholder`* con le tue informazioni.

```
aws transfer update-server --server-id server-ID --region region-ID
```

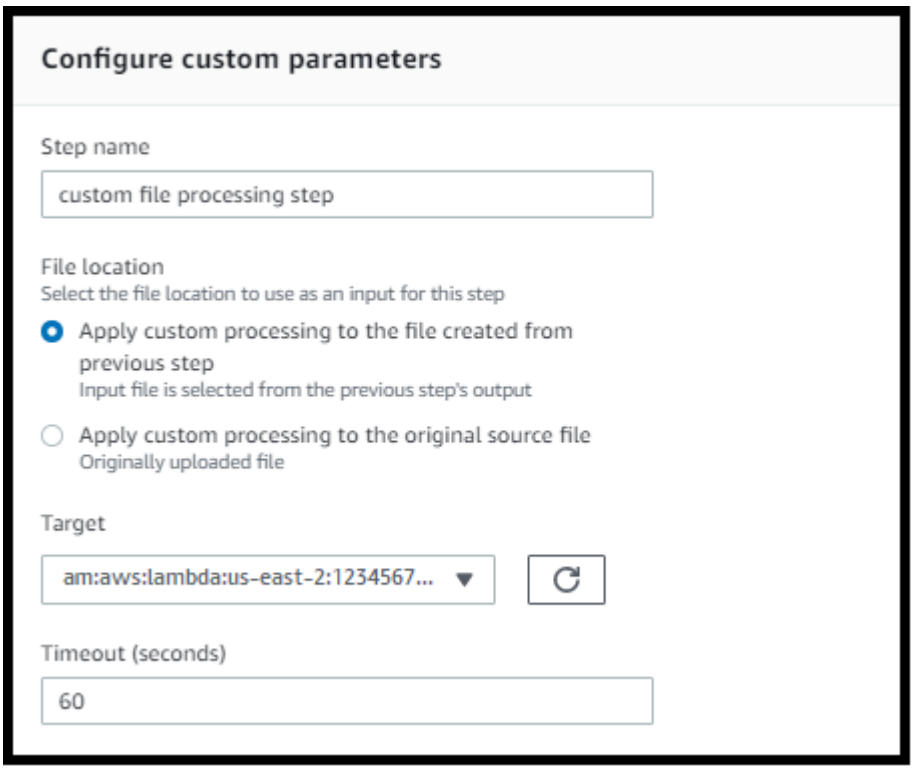
```
  --workflow-details '{"OnUpload":[{ "WorkflowId": "workflow-
ID","ExecutionRole": "execution-role-ARN"}]}'
```

Per esempio:

```
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"}]}'
```

Utilizza passaggi di elaborazione dei file personalizzati

Utilizzando una fase di elaborazione dei file personalizzata, è possibile utilizzare la logica di elaborazione dei file Bring Your Own. AWS Lambda All'arrivo dei file, un server Transfer Family richiama una funzione Lambda che contiene una logica di elaborazione dei file personalizzata, come la crittografia dei file, la scansione alla ricerca di malware o il controllo dei tipi di file errati. Nell'esempio seguente, la AWS Lambda funzione target viene utilizzata per elaborare il file di output del passaggio precedente.



> **Note**
>
> Per un esempio di funzione Lambda, consulta Esempio di funzione Lambda per una fase del flusso di lavoro personalizzata. Ad esempio, eventi (inclusa la posizione dei file passati in Lambda), vedi. Eventi di esempio inviati al AWS Lambda momento del caricamento del file

Con una fase del flusso di lavoro personalizzata, è necessario configurare la funzione Lambda per richiamare l'operazione SendWorkflowStepStateAPI. `SendWorkflowStepState`notifica all'esecuzione del flusso di lavoro che il passaggio è stato completato con uno stato di successo o di errore. Lo stato dell'operazione `SendWorkflowStepState` API richiama un passaggio del gestore delle eccezioni o un passaggio nominale nella sequenza lineare, in base al risultato della funzione Lambda.

Se la funzione Lambda fallisce o scade, il passaggio ha esito negativo e lo vedi `StepErrored` nei log. CloudWatch Se la funzione Lambda fa parte del passaggio nominale e la funzione risponde `SendWorkflowStepState` con `Status="FAILURE"` o scade, il flusso continua con i passaggi del gestore delle eccezioni. In questo caso, il flusso di lavoro non continua a eseguire i passaggi nominali rimanenti (se presenti). Per ulteriori dettagli, consulta Gestione delle eccezioni per un flusso di lavoro.

Quando si chiama l'operazione `SendWorkflowStepState` API, è necessario inviare i seguenti parametri:

```
{
    "ExecutionId": "string",
    "Status": "string",
    "Token": "string",
    "WorkflowId": "string"
}
```

È possibile estrarre il `ExecutionIdToken`, e `WorkflowId` dall'evento di input che viene passato quando viene eseguita la funzione Lambda (gli esempi sono mostrati nelle sezioni seguenti). Il `Status` valore può essere o. `SUCCESS` `FAILURE`

Per poter richiamare l'operazione `SendWorkflowStepState` API dalla funzione Lambda, è necessario utilizzare una versione dell' AWS SDK pubblicata dopo l'introduzione dei flussi di lavoro gestiti.

Utilizzo consecutivo di più funzioni Lambda

Quando si utilizzano più passaggi personalizzati uno dopo l'altro, l'opzione Posizione del file funziona in modo diverso rispetto all'utilizzo di un solo passaggio personalizzato. Transfer Family non supporta il trasferimento del file elaborato da Lambda per utilizzarlo come input del passaggio successivo. Quindi, se avete più passaggi personalizzati tutti configurati per utilizzare l'`previous.file`opzione, tutti utilizzano la stessa posizione del file (la posizione del file di input per il primo passaggio personalizzato).

> **Note**
>
> L'`previous.file`impostazione funziona in modo diverso anche se si dispone di un passaggio predefinito (etichettare, copiare, decrittografare o eliminare) dopo un passaggio personalizzato. Se il passaggio predefinito è configurato per utilizzare l'`previous.file`impostazione, il passaggio predefinito utilizza lo stesso file di input utilizzato dal passaggio personalizzato. Il file elaborato dal passaggio personalizzato non viene passato al passaggio predefinito.

Accesso a un file dopo l'elaborazione personalizzata

Se utilizzi Amazon S3 come storage e se il tuo flusso di lavoro include un passaggio personalizzato che esegue azioni sul file originariamente caricato, i passaggi successivi non possono accedere al file elaborato. In altre parole, nessun passaggio successivo al passaggio personalizzato non può fare riferimento al file aggiornato dall'output del passaggio personalizzato.

Ad esempio, supponiamo di avere i seguenti tre passaggi nel flusso di lavoro.

- Passaggio 1: carica un file denominato`example-file.txt`.
- Passaggio 2: richiama una funzione Lambda che `example-file.txt` cambia in qualche modo.
- Fase 3 — Tentativo di eseguire ulteriori elaborazioni sulla versione aggiornata di. `example-file.txt`

Se si configura `sourceFileLocation` la Fase 3 in modo che sia la Fase 3`${original.file}`, la Fase 3 utilizza la posizione originale del file da quando il server ha caricato il file nell'archivio nella Fase 1. Se lo utilizzi `${previous.file}` per lo Step 3, lo Step 3 riutilizza la posizione del file utilizzata dallo Step 2 come input.

Pertanto, lo Step 3 causa un errore. Ad esempio, se nel passaggio 3 si tenta di copiare l'aggiornamento`example-file.txt`, viene visualizzato il seguente errore:

```
{
    "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"
    },
```

Questo errore si verifica perché il passaggio personalizzato modifica il tag di entità (ETag) `example-file.txt` in modo che non corrisponda al file originale.

> **Note**
>
> Questo comportamento non si verifica se utilizzi Amazon EFS perché Amazon EFS non utilizza tag di entità per identificare i file.

Eventi di esempio inviati al AWS Lambda momento del caricamento del file

Gli esempi seguenti mostrano gli eventi a cui vengono inviati AWS Lambda quando il caricamento di un file è completo. Un esempio utilizza un server Transfer Family in cui il dominio è configurato con Amazon S3. L'altro esempio utilizza un server Transfer Family in cui il dominio utilizza 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"
    }
}
```

Esempio di funzione Lambda per una fase del flusso di lavoro personalizzata

La seguente funzione Lambda estrae le informazioni relative allo stato di esecuzione, quindi chiama l'operazione SendWorkflowStepStateAPI per restituire lo stato al flusso di lavoro per la fase, ovvero. `SUCCESS` `FAILURE` Prima che la funzione richiami l'operazione `SendWorkflowStepState` API, puoi configurare Lambda per eseguire un'azione basata sulla logica del tuo flusso di lavoro.

```
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)
    }
```

Autorizzazioni IAM per un passaggio personalizzato

Per consentire il completamento di un passaggio che richiama una Lambda, assicurati che il ruolo di esecuzione per il tuo flusso di lavoro contenga le seguenti autorizzazioni.

```
{
            "Sid": "Custom",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:region:account-id:function:function-name"
            ]
        }
```

Politiche IAM per i flussi di lavoro

Quando aggiungi un flusso di lavoro a un server, devi selezionare un ruolo di esecuzione. Il server utilizza questo ruolo quando esegue il flusso di lavoro. Se il ruolo non dispone delle autorizzazioni appropriate, non AWS Transfer Family può eseguire il flusso di lavoro.

Questa sezione descrive un possibile set di autorizzazioni AWS Identity and Access Management (IAM) che è possibile utilizzare per eseguire un flusso di lavoro. Altri esempi sono descritti più avanti in questo argomento.

> **Note**
>
> Se i tuoi file Amazon S3 hanno tag, devi aggiungere una o due autorizzazioni alla tua policy IAM.
>
> - Aggiungi `s3:GetObjectTagging` per un file Amazon S3 senza versione.
> - Aggiungi `s3:GetObjectVersionTagging` per un file Amazon S3 con versione.

Per creare un ruolo di esecuzione per il tuo flusso di lavoro

1. Crea un nuovo ruolo IAM e aggiungi la policy AWS gestita `AWSTransferFullAccess` al ruolo. Per ulteriori informazioni sulla creazione di un nuovo ruolo IAM, consultathe section called “Crea un ruolo e una policy IAM”.
2. Crea un'altra policy con le seguenti autorizzazioni e associala al tuo ruolo. Sostituisci ogni *`user input placeholder`* con le tue informazioni.

```
{
    "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. Salva questo ruolo e specificalo come ruolo di esecuzione quando aggiungi un flusso di lavoro a un server.

> **Note**
>
> Quando crei ruoli IAM, ti AWS consiglia di limitare l'accesso alle tue risorse il più possibile per il tuo flusso di lavoro.

Relazioni di fiducia nel workflow

I ruoli di esecuzione del flusso di lavoro richiedono anche una relazione di fiducia con `transfer.amazonaws.com`. Per stabilire una relazione di fiducia per AWS Transfer Family, vederePer stabilire una relazione di trust.

Mentre stabilite il vostro rapporto di fiducia, potete anche prendere provvedimenti per evitare il confuso problema del vicesceriffo. Per una descrizione di questo problema e per alcuni esempi su come evitarlo, consultathe section called “Prevenzione del problema "confused deputy" tra servizi”.

Esempio di ruolo di esecuzione: decrittografia, copia e tag

Se disponi di flussi di lavoro che includono passaggi di etichettatura, copia e decrittografia, puoi utilizzare la seguente politica IAM. Sostituisci ogni *`user input placeholder`* con le tue informazioni.

```
{
    "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/
*"
        }
    ]
}
```

Esempio di ruolo di esecuzione: Esegui la funzione ed elimina

In questo esempio, avete un flusso di lavoro che richiama una AWS Lambda funzione. Se il flusso di lavoro elimina il file caricato e prevede un passaggio di gestione delle eccezioni che interviene in caso di esecuzione non riuscita del flusso di lavoro nel passaggio precedente, utilizza la seguente policy IAM. Sostituisci ogni *user input placeholder* con le tue informazioni.

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

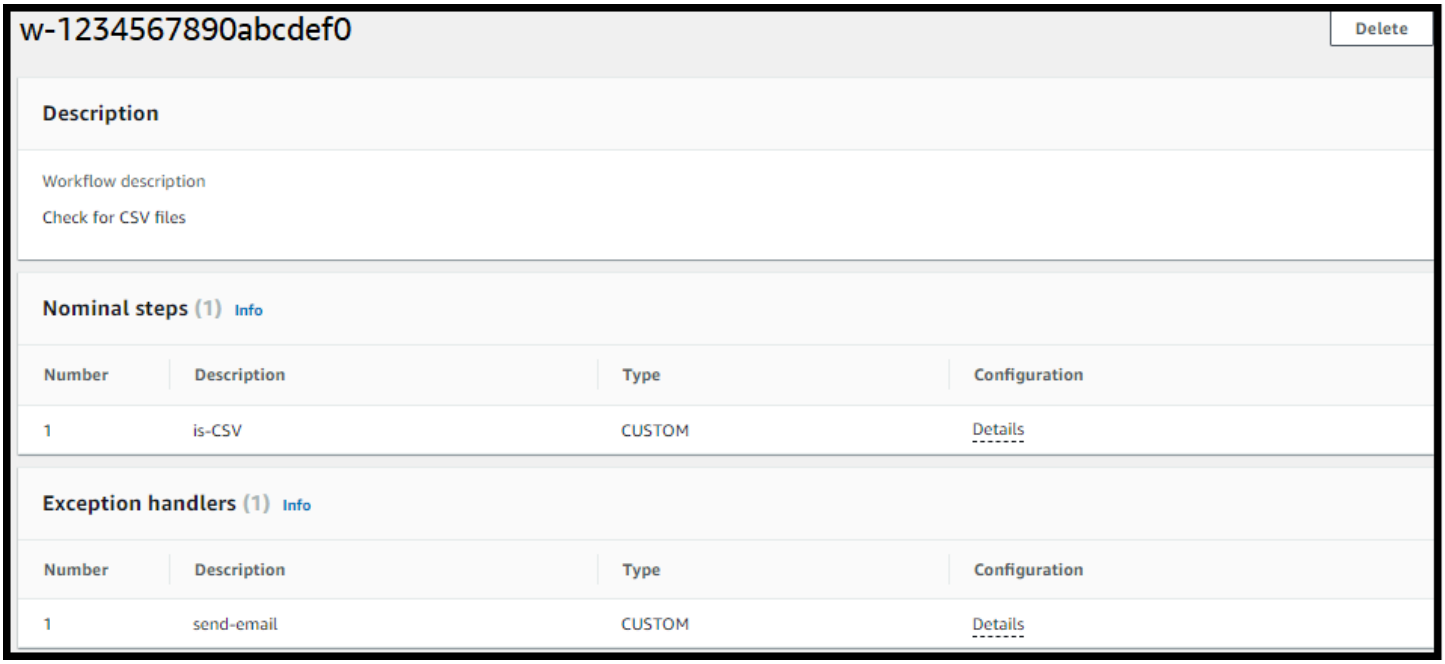
Gestione delle eccezioni per un flusso di lavoro

Se si verificano errori durante l'esecuzione di un flusso di lavoro, vengono eseguiti i passaggi di gestione delle eccezioni specificati. I passaggi di gestione degli errori per un flusso di lavoro vengono specificati nello stesso modo in cui si specificano i passaggi nominali per il flusso di lavoro. Ad esempio, supponete di aver configurato l'elaborazione personalizzata in passaggi nominali per convalidare i file in entrata. Se la convalida del file fallisce, una fase di gestione delle eccezioni può inviare un'e-mail all'amministratore.

Il flusso di lavoro di esempio seguente contiene due passaggi:

- Un passaggio nominale che verifica se il file caricato è in formato CSV
- Un passaggio di gestione delle eccezioni che invia un'e-mail nel caso in cui il file caricato non sia in formato CSV e il passaggio nominale fallisca

Per avviare la fase di gestione delle eccezioni, la AWS Lambda funzione nella fase nominale deve rispondere con. `Status="FAILURE"` Per ulteriori informazioni sulla gestione degli errori nei flussi di lavoro, vedere. the section called “Utilizza passaggi di elaborazione dei file personalizzati”



Monitora l'esecuzione del workflow

Amazon CloudWatch monitora AWS le tue risorse e le applicazioni che esegui Cloud AWS in tempo reale. Puoi usare Amazon CloudWatch per raccogliere e monitorare i parametri, che sono variabili che puoi misurare per i tuoi flussi di lavoro. Puoi visualizzare le metriche del flusso di lavoro e i log consolidati utilizzando Amazon. CloudWatch

CloudWatch registrazione per un flusso di lavoro

CloudWatch fornisce il controllo e la registrazione consolidati dell'avanzamento e dei risultati del flusso di lavoro.

Visualizza i CloudWatch log di Amazon per i flussi di lavoro

1. Apri la CloudWatch console Amazon all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione a sinistra, scegli Registri, quindi scegli Gruppi di log.
3. Nella pagina Gruppi di log, nella barra di navigazione, scegli la regione corretta per il tuo AWS Transfer Family server.
4. Scegli il gruppo di log che corrisponde al tuo server.

   Ad esempio, se l'ID del tuo server è`s-1234567890abcdef0`, il tuo gruppo di log lo è`/aws/transfer/s-1234567890abcdef0`.

5. Nella pagina dei dettagli del gruppo di log relativa al server, vengono visualizzati i flussi di log più recenti. Esistono due flussi di log per l'utente che stai esplorando:

   - Uno per ogni sessione di Secure Shell (SSH) File Transfer Protocol (SFTP).
   - Uno per il flusso di lavoro che viene eseguito per il server. Il formato per il flusso di log per il flusso di lavoro è*username*.*workflowID*.*uniqueStreamSuffix*.

   Ad esempio, se il tuo utente è`mary-major`, hai i seguenti flussi di log:

   ```
   mary-major-east.1234567890abcdef0
   mary.w-abcdef01234567890.021345abcdef6789
   ```

   > **Note**
   >
   > Gli identificatori alfanumerici a 16 cifre elencati in questo esempio sono fittizi. I valori che vedi in Amazon CloudWatch sono diversi.

La pagina degli eventi di registro `mary-major-usa-east.1234567890abcdef0` mostra i dettagli di ogni sessione utente e il flusso di `mary.w-abcdef01234567890.021345abcdef6789` registro contiene i dettagli del flusso di lavoro.

Di seguito è riportato un esempio di flusso di log per`mary.w-abcdef01234567890.021345abcdef6789`, basato su un workflow (`w-abcdef01234567890`) che contiene una fase di copia.

```
{
    "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 metriche per i flussi di lavoro

AWS Transfer Family fornisce diverse metriche per i flussi di lavoro. È possibile visualizzare le metriche relative al numero di esecuzioni di flussi di lavoro avviate, completate con successo e non riuscite nel minuto precedente. Tutte le CloudWatch metriche per Transfer Family sono descritte inUtilizzo delle CloudWatch metriche per Transfer Family.

Creare un flusso di lavoro a partire da un modello

È possibile distribuire uno AWS CloudFormation stack che crea un flusso di lavoro e un server a partire da un modello. Questa procedura contiene un esempio che è possibile utilizzare per distribuire rapidamente un flusso di lavoro.

Per creare uno AWS CloudFormation stack che crei un AWS Transfer Family flusso di lavoro e un server

1. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
2. Salva il codice seguente in un file.

   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. Sostituisci i seguenti elementi con i tuoi valori effettivi.

   - Sostituire *workflow-execution-role-arn* con l'ARN del ruolo di esecuzione del flusso di lavoro effettivo. Ad esempio, `arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`
   - Sostituisci `arn:aws:lambda:`*region*`:`*account-id*`:function:`*function-name* con l'ARN per la tua funzione Lambda. Ad esempio, `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`.

4. Segui le istruzioni per distribuire uno AWS CloudFormation stack da un modello esistente in Selezione di un modello di stack nella Guida per l'utente.AWS CloudFormation

Dopo aver distribuito lo stack, puoi visualizzarne i dettagli nella scheda Output della console. CloudFormation Il modello crea un nuovo server AWS Transfer Family SFTP che utilizza utenti gestiti dal servizio e un nuovo flusso di lavoro e associa il flusso di lavoro al nuovo server.

Rimuovere un flusso di lavoro da un server Transfer Family

Se hai associato un flusso di lavoro a un server Transfer Family e ora desideri rimuovere tale associazione, puoi farlo utilizzando la console o a livello di codice.

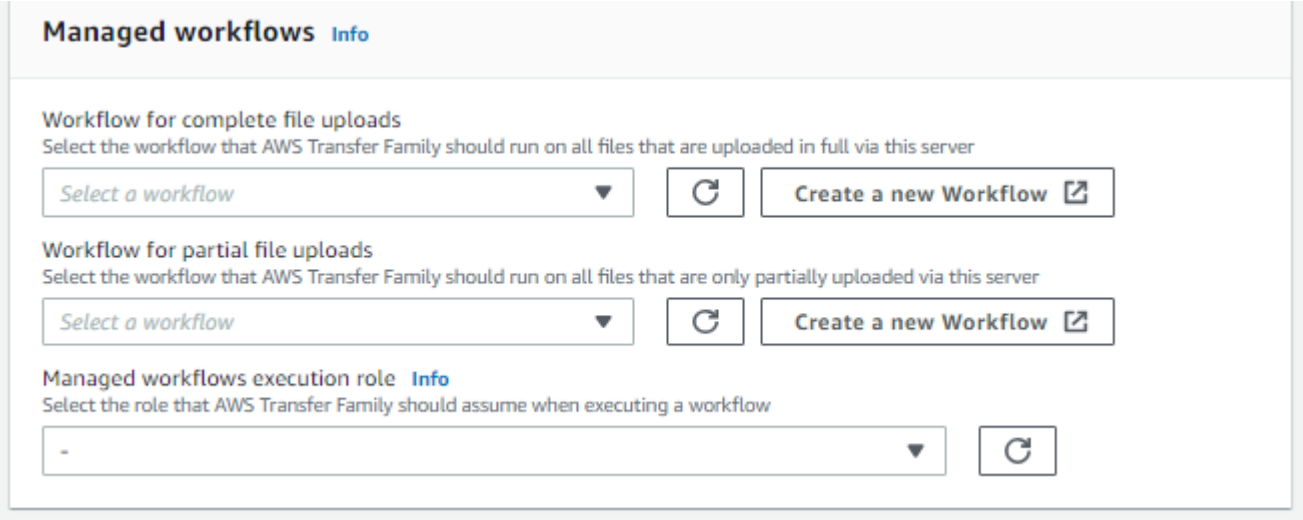
Console

Per rimuovere un flusso di lavoro da un server Transfer Family

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server.
3. Scegli l'identificatore per il server nella colonna Server ID.
4. Nella pagina dei dettagli del server, scorri verso il basso fino alla sezione Dettagli aggiuntivi, quindi scegli Modifica.
5. Nella pagina Modifica dettagli aggiuntivi, nella sezione Flussi di lavoro gestiti, cancella le informazioni relative a tutte le impostazioni:
   - Seleziona il trattino (-) dall'elenco dei flussi di lavoro per il flusso di lavoro per il caricamento completo dei file.
   - Se non è già deselezionato, seleziona il trattino (-) dall'elenco dei flussi di lavoro per il flusso di lavoro per i caricamenti parziali di file.
   - Seleziona il trattino (-) dall'elenco dei ruoli per il ruolo di esecuzione dei flussi di lavoro gestiti.

   Se non vedi il trattino, scorri verso l'alto fino a visualizzarlo, poiché è il primo valore in ogni menu.

   La schermata dovrebbe avere l'aspetto seguente.



6. Scorri verso il basso e scegli Salva per salvare le modifiche.

CLI

Utilizzate la chiamata `update-server` (o `UpdateServer` per l'API) e fornite argomenti vuoti per i `OnPartialUpload` parametri `OnUpload` and.

Da AWS CLI, esegui il seguente comando:

```
aws transfer update-server --server-id your-server-id --workflow-details
 '{"OnPartialUpload":[],"OnUpload":[]}'
```

Sostituiscilo *`your-server-id`* con l'ID del tuo server. Ad esempio, se l'ID del server è`s-01234567890abcdef`, il comando è il seguente:

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
 '{"OnPartialUpload":[],"OnUpload":[]}'
```

Restrizioni e limitazioni dei flussi di lavoro gestiti

Restrizioni

Le seguenti restrizioni si applicano attualmente ai flussi di lavoro di elaborazione post-caricamento per. AWS Transfer Family

- Le AWS Lambda funzioni tra account e aree geografiche non sono supportate. Tuttavia, è possibile eseguire la copia su più account, a condizione che le policy AWS Identity and Access Management (IAM) siano configurate correttamente.
- Per tutte le fasi del flusso di lavoro, tutti i bucket Amazon S3 a cui il flusso di lavoro accede devono trovarsi nella stessa regione del flusso di lavoro stesso.
- Per una fase di decrittografia, la destinazione di decrittografia deve corrispondere all'origine per la regione e l'archivio di backup (ad esempio, se il file da decrittografare è archiviato in Amazon S3, anche la destinazione specificata deve essere in Amazon S3).
- Sono supportati solo passaggi personalizzati asincroni.
- I timeout dei passaggi personalizzati sono approssimativi. Cioè, il timeout potrebbe richiedere un tempo leggermente più lungo di quanto specificato. Inoltre, il flusso di lavoro dipende dalla funzione Lambda. Pertanto, se la funzione viene ritardata durante l'esecuzione, il flusso di lavoro non è a conoscenza del ritardo.
- Se superi il limite di limitazione, Transfer Family non aggiunge le operazioni del flusso di lavoro alla coda.
- I flussi di lavoro non vengono avviati per i file che hanno una dimensione pari a 0. I file con una dimensione superiore a 0 avviano il flusso di lavoro associato.

Limitazioni

Inoltre, i seguenti limiti funzionali si applicano ai flussi di lavoro per Transfer Family:

- Il numero di flussi di lavoro per regione, per account, è limitato a 10.
- Il timeout massimo per i passaggi personalizzati è di 30 minuti.
- Il numero massimo di passaggi in un flusso di lavoro è 8.
- Il numero massimo di tag per flusso di lavoro è 50.
- Il numero massimo di esecuzioni simultanee che contengono una fase di decrittografia è 250 per flusso di lavoro.
- È possibile memorizzare un massimo di 3 chiavi private PGP, per server Transfer Family, per utente.
- La dimensione massima per un file decrittografato è di 10 GB.
- Limitiamo la nuova velocità di esecuzione utilizzando un sistema di token bucket con una capacità di burst di 100 e una frequenza di ricarica di 1.

- Ogni volta che rimuovi un flusso di lavoro da un server e lo sostituisci con uno nuovo o aggiorni la configurazione del server (che influisce sul ruolo di esecuzione di un flusso di lavoro), devi attendere circa 10 minuti prima di eseguire il nuovo flusso di lavoro. Il server Transfer Family memorizza nella cache i dettagli del flusso di lavoro e il server impiega 10 minuti per aggiornare la cache.

  Inoltre, è necessario disconnettersi da tutte le sessioni SFTP attive e quindi riconnettersi dopo il periodo di attesa di 10 minuti per visualizzare le modifiche.

Gestione dei server

In questa sezione, puoi trovare informazioni su come visualizzare un elenco dei tuoi server, come visualizzare i dettagli del server, come modificare i dettagli del server e come modificare la chiave host per il tuo server compatibile con SFTP.

Argomenti

Visualizza un elenco di server

Sulla AWS Transfer Family console, puoi trovare un elenco di tutti i server che si trovano nella AWS regione che hai scelto.

Per trovare un elenco dei tuoi server esistenti in una AWS regione

- Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.

  Se hai uno o più server nella AWS regione corrente, la console si apre e mostra un elenco dei tuoi server. Se non vedi un elenco di server, assicurati di trovarti nella regione corretta. È anche possibile scegliere Servers (Server) dal riquadro di navigazione.

  Per ulteriori informazioni sulla visualizzazione dei dettagli del server, consultaVisualizza i dettagli dei server SFTP, FTPS e FTP.

Eliminare un server

Questa procedura spiega come eliminare un server Transfer Family utilizzando la AWS Transfer Family console o AWS CLI.

> **Important**
>
> Ti verrà addebitato, per ciascuno dei protocolli abilitati all'accesso al tuo endpoint, fino all'eliminazione del server.

> **Warning**
>
> L'eliminazione di un server comporta l'eliminazione di tutti i relativi utenti. I dati nel bucket a cui è stato effettuato l'accesso utilizzando il server non vengono eliminati e rimangono accessibili agli AWS utenti che dispongono di privilegi per tali bucket Amazon S3.

Console

Per eliminare un server utilizzando la console

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server.
3. Seleziona la casella di controllo del server che desideri eliminare.
4. In Actions (Azioni), scegliere Delete (Elimina).
5. Nella finestra di dialogo di conferma che appare, inserisci la parola**`delete`**, quindi scegli Elimina per confermare che desideri eliminare il server.

Il server viene eliminato dalla pagina Server e non ti viene più addebitato alcun costo.

AWS CLI

Per eliminare un server utilizzando la CLI

1. (Facoltativo) Eseguite il comando seguente per visualizzare i dettagli del server che desiderate eliminare definitivamente.

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

   Questo `describe-server` comando restituisce tutti i dettagli del server.
2. Esegui il comando seguente per eliminare il server.

```
aws transfer delete-server --server-id your-server-id
```

In caso di successo, il comando elimina il server e non restituisce alcuna informazione.

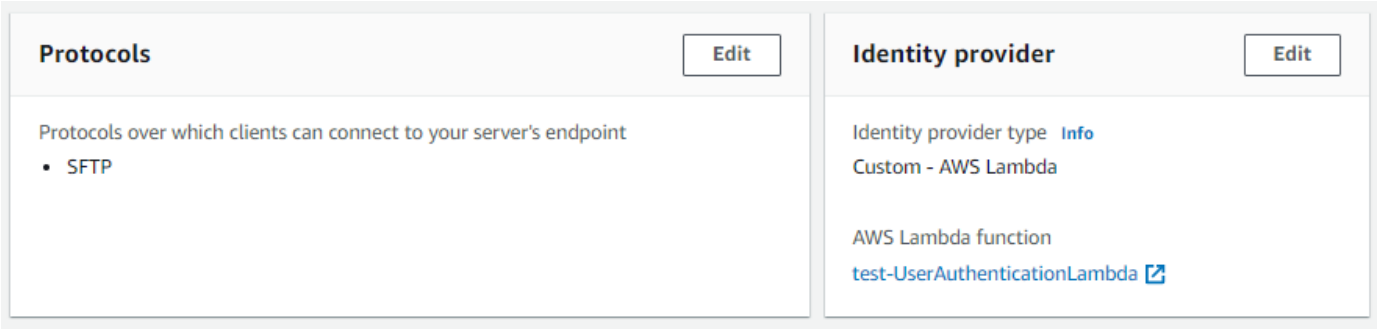
Visualizza i dettagli dei server SFTP, FTPS e FTP

È possibile trovare un elenco di dettagli e proprietà per un singolo AWS Transfer Family server. Le proprietà del server includono protocolli, provider di identità, status, tipo di endpoint, nome host personalizzato, endpoint, utenti, ruolo di registrazione, chiave host del server e tag.

Per visualizzare i dettagli del server

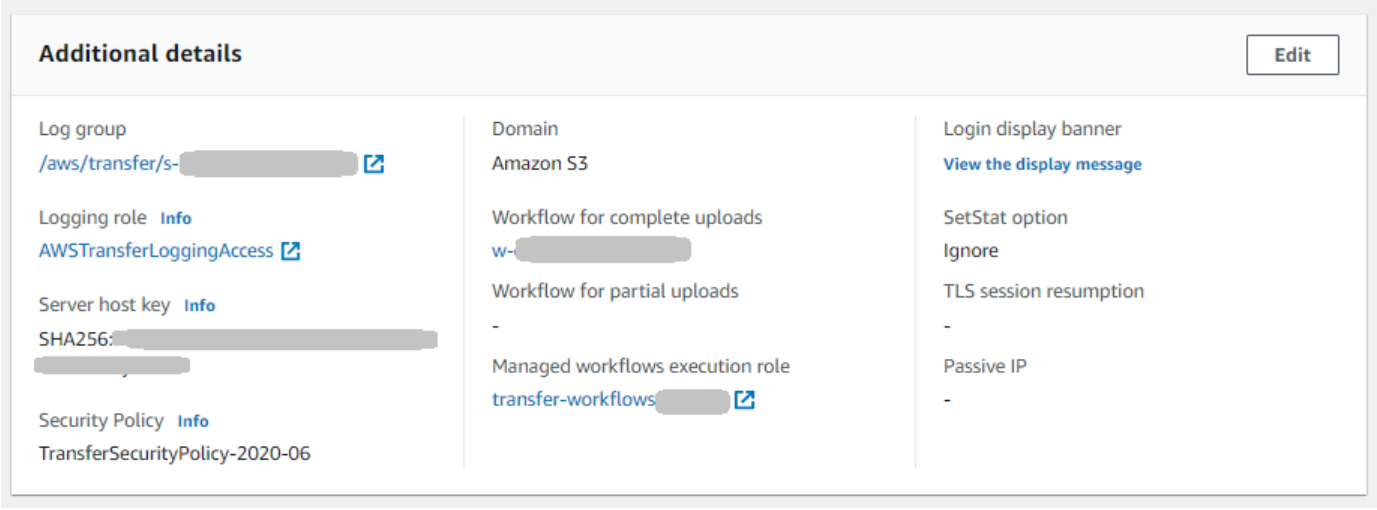
1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione, selezionare Servers (Server).
3. Scegli l'identificatore nella colonna Server ID per visualizzare la pagina dei dettagli del server, mostrata di seguito.

   Puoi modificare le proprietà del server in questa pagina scegliendo Modifica. Per ulteriori informazioni sulla modifica dei dettagli del server, vedereModifica i dettagli del server. La pagina dei dettagli per i server AS2 è leggermente diversa. Per i server AS2, vedere. Visualizza i dettagli del server AS2



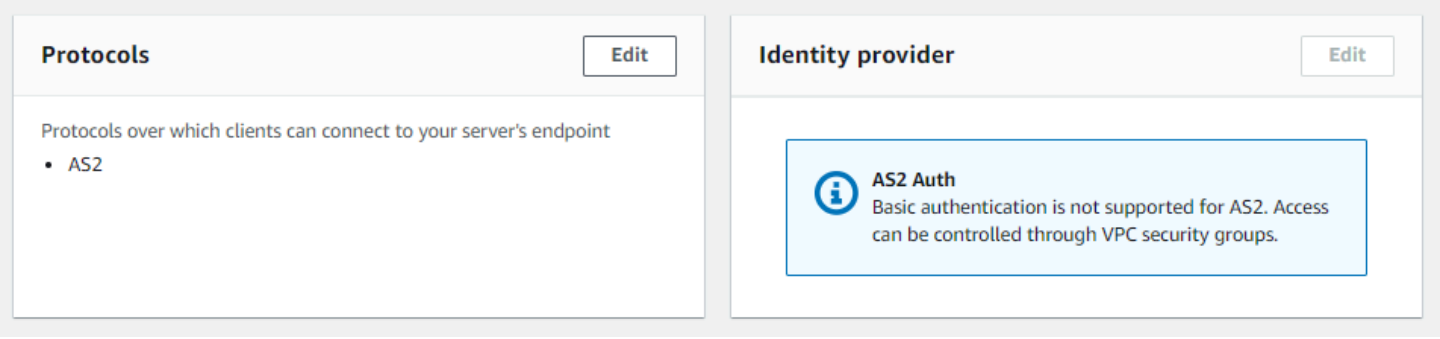
> **Note**
>
> I valori Description e Date import della chiave host del server sono nuovi a settembre 2022. Questi valori sono stati introdotti per supportare la funzionalità di chiavi host multiple. Questa funzionalità richiedeva la migrazione di tutte le singole chiavi host utilizzate prima dell'introduzione di più chiavi host.

Il valore Date import per una chiave host del server migrata è impostato sulla data dell'ultima modifica del server. Cioè, la data visualizzata per la chiave host migrata corrisponde alla data dell'ultima modifica del server in qualsiasi modo, prima della migrazione della chiave host del server.
L'unica chiave che è stata migrata è la chiave dell'host del server più vecchia o l'unica. Tutte le chiavi aggiuntive hanno la data effettiva in cui sono state importate. Inoltre, la chiave migrata ha una descrizione che consente di identificarla facilmente come migrata. La migrazione è avvenuta tra il 2 settembre e il 13 settembre. La data di migrazione effettiva all'interno di questo intervallo dipende dalla regione del server.

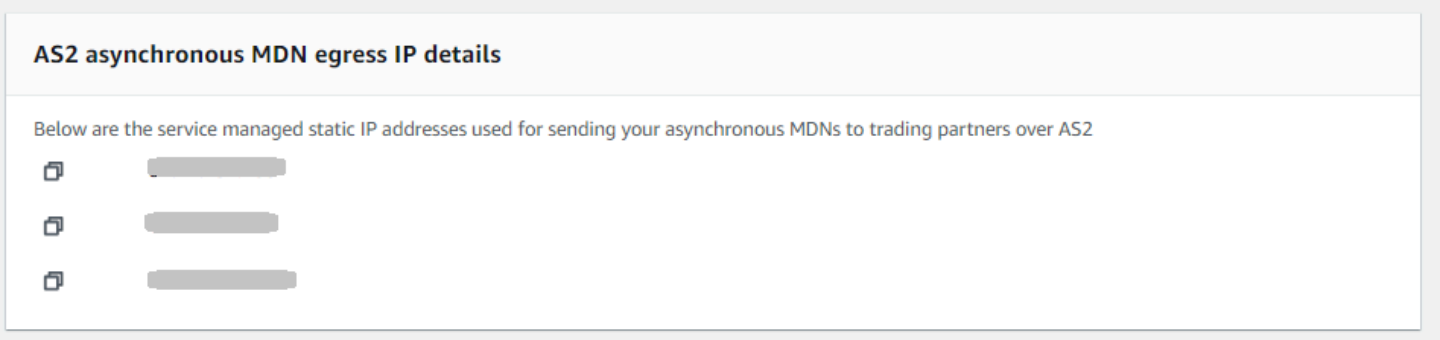


Visualizza i dettagli del server AS2

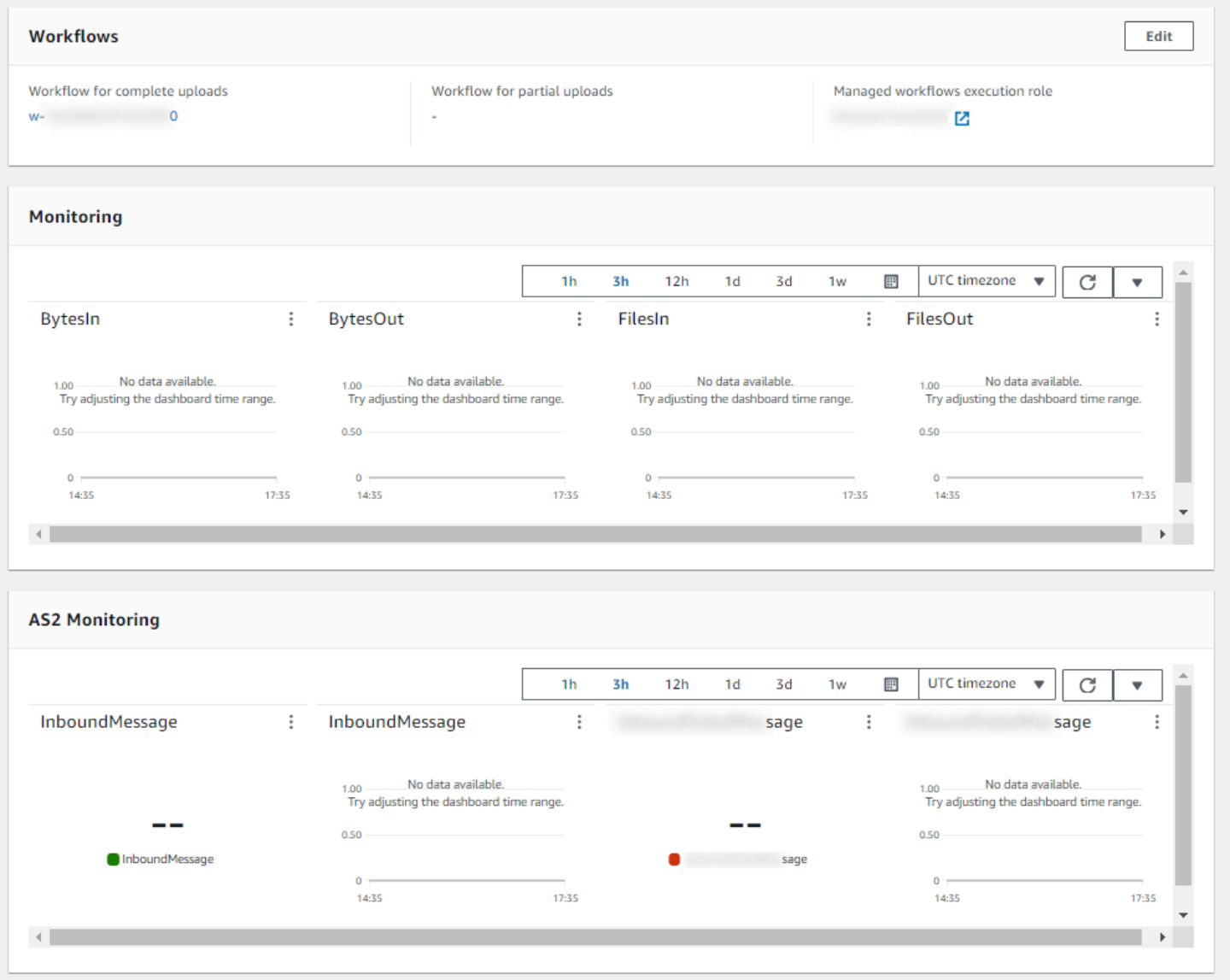
È possibile trovare un elenco di dettagli e proprietà per un singolo AWS Transfer Family server. Le proprietà del server includono protocolli, stato e altro. Per i server AS2, puoi anche visualizzare gli indirizzi IP di uscita MDN asincroni AS2.



A ciascun server AS2 vengono assegnati tre indirizzi IP statici. Utilizza questi indirizzi IP per inviare mDNS asincroni ai tuoi partner commerciali tramite AS2.



La parte inferiore della pagina dei dettagli del server AS2 contiene i dettagli per qualsiasi flusso di lavoro associato e le informazioni di monitoraggio e etichettatura.



Modifica i dettagli del server

Dopo aver creato un AWS Transfer Family server, è possibile modificare la configurazione del server.

Argomenti

Per modificare la configurazione di un server

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server.
3. Scegli l'identificatore nella colonna Server ID per visualizzare la pagina dei dettagli del server, mostrata di seguito.

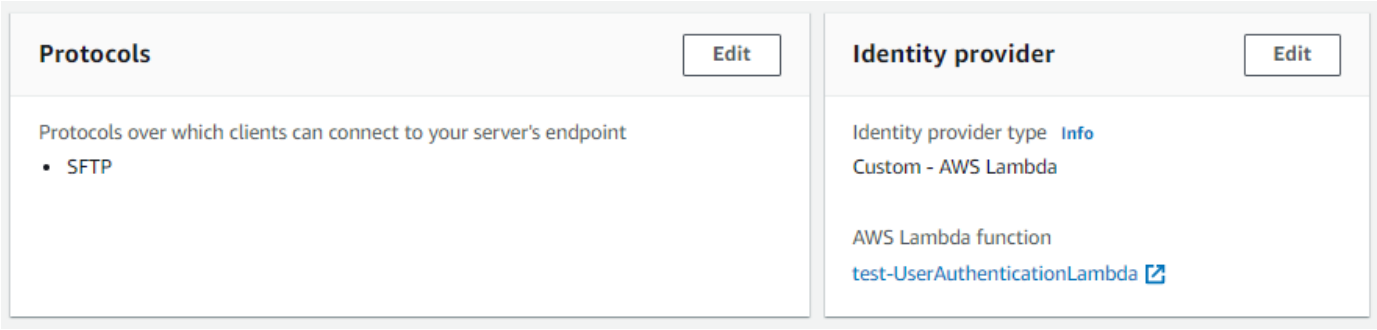
   Puoi modificare le proprietà del server in questa pagina scegliendo Modifica:

   - Per modificare i protocolli, vedereModifica i protocolli di trasferimento dei file.
   - Per quanto riguarda il provider di identità, tieni presente che non puoi modificare il tipo di provider di identità di un server dopo averlo creato. Per modificare il provider di identità, elimina il server e creane uno nuovo con il provider di identità desiderato.

     > **Note**
     >
     > Se il server utilizza un provider di identità personalizzato, puoi modificare alcune proprietà. Per informazioni dettagliate, vedi Modifica i parametri personalizzati del provider di identità.

   - Per modificare il tipo di endpoint o il nome host personalizzato, consulta. Modifica l'endpoint del server

- Per aggiungere un accordo, devi prima aggiungere AS2 come protocollo al tuo server. Per informazioni dettagliate, vedi Modifica i protocolli di trasferimento dei file.
- Per gestire le chiavi host per il tuo server, consultaGestisci le chiavi host per il tuo server compatibile con SFTP.
- In Dettagli aggiuntivi, puoi modificare le seguenti informazioni:
  - Per modificare il ruolo di registrazione, vedereModifica la configurazione di registrazione.
  - Per modificare la politica di sicurezza, vedereModifica la politica di sicurezza.
  - Per modificare la chiave dell'host del server, vedereGestisci le chiavi host per il tuo server compatibile con SFTP.
  - Per modificare il flusso di lavoro gestito per il server, consultaModifica il flusso di lavoro gestito per il tuo server.
  - Per modificare i banner di visualizzazione per il tuo server, consultaCambia i banner di visualizzazione per il tuo server.
- In Configurazione aggiuntiva, puoi modificare le seguenti informazioni:
  - SetStat opzione: abilita questa opzione per ignorare l'errore generato quando un client tenta di utilizzarlo `SETSTAT` su un file che stai caricando su un bucket Amazon S3. Per ulteriori dettagli, consulta la `SetStatOption` documentazione nell'argomento. ProtocolDetails
  - Ripresa della sessione TLS: fornisce un meccanismo per riprendere o condividere una chiave segreta negoziata tra il controllo e la connessione dati per una sessione FTPS. Per ulteriori dettagli, consultate la documentazione nell'argomento. `TlsSessionResumptionMode` ProtocolDetails
  - IP passivo: indica la modalità passiva, per i protocolli FTP e FTPS. Inserisci un singolo indirizzo IPv4, ad esempio l'indirizzo IP pubblico di un firewall, router o load balancer. Per ulteriori dettagli, consultate la `PassiveIp` documentazione nell'ProtocolDetailsargomento.
- Per avviare o arrestare il server, consultaMetti il tuo server online o offline.
- Per eliminare un server, vedereEliminare un server.
- Per modificare le proprietà di un utente, vedereGestione dei controlli di accesso.

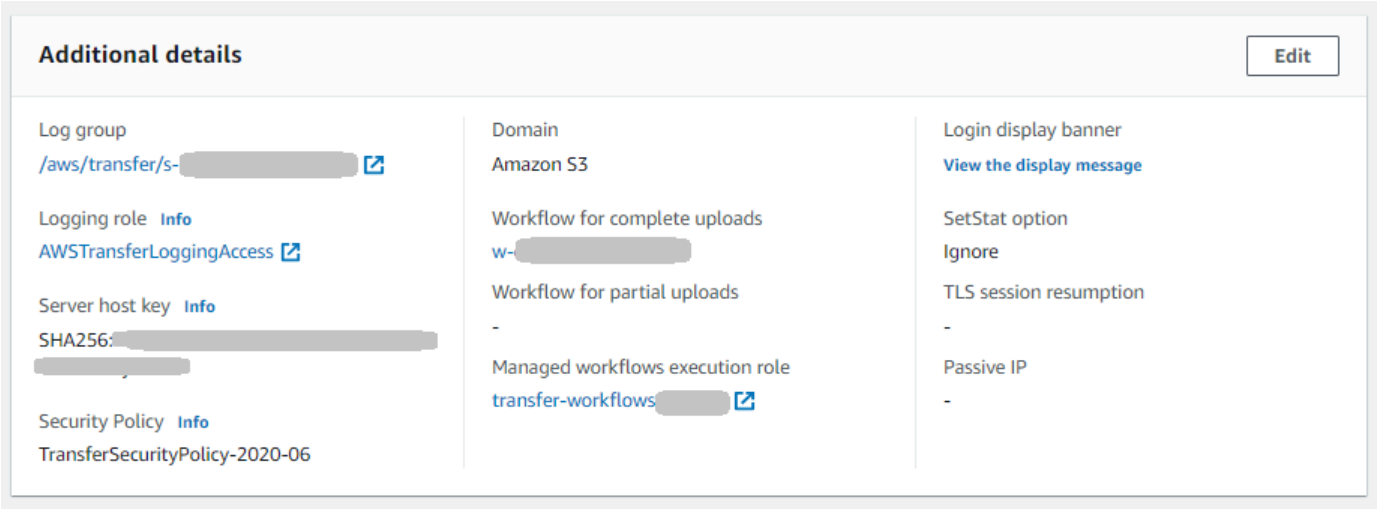


Note

I valori Description e Date import della chiave host del server sono nuovi a settembre 2022. Questi valori sono stati introdotti per supportare la funzionalità di chiavi host multiple. Questa funzionalità richiedeva la migrazione di tutte le singole chiavi host utilizzate prima dell'introduzione di più chiavi host.

Il valore Date import per una chiave host del server migrata è impostato sulla data dell'ultima modifica del server. Cioè, la data visualizzata per la chiave host migrata corrisponde alla data dell'ultima modifica del server in qualsiasi modo, prima della migrazione della chiave host del server.

L'unica chiave che è stata migrata è la chiave dell'host del server più vecchia o l'unica. Tutte le chiavi aggiuntive hanno la data effettiva in cui sono state importate. Inoltre, la chiave migrata ha una descrizione che consente di identificarla facilmente come migrata. La migrazione è avvenuta tra il 2 settembre e il 13 settembre. La data di migrazione effettiva all'interno di questo intervallo dipende dalla regione del server.



Modifica i protocolli di trasferimento dei file

Sulla AWS Transfer Family console, è possibile modificare il protocollo di trasferimento dei file. Il protocollo di trasferimento dei file collega il client all'endpoint del server.

Per modificare i protocolli

1. Nella pagina dei dettagli del server, scegli Modifica accanto a Protocolli.
2. Nella pagina Modifica protocolli, seleziona o deseleziona la casella o le caselle di controllo del protocollo per aggiungere o rimuovere i seguenti protocolli di trasferimento file:

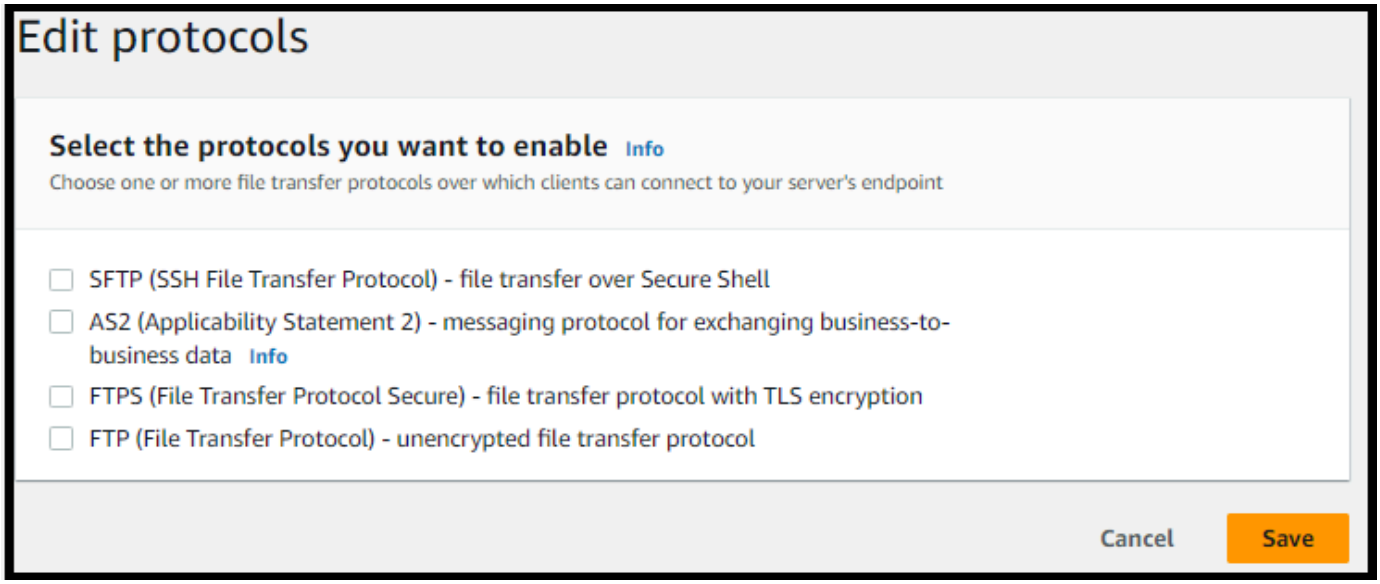
   - Secure Shell (SSH) File Transfer Protocol (SFTP): trasferimento di file tramite SSH

     Per ulteriori informazioni su SFTP, vedere. Crea un server compatibile con SFTP
   - File Transfer Protocol Secure (FTPS): trasferimento di file con crittografia TLS

     Per ulteriori informazioni su FTP, vedere. Creare un server compatibile con FTPS
   - File Transfer Protocol (FTP): trasferimento di file non crittografato

     Per ulteriori informazioni su FTPS, vedere. Crea un server abilitato all'FTP

> **Note**
>
> Se disponi di un server esistente abilitato solo per SFTP e desideri aggiungere FTPS e FTP, devi assicurarti di disporre delle impostazioni corrette del provider di identità e del tipo di endpoint compatibili con FTPS e FTP.



Se si seleziona FTPS, è necessario scegliere un certificato archiviato in AWS Certificate Manager (ACM) che verrà utilizzato per identificare il server quando i client si connettono ad esso tramite FTPS.

Per richiedere un nuovo certificato pubblico, consulta Richiedere un certificato pubblico nella Guida per l'AWS Certificate Manager utente.

Per importare un certificato esistente in ACM, consulta Importazione di certificati in ACM nella Guida per l'AWS Certificate Manager utente.

Per richiedere un certificato privato per utilizzare FTPS tramite indirizzi IP privati, consulta Richiesta di un certificato privato nella Guida per l'utente.AWS Certificate Manager

Sono supportati i certificati con gli algoritmi di crittografia e le dimensioni delle chiavi seguenti:

- RSA a 2048 bit (RSA_2048)

- RSA a 4096 bit (RSA_4096)
- Elliptic Prime Curve a 256 bit (EC_prime256v1)
- Elliptic Prime Curve a 384 bit (EC_secp384r1)
- Elliptic Prime Curve a 521 bit (EC_secp521r1)

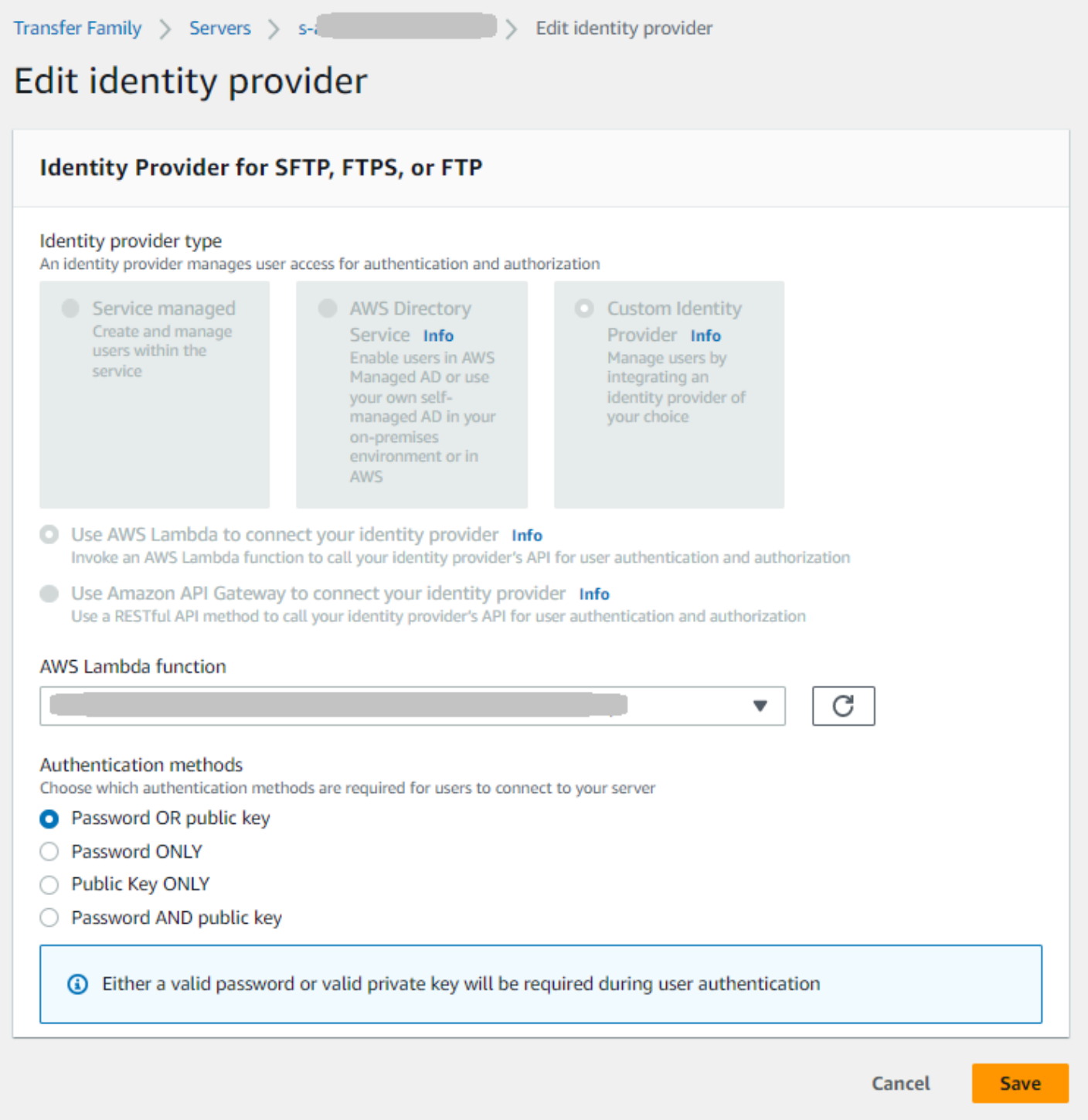
> **Note**
>
> Il certificato deve essere un certificato SSL/TLS X.509 versione 3 valido con FQDN o indirizzo IP specificato e contenere informazioni sull'emittente.

3. Selezionare Salva. Si torna alla pagina dei dettagli del server.

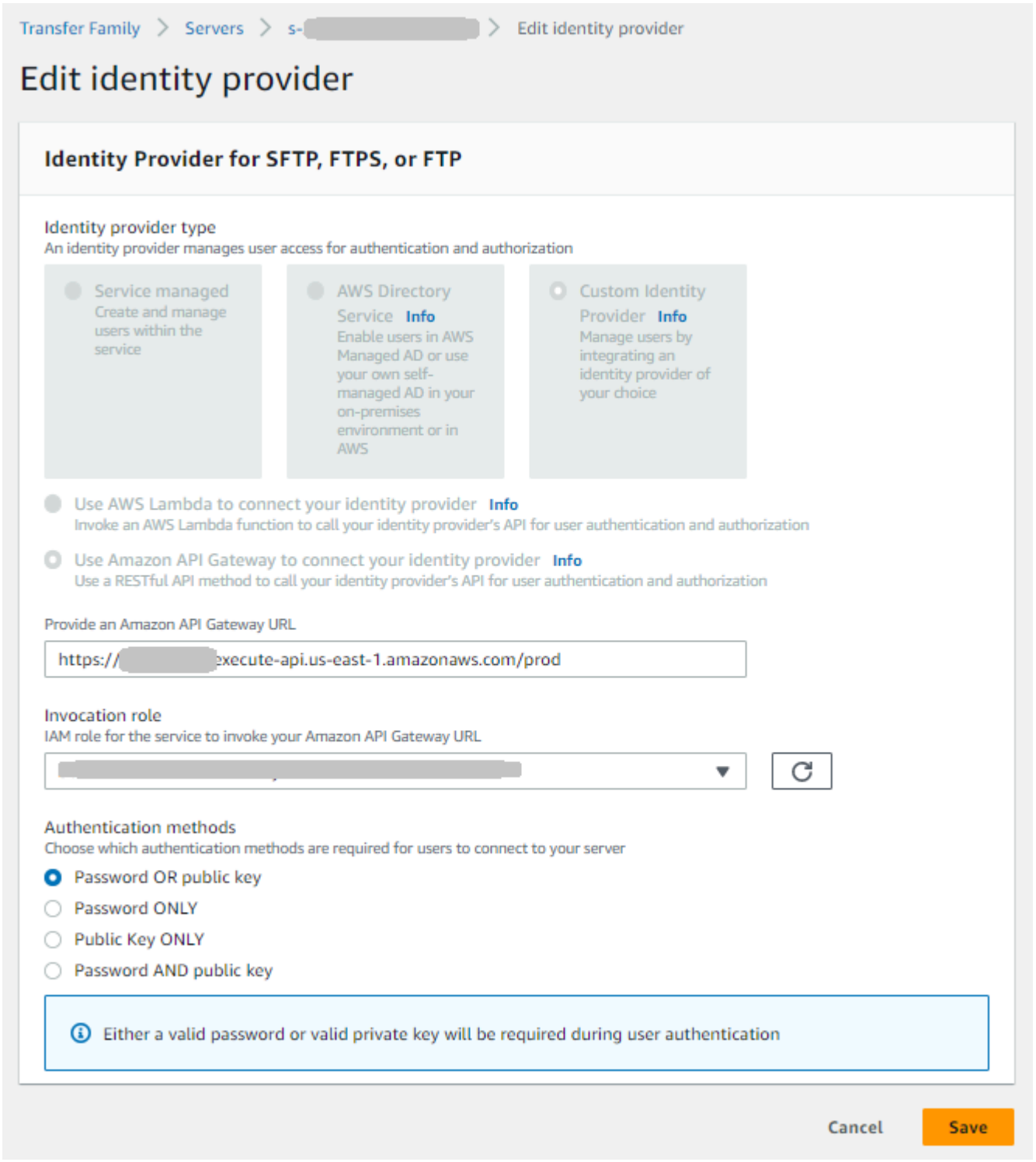
Modifica i parametri personalizzati del provider di identità

Sulla AWS Transfer Family console, per i provider di identità personalizzati, puoi modificare alcune impostazioni, a seconda che tu stia utilizzando una funzione Lambda o un API Gateway. In entrambi i casi, se il server utilizza il protocollo SFTP, è possibile modificare il metodo di autenticazione.

- Se utilizzi un Lambda come provider di identità, puoi modificare la funzione Lambda sottostante.



- Se utilizzi un API Gateway come provider di identità, puoi aggiornare l'URL del gateway o il ruolo di invocazione, o entrambi.


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

Modifica l'endpoint del server

Sulla AWS Transfer Family console, è possibile modificare il tipo di endpoint del server e il nome host personalizzato. Inoltre, per gli endpoint VPC, puoi modificare le informazioni sulla zona di disponibilità.

Per modificare i dettagli degli endpoint del server

1. Nella pagina dei dettagli del server, scegli Modifica accanto ai dettagli dell'endpoint.
2. Prima di poter modificare il tipo di endpoint, devi prima arrestare il server. Quindi, nella pagina Modifica configurazione dell'endpoint, per Tipo di endpoint, puoi scegliere uno dei seguenti valori:

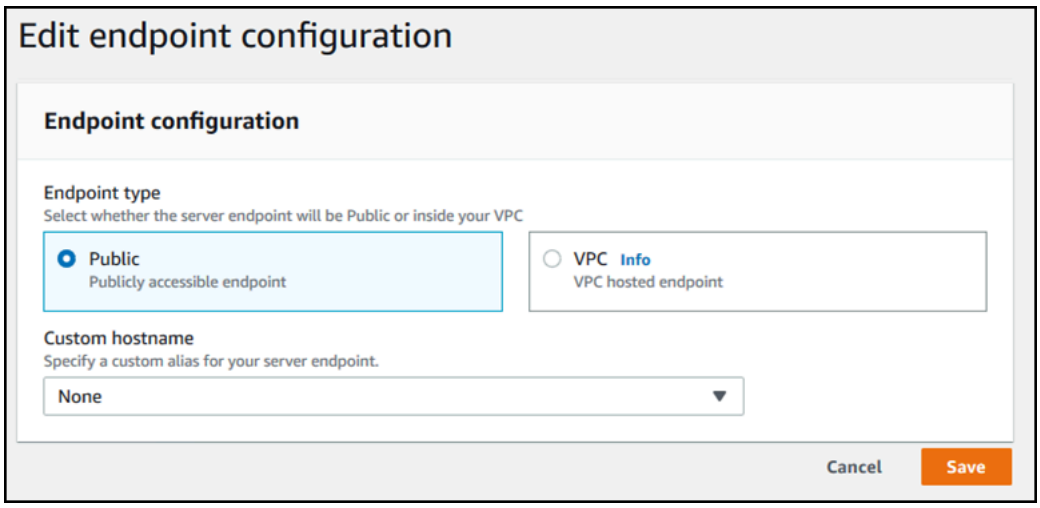
   - Pubblico: questa opzione rende il server accessibile su Internet.
   - VPC: questa opzione rende il server accessibile nel cloud privato virtuale (VPC). Per informazioni su VPC, vedere. Crea un server in un cloud privato virtuale
3. Per Nome host personalizzato, scegli una delle seguenti opzioni:

   - Nessuno: se non desideri utilizzare un dominio personalizzato, scegli Nessuno.

     Ottieni un nome host del server fornito da AWS Transfer Family. Il nome host del server ha il formato `serverId.server.transfer.regionId.amazonaws.com`.
   - Alias DNS Amazon Route 53: per utilizzare un alias DNS creato automaticamente per te in Route 53, scegli questa opzione.
   - Altro DNS: per utilizzare un nome host che già possiedi in un servizio DNS esterno, scegli Altro DNS.

   La scelta dell'alias DNS di Amazon Route 53 o di Altro DNS specifica il metodo di risoluzione dei nomi da associare all'endpoint del server.

   Ad esempio, il dominio personalizzato potrebbe essere `sftp.inbox.example.com`. Un nome host personalizzato utilizza un nome DNS fornito e che un servizio DNS è in grado di risolvere. Puoi usare Route 53 come resolver DNS o utilizzare il tuo provider di servizi DNS. Per informazioni su come AWS Transfer Family utilizza Route 53 per indirizzare il traffico dal dominio personalizzato all'endpoint del server, consulta. Lavorare con nomi host personalizzati



4. Per gli endpoint VPC, puoi modificare le informazioni nel riquadro Zone di disponibilità.
5. Selezionare Salva. Si torna alla pagina dei dettagli del server.

Modifica la configurazione di registrazione

Sulla AWS Transfer Family console, è possibile modificare la configurazione di registrazione.

> **Note**
>
> Se Transfer Family ha creato un ruolo IAM di CloudWatch registrazione per te quando hai creato un server, viene chiamato `AWSTransferLoggingAccess` il ruolo IAM. Puoi usarlo per tutti i tuoi server Transfer Family.

Per modificare la configurazione di registrazione

1. Nella pagina dei dettagli del server, scegli Modifica accanto a Dettagli aggiuntivi.
2. In base alla configurazione, scegli tra un ruolo di registrazione, una registrazione JSON strutturata o entrambi. Per ulteriori informazioni, consulta Aggiornamento della registrazione per un server.

Modifica la politica di sicurezza

Questa procedura spiega come modificare la politica di sicurezza di un server Transfer Family utilizzando la AWS Transfer Family console o AWS CLI.

> **Note**
>
> Se il tuo endpoint è compatibile con FIPS, non puoi modificare la politica di sicurezza FIPS con una politica di sicurezza non FIPS.

Console

Per modificare la politica di sicurezza utilizzando la console

1. Nella pagina dei dettagli del server, scegli Modifica accanto a Dettagli aggiuntivi.
2. Nella sezione Opzioni dell'algoritmo crittografico, scegli una politica di sicurezza che contenga gli algoritmi crittografici abilitati all'uso dal tuo server.

   Per ulteriori informazioni sulle policy di sicurezza, consulta Politiche di sicurezza per AWS Transfer Family i server.
3. Selezionare Salva.

   Verrai reindirizzato alla pagina dei dettagli del server dove puoi vedere la politica di sicurezza aggiornata.

AWS CLI

Per modificare la politica di sicurezza utilizzando la CLI

1. Esegui il comando seguente per visualizzare la politica di sicurezza corrente allegata al tuo server.

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

   Questo `describe-server` comando restituisce tutti i dettagli del server, inclusa la riga seguente:

   ```
   "SecurityPolicyName": "TransferSecurityPolicy-2018-11"
   ```

   In questo caso, la politica di sicurezza per il server è`TransferSecurityPolicy-2018-11`.
2. Assicurati di fornire al comando il nome esatto della politica di sicurezza. Ad esempio, esegui il comando seguente per aggiornare il server a`TransferSecurityPolicy-2023-05`.

```
aws transfer update-server --server-id your-server-id --security-policy-name
 "TransferSecurityPolicy-2023-05"
```

> **Note**
>
> I nomi delle politiche di sicurezza disponibili sono elencati in[Politiche di sicurezza per AWS Transfer Family i server](#).

In caso di successo, il comando restituisce il codice seguente e aggiorna la politica di sicurezza del server.

```
{
    "ServerId": "your-server-id"
}
```

Modifica il flusso di lavoro gestito per il tuo server

Sulla AWS Transfer Family console, è possibile modificare il flusso di lavoro gestito associato al server.

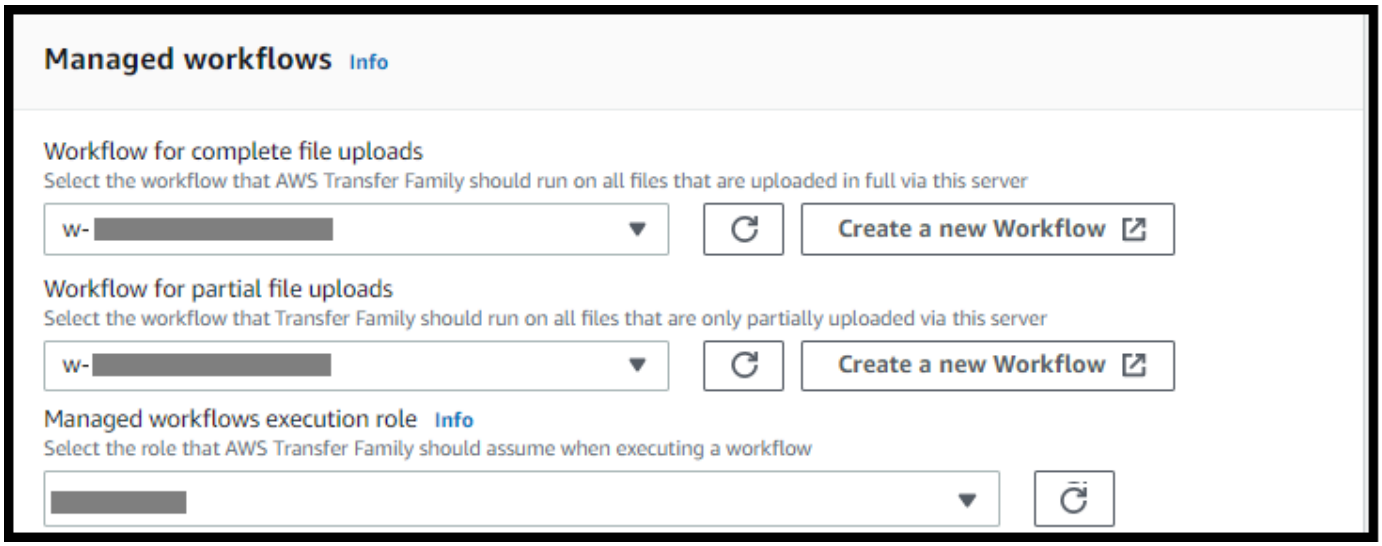
Per modificare il flusso di lavoro gestito

1. Nella pagina dei dettagli del server, scegli Modifica accanto a Dettagli aggiuntivi.
2. Nella pagina Modifica dettagli aggiuntivi, nella sezione Flussi di lavoro gestiti, seleziona un flusso di lavoro da eseguire su tutti i caricamenti.

> **Note**
>
> Se non disponi già di un flusso di lavoro, scegli Crea un nuovo flusso di lavoro per crearne uno.

   a. Seleziona l'ID del flusso di lavoro da utilizzare.

b. Scegli un ruolo di esecuzione. Questo è il ruolo che Transfer Family assume durante l'esecuzione dei passaggi del flusso di lavoro. Per ulteriori informazioni, consulta Politiche IAM per i flussi di lavoro. Seleziona Save (Salva.



3. Selezionare Salva. Si torna alla pagina dei dettagli del server.

Cambia i banner di visualizzazione per il tuo server

Sulla AWS Transfer Family console, puoi modificare i banner di visualizzazione associati al server.

Per modificare i banner di visualizzazione

1. Nella pagina dei dettagli del server, scegli Modifica accanto a Dettagli aggiuntivi.
2. Nella pagina Modifica dettagli aggiuntivi, nella sezione Banner di visualizzazione, inserisci il testo per i banner di visualizzazione disponibili.
3. Selezionare Salva. Verrai reindirizzato alla pagina dei dettagli del server.

Metti il tuo server online o offline

Sulla AWS Transfer Family console, puoi portare il tuo server online o metterlo offline.

Per portare il tuo server online

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.

2. Nel riquadro di navigazione, selezionare Servers (Server).
3. Seleziona la casella di controllo del server che è offline.
4. In Actions (Operazioni), scegliere Start (Avvia).

Un server può impiegare un paio di minuti per passare dalla modalità offline a quella online.

> **Note**
>
> Quando interrompi un server per metterlo offline, al momento continui ad addebitare i costi di servizio per quel server. Per eliminare i costi aggiuntivi basati sul server, elimina quel server.

Per mettere offline il server

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione, selezionare Servers (Server).
3. Seleziona la casella di controllo del server online.
4. In Actions (Operazioni), scegliere Stop (Arresta).

Durante l'avvio o lo spegnimento di un server, i server non sono disponibili per le operazioni sui file. La console non mostra gli stati di avvio e di arresto.

Se trovi la condizione di errore `START_FAILED` oppure`STOP_FAILED`, contattaci AWS Support per aiutarti a risolvere i tuoi problemi.

Gestisci le chiavi host per il tuo server compatibile con SFTP

> **Important**
>
> Se non avete intenzione di migrare gli utenti esistenti da un server compatibile con SFTP esistente a un nuovo server compatibile con SFTP, ignorate questa sezione.
> La modifica accidentale della chiave host di un server può creare problemi. A seconda di come è configurato il client SFTP, può fallire immediatamente, con il messaggio che non esiste una chiave host affidabile o presentare richieste pericolose. Se esistono script per automatizzare le connessioni, molto probabilmente anche questi fallirebbero.

Per impostazione predefinita, AWS Transfer Family fornisce una chiave host per il server compatibile con SFTP. Puoi sostituire la chiave host predefinita con una chiave host di un altro server. Fatelo solo se intendete spostare gli utenti esistenti da un server esistente abilitato per SFTP al nuovo server compatibile con SFTP.

Per evitare che agli utenti venga richiesto di verificare nuovamente l'autenticità del server compatibile con SFTP, importate la chiave host per il server locale nel server compatibile con SFTP. In questo modo si evita inoltre che gli utenti ricevano avvisi su un potenziale attacco. man-in-the-middle

Puoi anche ruotare periodicamente le chiavi dell'host, come misura di sicurezza aggiuntiva.

> **Note**
>
> Sebbene la console Transfer Family consenta di specificare e aggiungere chiavi host del server per tutti i server, queste chiavi sono utili solo per i server che utilizzano il protocollo SFTP.

Argomenti

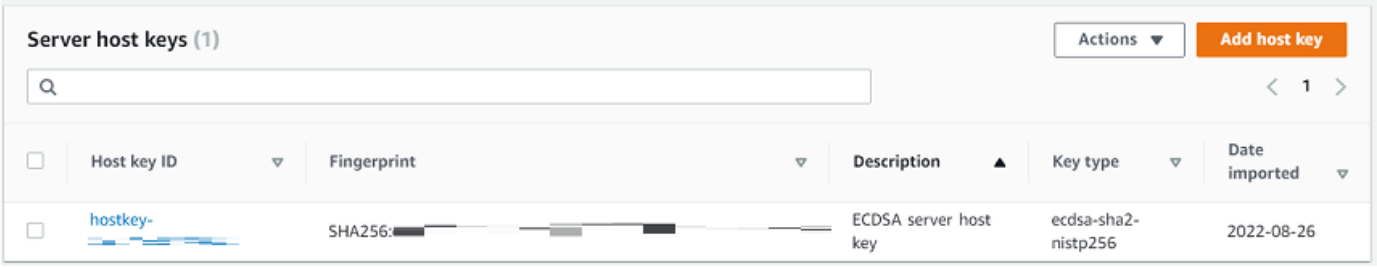
Aggiungere una chiave host del server aggiuntiva

Sulla AWS Transfer Family console, è possibile aggiungere ulteriori chiavi dell'host del server. L'aggiunta di chiavi host aggiuntive di diversi formati può essere utile per identificare un server quando i client si connettono ad esso, oltre che per migliorare il profilo di sicurezza. Ad esempio, se la chiave originale è una chiave RSA, è possibile aggiungere una chiave ECDSA aggiuntiva.

> **Note**
>
> Il client SFTP si connette utilizzando la prima chiave pubblica di cui dispone, che può corrispondere a una delle chiavi attive del server.

Per aggiungere una chiave host del server aggiuntiva

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server, quindi scegli un server che utilizza il protocollo SFTP.
3. Nella pagina dei dettagli del server, scorri verso il basso fino alla sezione Chiavi host del server.



4. Scegli Aggiungi chiave host.

   Viene visualizzata la pagina Aggiungi chiave host del server.
5. Nella sezione Chiave host del server, inserisci una chiave privata RSA, ECDSA o ED25519 che viene utilizzata per identificare il server quando i client si connettono ad esso tramite il server abilitato SFTP.

   > **Note**
   >
   > Quando crei una chiave host del server, assicurati di specificare (nessuna passphrase). `-N ""` Vedi Creazione di chiavi SSH su macOS, Linux o Unix i dettagli su come generare coppie di chiavi.
6. (Facoltativo) Aggiungi una descrizione per distinguere tra più chiavi host del server. Puoi anche aggiungere tag per la tua chiave.
7. Scegliere Add key (Aggiungi chiave). Si torna alla pagina dei dettagli del server.

Per aggiungere una chiave host utilizzando AWS Command Line Interface (AWS CLI), utilizza l'operazione the section called “ImportHostKey” API e fornisci la nuova chiave host. Se create un nuovo server compatibile con SFTP, fornite la chiave host come parametro nell'the section called “CreateServer”operazione API. È inoltre possibile utilizzare il AWS CLI per aggiornare la descrizione di una chiave host esistente.

Il `import-host-key` AWS CLI comando di esempio seguente importa una chiave host per il server abilitato per SFTP specificato.

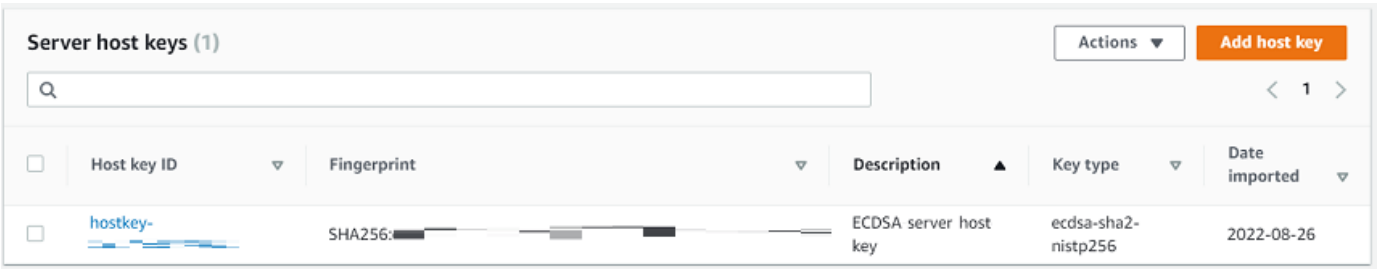
```
aws transfer import-host-key --description key-description --server-id your-server-id
 --host-key-body file://my-host-key
```

Eliminare una chiave host del server

Sulla AWS Transfer Family console, è possibile eliminare una chiave dell'host del server.

Per eliminare una chiave dell'host del server

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Nel riquadro di navigazione a sinistra, scegli Server, quindi scegli un server che utilizza il protocollo SFTP.
3. Nella pagina dei dettagli del server, scorri verso il basso fino alla sezione Chiavi host del server.



4. Nella sezione Chiavi host del server, seleziona una chiave, quindi in Azioni scegli Elimina.
5. Nella finestra di dialogo di conferma che appare, inserisci la parola**`delete`**, quindi scegli Elimina per confermare che desideri eliminare la chiave host.

La chiave host viene eliminata dalla pagina Server.

Per eliminare la chiave host utilizzando il AWS CLI, utilizza l'operazione the section called "DeleteHostKey" API e fornisci l'ID del server e l'ID della chiave host.

Il `delete-host-key` AWS CLI comando di esempio seguente elimina una chiave host per il server abilitato per SFTP specificato.

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

Ruota le chiavi dell'host del server

Periodicamente, è possibile ruotare la chiave dell'host del server.

In che modo il client sceglie la chiave dell'host del server

Il modo in cui Transfer Family sceglie la chiave del server da applicare dipende dalle condizioni del client SFTP, come spiegato qui. Il presupposto è che ci sia una chiave più vecchia e una chiave più recente.

- Un client SFTP non dispone di una chiave host pubblica precedente per il server. La prima volta che il client si connette al server, si verifica una delle seguenti situazioni:
  - Il client interrompe la connessione, se è configurato per farlo.
  - In alternativa, il client sceglie la prima chiave che corrisponde ai possibili algoritmi disponibili e chiede all'utente se quella chiave è attendibile. In tal caso, il client aggiorna automaticamente il `known_hosts` file (o qualsiasi file o risorsa di configurazione locale che il client utilizza per registrare le decisioni di fiducia) e inserisce quella chiave.
- Un client SFTP ha una vecchia chiave nel suo `known_hosts` file. Il client preferisce utilizzare questa chiave, anche se esiste una chiave più recente, per l'algoritmo di questa chiave o per un altro algoritmo. Questo perché il client ha un livello di fiducia più elevato per la chiave contenuta nel suo `known_hosts` file.
- Un client SFTP ha la nuova chiave (in uno qualsiasi degli algoritmi disponibili) nel suo file di `known_hosts` chiavi. Il client ignora le chiavi più vecchie perché non sono affidabili e utilizza la nuova chiave.
- Un client SFTP ha entrambe le chiavi nel suo `known_hosts` file. Il client sceglie la prima chiave per indice che corrisponde all'elenco delle chiavi disponibili offerto dal server.

Transfer Family preferisce che il client SFTP abbia tutte le chiavi nel suo `known_hosts` file, poiché ciò consente la massima flessibilità durante la connessione a un server Transfer Family. La rotazione delle chiavi si basa sul fatto che possono esistere più voci nel `known_hosts` file per lo stesso server Transfer Family.

Ruota la procedura della chiave host del server

Ad esempio, supponiamo di aver aggiunto il seguente set di chiavi host del server al server Transfer Family.

Chiavi dell'host del server

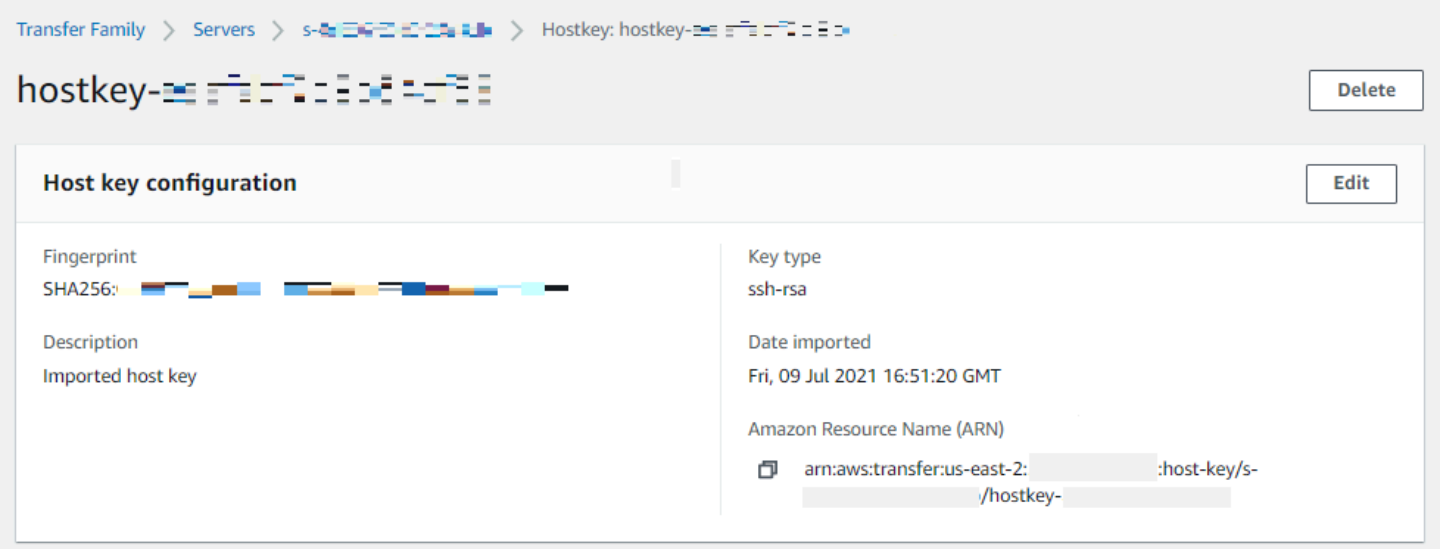
Tipo di chiave host	Data aggiunta al server
RSA	1 Aprile 2020
ECDSA	1 febbraio 2020
ED25519	1 dicembre 2019
RSA	1 ottobre 2019
ECDSA	1 giugno 2019
ED25519	1 marzo 2019

Per ruotare la chiave dell'host del server

1. Aggiungere una nuova chiave dell'host del server. Questa procedura è descritta in Aggiungere una chiave host del server aggiuntiva.
2. Eliminare una o più chiavi host dello stesso tipo aggiunte in precedenza. Questa procedura è descritta in Eliminare una chiave host del server.
3. Tutti i tasti sono visibili e possono essere attivi, in base al comportamento descritto in precedenza in In che modo il client sceglie la chiave dell'host del server.

Informazioni aggiuntive sulla chiave dell'host del server

È possibile selezionare una chiave host per visualizzare i relativi dettagli.



È possibile eliminare una chiave host o modificarne la descrizione dal menu Azioni nella schermata dei dettagli del server. Seleziona la chiave host, quindi scegli l'azione appropriata dal menu.

Monitoraggio dell'utilizzo nella console

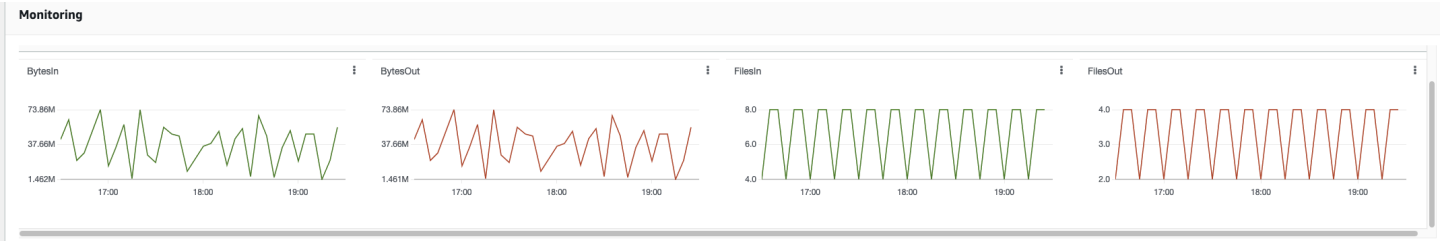
Puoi ottenere informazioni sulle metriche del tuo server nella pagina dei dettagli del server. In questo modo disponete di un unico posto per monitorare i carichi di lavoro relativi ai trasferimenti di file. Puoi tenere traccia del numero di file che hai scambiato con i tuoi partner e monitorare attentamente il loro utilizzo utilizzando una dashboard centralizzata. Per informazioni dettagliate, vedi Visualizza i dettagli dei server SFTP, FTPS e FTP. La tabella seguente descrive le metriche disponibili per Transfer Family.

Spazio dei nomi	Parametro	Descrizione
`AWS/Transfer`	`BytesIn`	Il numero totale di byte trasferiti nel server. Unità: numero

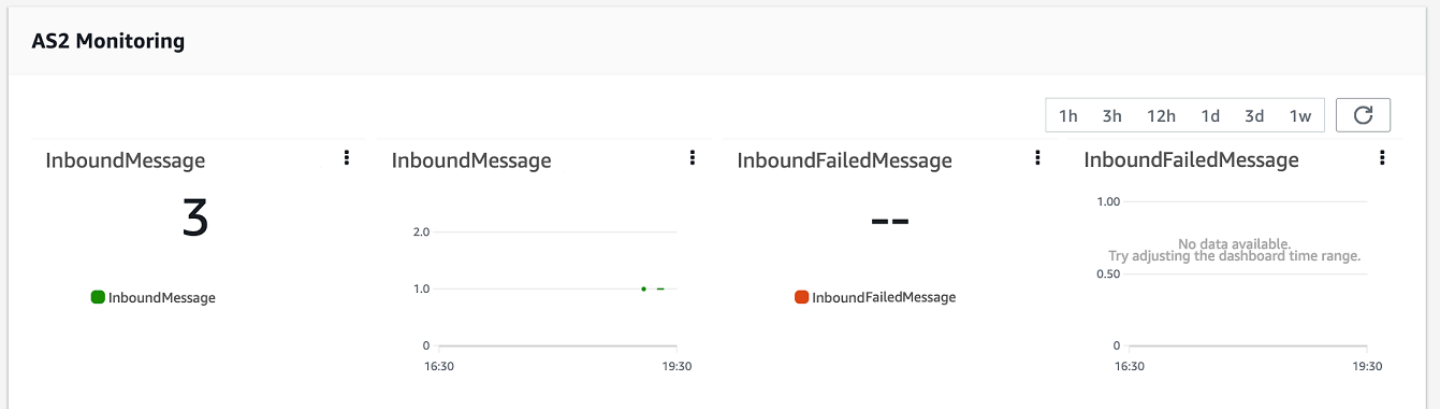
Spazio dei nomi	Parametro	Descrizione
		Periodo: 5 minuti
	`BytesOut`	Il numero totale di byte trasferiti dal server. Unità: numero Periodo: 5 minuti
	`FilesIn`	Il numero totale di file trasferiti nel server. Per i server che utilizzano il protocollo AS2, questa metrica rappresenta il numero di messaggi ricevuti. Unità: numero Periodo: 5 minuti
	`FilesOut`	Il numero totale di file trasferiti dal server. Unità: numero Periodo: 5 minuti
	`InboundMessage`	Il numero totale di messaggi AS2 ricevuti con successo da un partner commerciale. Unità: numero Periodo: 5 minuti
	`InboundFailedMessage`	Il numero totale di messaggi AS2 ricevuti senza successo da un partner commerciale. Cioè, un partner commerciale ha inviato un messaggio, ma il server Transfer Family non è stato in grado di elaborarlo correttamente. Unità: numero Periodo: 5 minuti

Spazio dei nomi	Parametro	Descrizione
	`OnUploadExecutionsStarted`	Il numero totale di esecuzioni del flusso di lavoro avviate sul server. Unità: numero Periodo: 1 minuto
	`OnUploadExecutionsSuccess`	Il numero totale di esecuzioni di workflow riuscite sul server. Unità: numero Periodo: 1 minuto
	`OnUploadExecutionsFailed`	Il numero totale di esecuzioni di workflow non riuscite sul server. Unità: numero Periodo: 1 minuto

La sezione Monitoraggio contiene quattro grafici individuali. Questi grafici mostrano i byte in entrata, i byte in uscita, i file in entrata e i file in uscita.



Per i server che hanno il protocollo AS2 abilitato, c'è una sezione di monitoraggio AS2 sotto le informazioni di monitoraggio. Questa sezione contiene dettagli sul numero di messaggi in entrata, sia riusciti che non riusciti.



Per aprire il grafico selezionato in una finestra separata, scegliete l'icona di espansione (). Puoi anche fare clic sull'icona con i puntini di sospensione verticali di un grafico () per aprire un menu a discesa con i seguenti elementi:

- Ingrandisci: apre il grafico selezionato in una finestra separata.
- Aggiorna: ricarica il grafico con i dati più recenti.
- Visualizza nei parametri: apre i dettagli delle metriche corrispondenti in Amazon. CloudWatch
- Visualizza i log: apre il gruppo di log corrispondente. CloudWatch

Gestione dei controlli di accesso

Puoi controllare l'accesso di un utente alle AWS Transfer Family risorse utilizzando una policy AWS Identity and Access Management (IAM). Una policy IAM è una dichiarazione, in genere in formato JSON, che consente un certo livello di accesso a una risorsa. Utilizzi una policy IAM per definire quali operazioni sui file desideri consentire agli utenti di eseguire e quali no. Puoi anche utilizzare una policy IAM per definire a quale bucket o a quali bucket Amazon S3 desideri consentire l'accesso ai tuoi utenti. Per specificare queste politiche per gli utenti, crei un ruolo IAM a AWS Transfer Family cui sono associate la politica IAM e la relazione di fiducia.

A ogni utente viene assegnato un ruolo IAM. Il tipo di ruolo IAM AWS Transfer Family utilizzato è chiamato ruolo di servizio. Quando un utente accede al tuo server, AWS Transfer Family assume il ruolo IAM mappato all'utente. Per ulteriori informazioni sulla creazione di un ruolo IAM che fornisce a un utente l'accesso a un bucket Amazon S3, consulta Creating a role to delegate permissions to an AWS service nella IAM User Guide.

Puoi concedere l'accesso in sola scrittura agli oggetti Amazon S3 utilizzando determinate autorizzazioni all'interno di una policy IAM. Per informazioni dettagliate, vedi Concedi la possibilità di scrivere ed elencare solo file.

Lo AWS Storage Blog contiene un post che descrive in dettaglio come configurare l'accesso con privilegi minimi. Per i dettagli, consulta Implementazione dell'accesso con privilegi minimi in un flusso di lavoro. AWS Transfer Family

> **Note**
>
> Se il tuo bucket Amazon S3 è crittografato utilizzando AWS Key Management Service (AWS KMS), devi specificare autorizzazioni aggiuntive nella tua policy. Per informazioni dettagliate, vedi Crittografia dei dati in Amazon S3. Inoltre, puoi trovare ulteriori informazioni sulle policy di sessione nella IAM User Guide.

Argomenti

- Consentire l'accesso in lettura e scrittura a un bucket Amazon S3
- Creazione di una politica di sessione per un bucket Amazon S3
- Impedire agli utenti di funzionare mkdir in un bucket S3

Consentire l'accesso in lettura e scrittura a un bucket Amazon S3

Questa sezione descrive come creare una policy IAM che consenta l'accesso in lettura e scrittura a uno specifico bucket Amazon S3. L'assegnazione di un ruolo IAM con questa policy IAM all'utente fornisce all'utente l'accesso in lettura/scrittura al bucket Amazon S3 specificato.

La seguente policy fornisce l'accesso programmatico in lettura, scrittura e tagging a un bucket Amazon S3. Le `PutObjectACL` istruzioni `GetObjectACL` e sono obbligatorie solo se è necessario abilitare Cross Account Access. Cioè, il tuo server Transfer Family deve accedere a un bucket in un altro account.

```
{
  "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/*"]
    }
  ]
}
```

L'operazione `ListBucket` richiede l'autorizzazione per il bucket stesso. Le operazioni `PUT`, `GET` e `DELETE` richiedono autorizzazioni oggetto. Poiché si tratta di risorse diverse, vengono specificate utilizzando diversi Amazon Resource Names (ARN).

Per limitare ulteriormente l'accesso degli utenti solo al `home` prefisso del bucket Amazon S3 specificato, consulta. Creazione di una politica di sessione per un bucket Amazon S3

Creazione di una politica di sessione per un bucket Amazon S3

Una policy di sessione è una policy AWS Identity and Access Management (IAM) che limita gli utenti a determinate porzioni di un bucket Amazon S3. valutando l'accesso in tempo reale.

> **Note**
>
> Le policy di sessione vengono utilizzate solo con Amazon S3. Per Amazon EFS, utilizzi le autorizzazioni dei file POSIX per limitare l'accesso.

Puoi utilizzare una policy di sessione quando devi concedere lo stesso accesso a un gruppo di utenti a una parte particolare del tuo bucket Amazon S3. Ad esempio, è possibile che un gruppo di utenti richieda l'accesso solo alla directory `home`. Quel gruppo di utenti condivide lo stesso ruolo IAM.

> **Note**
>
> La lunghezza massima di una policy di sessione è di 2048 caratteri. Per maggiori dettagli, consulta il parametro Policy request per l'`CreateUser`azione nel riferimento API.

Per creare una policy di sessione, utilizza le seguenti variabili di policy nella tua policy IAM:

- `${transfer:HomeBucket}`
- `${transfer:HomeDirectory}`
- `${transfer:HomeFolder}`
- `${transfer:UserName}`

> **Important**
>
> Non puoi utilizzare le variabili precedenti in Managed Policies. Né puoi usarle come variabili di policy in una definizione di ruolo IAM. Crei queste variabili in una policy IAM e le fornisci direttamente durante la configurazione dell'utente. Inoltre, non è possibile utilizzare la `${aws:Username}` variabile in questa politica di sessione. Questa variabile si riferisce a un nome utente IAM e non al nome utente richiesto da AWS Transfer Family.

Il codice seguente mostra un esempio di policy di sessione.

```
{
  "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**
>
> L'esempio di policy precedente presuppone che le directory home degli utenti siano impostate in modo da includere una barra finale, a indicare che si tratta di una directory. Se, al contrario, imposti quella di un utente `HomeDirectory` senza la barra finale, dovresti includerla come parte della tua politica.

Nella policy di esempio precedente, prendete nota dell'uso dei parametri `transfer:HomeFoldertransfer:HomeBucket`, e `transfer:HomeDirectory` policy. Questi parametri sono impostati per `HomeDirectory` i parametri configurati per l'utente, come descritto in HomeDirectoryandImplementazione del metodo API Gateway. Questi parametri hanno le seguenti definizioni:

- Il `transfer:HomeBucket` parametro viene sostituito con il primo componente di`HomeDirectory`.
- Il `transfer:HomeFolder` parametro viene sostituito con le parti rimanenti del `HomeDirectory` parametro.
- Al `transfer:HomeDirectory` parametro è stata rimossa la barra anteriore (`/`) iniziale in modo che possa essere utilizzata come parte di un Amazon Resource Name (ARN) di S3 in un'istruzione. `Resource`

> **Note**
>
> Se utilizzi directory logiche, ovvero quelle dell'utente, `LOGICAL` questi parametri di policy (`HomeBucket`, e) `homeDirectoryType` non sono supportati. `HomeDirectory` `HomeFolder`

Ad esempio, supponiamo che il `HomeDirectory` parametro configurato per l'utente Transfer Family sia`/home/bob/amazon/stuff/`.

- `transfer:HomeBucket`è impostato su`/home`.
- `transfer:HomeFolder`è impostato su`/bob/amazon/stuff/`.
- `transfer:HomeDirectory`diventa`home/bob/amazon/stuff/`.

Il primo `"Sid"` consente all'utente di elencare tutte le directory a partire da`/home/bob/amazon/stuff/`.

Il secondo `"Sid"` limita l'`get`accesso dell'utente `put` e quello dello stesso percorso,. `/home/bob/amazon/stuff/`

Con la politica precedente in vigore, quando un utente effettua il login, può accedere solo agli oggetti nella propria home directory. Al momento della connessione, AWS Transfer Family sostituisce queste variabili con i valori appropriati per l'utente. Questo rende più semplice applicare gli stessi documenti di policy a più utenti. Questo approccio riduce il sovraccarico della gestione dei ruoli e delle policy di IAM per la gestione dell'accesso degli utenti al bucket Amazon S3.

Puoi anche utilizzare una policy di sessione per personalizzare l'accesso per ciascuno dei tuoi utenti in base ai tuoi requisiti aziendali. Per ulteriori informazioni, consulta Permissions for AssumeRole, AssumeRoleWith SAML e AssumeRoleWithWebIdentity nella IAM User Guide.

> **Note**
>
> AWS Transfer Family memorizza il codice JSON della policy, anziché l'Amazon Resource Name (ARN) della policy. Pertanto, quando modifichi la policy nella console IAM, devi tornare alla AWS Transfer Family console e aggiornare gli utenti con i contenuti più recenti della policy. Puoi aggiornare l'utente nella scheda Informazioni sulla politica nella sezione Configurazione utente.
> Se si utilizza il AWS CLI, è possibile utilizzare il seguente comando per aggiornare la politica.
>
> ```
> aws transfer update-user --server-id server --user-name user --policy \
>    "$(aws iam get-policy-version --policy-arn policy --version-id version --
> output json)"
> ```

Impedire agli utenti di funzionare **`mkdir`** in un bucket S3

Puoi limitare la capacità degli utenti di creare una directory in un bucket Amazon S3. A tal fine, crei una policy IAM che consenta l'`s3:PutObject`azione ma la neghi anche quando la chiave termina con un «/» (barra). La seguente policy di esempio consente agli utenti di caricare file in un bucket Amazon S3 ma nega il mkdir comando nel bucket Amazon S3.

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

> **Note**
>
> La seconda riga di risorse impedisce agli utenti di creare sottocartelle eseguendo un comando come. `put my-file DOC-EXAMPLE-BUCKET/new-folder/my-file`

Registrazione per AWS Transfer Family

AWS Transfer Familysi integra sia AWS CloudTrail con Amazon che con Amazon CloudWatch. CloudTrail e CloudWatch servono a scopi diversi ma complementari:

- CloudTrail è un AWS servizio che crea un registro delle azioni intraprese all'interno dell'utenteAccount AWS. Monitora e registra continuamente le chiamate API per attività come accessi alla console, AWS Command Line Interface comandi e chiamate SDK/API. Ciò consente di tenere un registro di chi ha intrapreso quali azioni, quando e da dove. CloudTrail facilita il controllo, la gestione degli accessi e la conformità normativa fornendo una cronologia di tutte le attività nell'AWSambiente. Per i dettagli, consulta la Guida per l'AWS CloudTrailutente.
- CloudWatch è un servizio di monitoraggio per AWS risorse e applicazioni. Raccoglie metriche e registri per fornire visibilità sull'utilizzo delle risorse, sulle prestazioni delle applicazioni e sullo stato generale del sistema. CloudWatch aiuta con attività operative come la risoluzione dei problemi, l'impostazione di allarmi e la scalabilità automatica. Per i dettagli, consulta la Amazon CloudWatch User Guide.

Argomenti

AWS CloudTrailregistrazione per AWS Transfer Family

AWS Transfer Familyè integrato conAWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, da un ruolo o da un AWS servizio in. AWS Transfer Family CloudTrail acquisisce tutte le chiamate API AWS Transfer Family come eventi. Le chiamate acquisite includono le chiamate dalla console di AWS Transfer Family e le chiamate di codice alle operazioni delle API AWS Transfer Family.

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Per una registrazione continua degli eventi nell'account AWS che includa gli eventi per AWS Transfer Family, crea un trail. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte AWS Transfer Family le azioni vengono registrate CloudTrail e documentate in. ActionsAPI reference Ad esempio, le chiamate a `ListUsers` e `CreateServer` le `StopServer` azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente AWS Identity and Access Management o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Transfer Family Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi.

Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviataAWS Transfer Family, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Argomenti

Abilita la AWS CloudTrail registrazione

Puoi monitorare le chiamate API di AWS Transfer Family utilizzando AWS CloudTrail. Grazie al monitoraggio delle chiamate API, puoi ottenere informazioni di sicurezza e operative utili. Se hai abilitato la registrazione a livello di oggetto di Amazon S3, `RoleSessionName` è contenuta nel campo Requester come. `[AWS:Role Unique Identifier]/username.sessionid@server-id` Per ulteriori informazioni sugli identificatori univoci dei ruoli AWS Identity and Access Management (IAM), consulta Identificatori univoci nella Guida per l'utente. AWS Identity and Access Management

> **Important**
>
> La lunghezza massima `RoleSessionName` è di 64 caratteri. Se `RoleSessionName` è più lungo, `server-id` viene troncato.

Esempio di registrazione per la creazione di un server

L'esempio seguente mostra una voce di CloudTrail registro (in formato JSON) che illustra l'`CreateServer`azione.

```
{
    "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"
}
```

CloudWatch Registrazione Amazon per AWS Transfer Family

Amazon CloudWatch monitora AWS Transfer Family le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi utilizzarlo CloudWatch per raccogliere e tenere traccia delle metriche, che sono variabili che puoi misurare per le tue risorse e applicazioni.

La CloudWatch home page mostra automaticamente le metriche su Transfer Family e ogni altro AWS servizio che utilizzi. Puoi inoltre creare pannelli di controllo personalizzati per visualizzare i parametri relativi alle applicazioni personalizzate e visualizzare raccolte personalizzate dei parametri scelti.

Puoi creare allarmi con parametri di controllo e inviare notifiche o apportare automaticamente modifiche alle risorse che stai monitorando quando viene superata una soglia. Ad esempio, è possibile monitorare i file trasferiti su un server Transfer Family e utilizzare tali dati per determinare se è necessario implementare server aggiuntivi per gestire un carico maggiore. È inoltre possibile utilizzare questi dati per interrompere o eliminare le istanze sottoutilizzate per risparmiare denaro.

Tipi di CloudWatch registrazione per Transfer Family

Transfer Family offre due modi per registrare gli eventi su CloudWatch:

- Registrazione strutturata JSON
- Registrazione tramite un ruolo di registrazione

Per i server Transfer Family, puoi scegliere il meccanismo di registrazione che preferisci. Per i connettori e i flussi di lavoro, sono supportati solo i ruoli di registrazione.

Registrazione strutturata JSON

Per la registrazione degli eventi del server, consigliamo di utilizzare la registrazione strutturata JSON. Ciò fornisce un formato di registrazione più completo che consente l'interrogazione dei log. CloudWatch Per questo tipo di registrazione, la policy IAM per l'utente che crea il server (o modifica la configurazione di registrazione del server) deve contenere le seguenti autorizzazioni:

- logs:CreateLogDelivery
- logs:DeleteLogDelivery
- logs:DescribeLogGroups
- logs:DescribeResourcePolicies
- logs:GetLogDelivery
- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

Di seguito è riportata una policy di esempio.

```
{
    "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:Account AWS:log-group:/aws/transfer/*"
        }
    ]
}
```

Per i dettagli sulla configurazione della registrazione strutturata JSON, consulta. Creazione, aggiornamento e visualizzazione della registrazione per i server

Ruolo di registrazione

Per registrare gli eventi per un flusso di lavoro gestito collegato a un server, nonché per i connettori, è necessario specificare un ruolo di registrazione. Per impostare l'accesso, crei una policy IAM

basata sulle risorse e un ruolo IAM che fornisce tali informazioni di accesso. Di seguito è riportato un esempio di policy per un utente in grado di registrare Account AWS gli eventi del server.

```
{
    "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/*"
        }
    ]
}
```

Per i dettagli sulla configurazione di un ruolo di registrazione per registrare gli eventi del flusso di lavoro, vedere. Gestione della registrazione per i flussi di lavoro

Argomenti

- Creazione, aggiornamento e visualizzazione della registrazione per i server
- Gestione della registrazione per i flussi di lavoro
- Configura il CloudWatch ruolo di registrazione
- Visualizzazione dei flussi di log di Transfer Family
- Creazione di CloudWatch allarmi Amazon
- Registrazione delle chiamate API di Amazon S3 nei log di accesso S3
- Esempi per limitare il problema confuso dei deputati
- CloudWatch struttura di log per Transfer Family
- Esempi di voci di CloudWatch registro
- Utilizzo delle CloudWatch metriche per Transfer Family
- Utilizzo Notifiche all'utente AWS con AWS Transfer Family
- Utilizzo delle query per filtrare le voci di registro

Creazione, aggiornamento e visualizzazione della registrazione per i server

Per tutti i AWS Transfer Family server, è possibile scegliere tra due opzioni di registrazione: `LoggingRole` (utilizzata per la registrazione dei flussi di lavoro collegati al server) oppure. `StructuredLogDestinations` Alcuni dei vantaggi derivanti dall'uso di `StructuredLogDestinations` sono:

- Ricevi i log in un formato JSON strutturato.
- Interroga i tuoi log con Amazon CloudWatch Logs Insights, che rileva automaticamente i campi in formato JSON.
- La condivisione dei gruppi di log tra AWS Transfer Family le risorse consente di combinare i flussi di log provenienti da più server in un unico gruppo di log, semplificando la gestione delle configurazioni di monitoraggio e delle impostazioni di conservazione dei log.
- Crea metriche e visualizzazioni aggregate che possono essere aggiunte ai dashboard. CloudWatch
- Tieni traccia dei dati sull'utilizzo e sulle prestazioni utilizzando i gruppi di log per creare metriche, visualizzazioni e dashboard di log consolidati.

Le opzioni per `LoggingRole` o `StructuredLogDestinations` sono configurate e controllate separatamente. Per ogni server, è possibile impostare uno o entrambi i metodi di registrazione oppure configurare il server in modo che non disponga di alcuna registrazione (sebbene questa operazione non sia consigliata).

Se crei un nuovo server utilizzando la console Transfer Family, la registrazione è abilitata per impostazione predefinita. Dopo aver creato il server, puoi utilizzare la chiamata `UpdateServer` API per modificare la configurazione di registrazione. Per i dettagli, consulta StructuredLogDestinazioni.

Attualmente, per i flussi di lavoro, se desideri abilitare la registrazione, devi specificare un ruolo di registrazione:

- Se si associa un flusso di lavoro a un server, utilizzando la chiamata `CreateServer` o l'`UpdateServer`API, il sistema non crea automaticamente un ruolo di registrazione. Se si desidera registrare gli eventi del flusso di lavoro, è necessario associare in modo esplicito un ruolo di registrazione al server.
- Se si crea un server utilizzando la console Transfer Family e si collega un flusso di lavoro, i log vengono inviati a un gruppo di log che contiene l'ID del server nel nome. Il formato è`/aws/transfer/`*`server-id`*, ad esempio,`/aws/transfer/s-1111aaaa2222bbbb3`. I log del server possono essere inviati allo stesso gruppo di log o a uno diverso.

Considerazioni sulla registrazione per la creazione e la modifica dei server nella console

- I nuovi server creati tramite la console supportano solo la registrazione JSON strutturata, a meno che al server non sia collegato un flusso di lavoro.
- La registrazione senza registrazione non è un'opzione per i nuovi server creati nella console.
- I server esistenti possono abilitare la registrazione JSON strutturata tramite la console in qualsiasi momento.
- L'abilitazione della registrazione JSON strutturata tramite la console disabilita il metodo di registrazione esistente, in modo da non addebitare due volte ai clienti. L'eccezione è se un flusso di lavoro è collegato al server.
- Se abiliti la registrazione JSON strutturata, non puoi disabilitarla successivamente tramite la console.
- Se abiliti la registrazione JSON strutturata, puoi modificare la destinazione del gruppo di log tramite la console in qualsiasi momento.
- Se abiliti la registrazione JSON strutturata, non puoi modificare il ruolo di registrazione tramite la console se hai abilitato entrambi i tipi di registrazione tramite l'API. L'eccezione è se al server è collegato un flusso di lavoro. Tuttavia, il ruolo di registrazione continua a essere visualizzato in Dettagli aggiuntivi.

Considerazioni sulla registrazione per la creazione e la modifica di server utilizzando l'API o l'SDK

- Se crei un nuovo server tramite l'API, puoi configurare uno o entrambi i tipi di registrazione oppure scegliere nessuna registrazione.
- Per i server esistenti, abilita e disabilita la registrazione JSON strutturata in qualsiasi momento.
- Puoi modificare il gruppo di log tramite l'API in qualsiasi momento.
- Puoi modificare il ruolo di registrazione tramite l'API in qualsiasi momento.

Per abilitare la registrazione strutturata, è necessario accedere a un account con le seguenti autorizzazioni

- `logs:CreateLogDelivery`
- `logs:DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`

- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

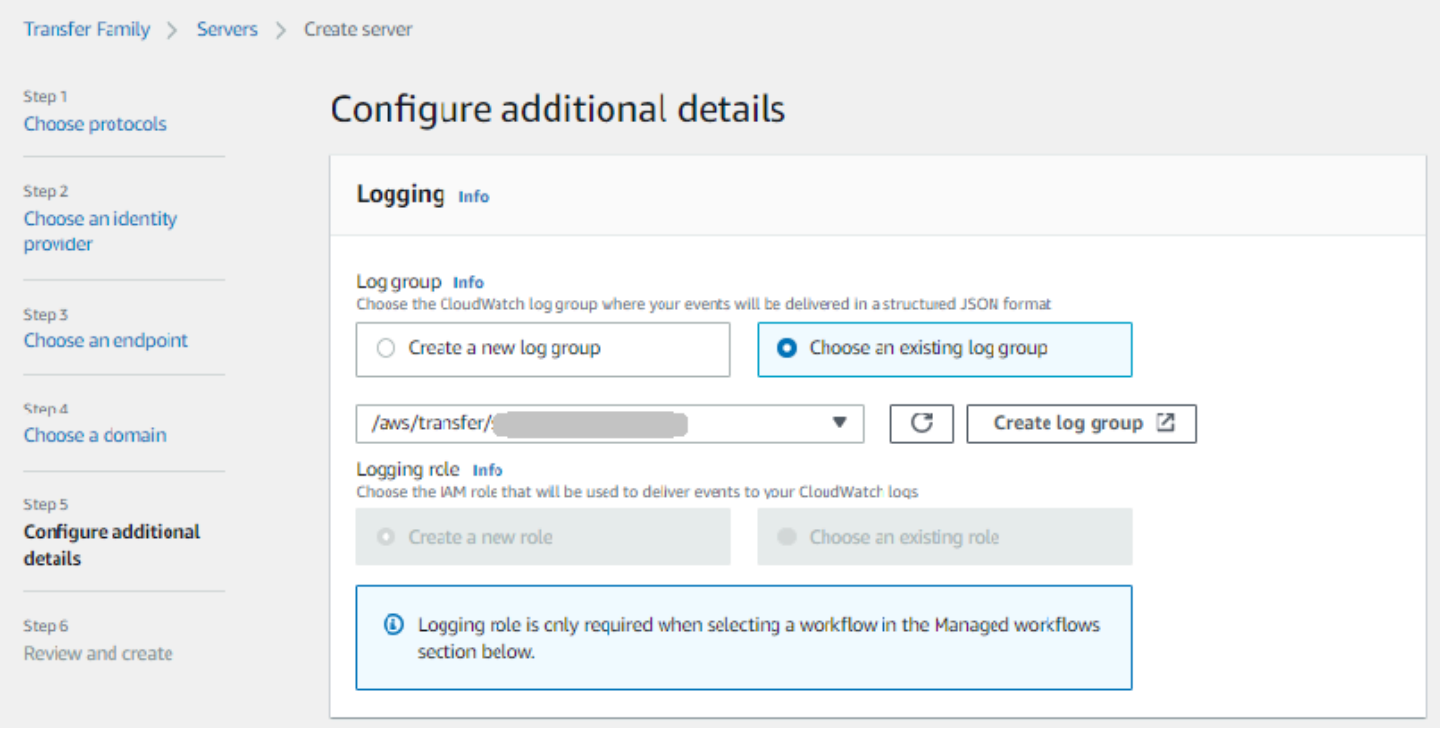
Un esempio di politica è disponibile nella sezione. Configura il CloudWatch ruolo di registrazione

Argomenti

- Creazione della registrazione per i server
- Aggiornamento della registrazione per un server
- Visualizzazione della configurazione del server

Creazione della registrazione per i server

Quando si crea un nuovo server, nella pagina Configura dettagli aggiuntivi, è possibile specificare un gruppo di log esistente o crearne uno nuovo.



Se scegli Crea gruppo di log, la CloudWatch console (https://console.aws.amazon.com/cloudwatch/) apre la pagina Crea gruppo di log. Per i dettagli, consulta Creare un gruppo di log in CloudWatch Logs.

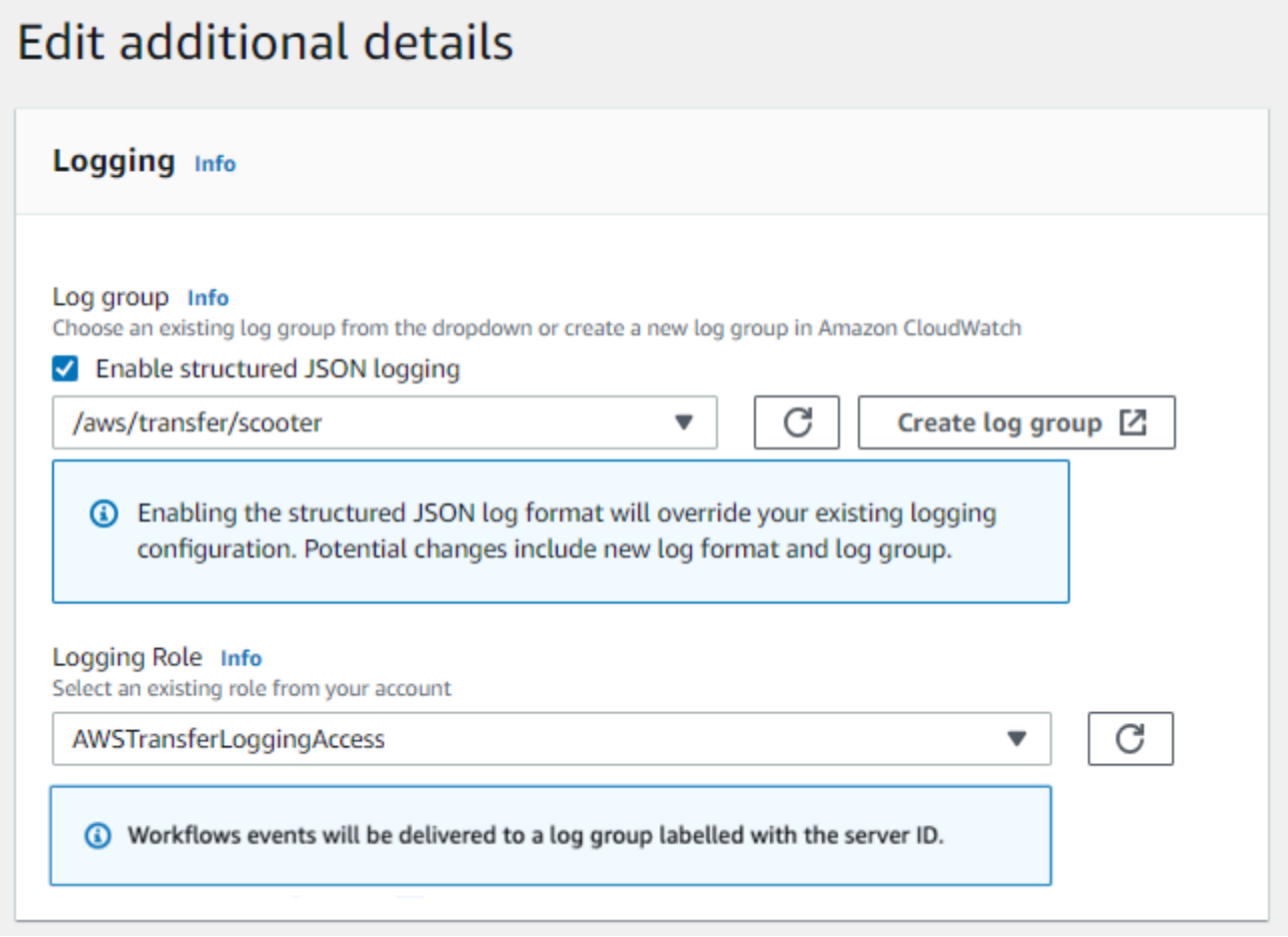
Aggiornamento della registrazione per un server

I dettagli per la registrazione dipendono dallo scenario dell'aggiornamento.

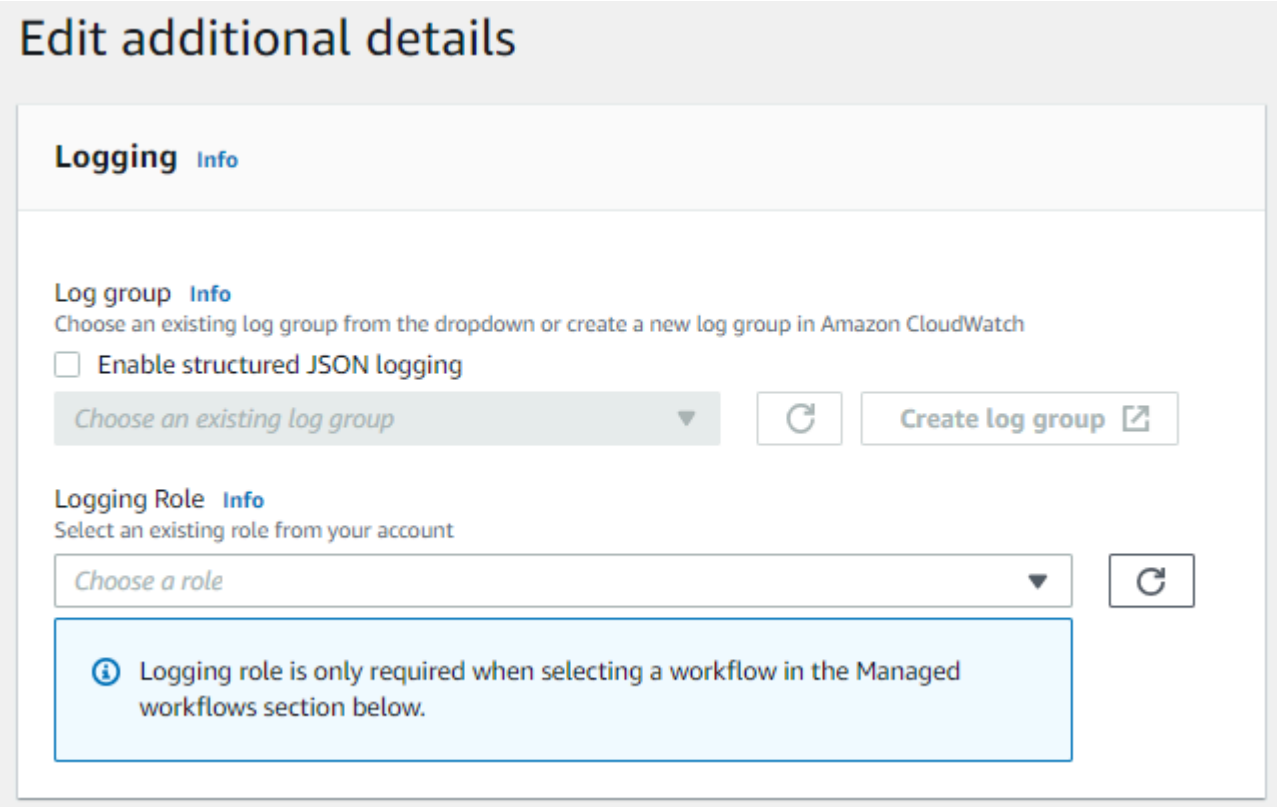
> **Note**
>
> Quando si sceglie la registrazione JSON strutturata, può verificarsi un ritardo, in rari casi, in cui Transfer Family interrompe la registrazione nel vecchio formato, ma impiega del tempo per avviare la registrazione nel nuovo formato JSON. Ciò può causare eventi che non vengono registrati. Non ci saranno interruzioni del servizio, ma è necessario fare attenzione a trasferire i file durante la prima ora dopo aver modificato il metodo di registrazione, poiché i log potrebbero essere eliminati.

Se state modificando un server esistente, le opzioni disponibili dipendono dallo stato del server.

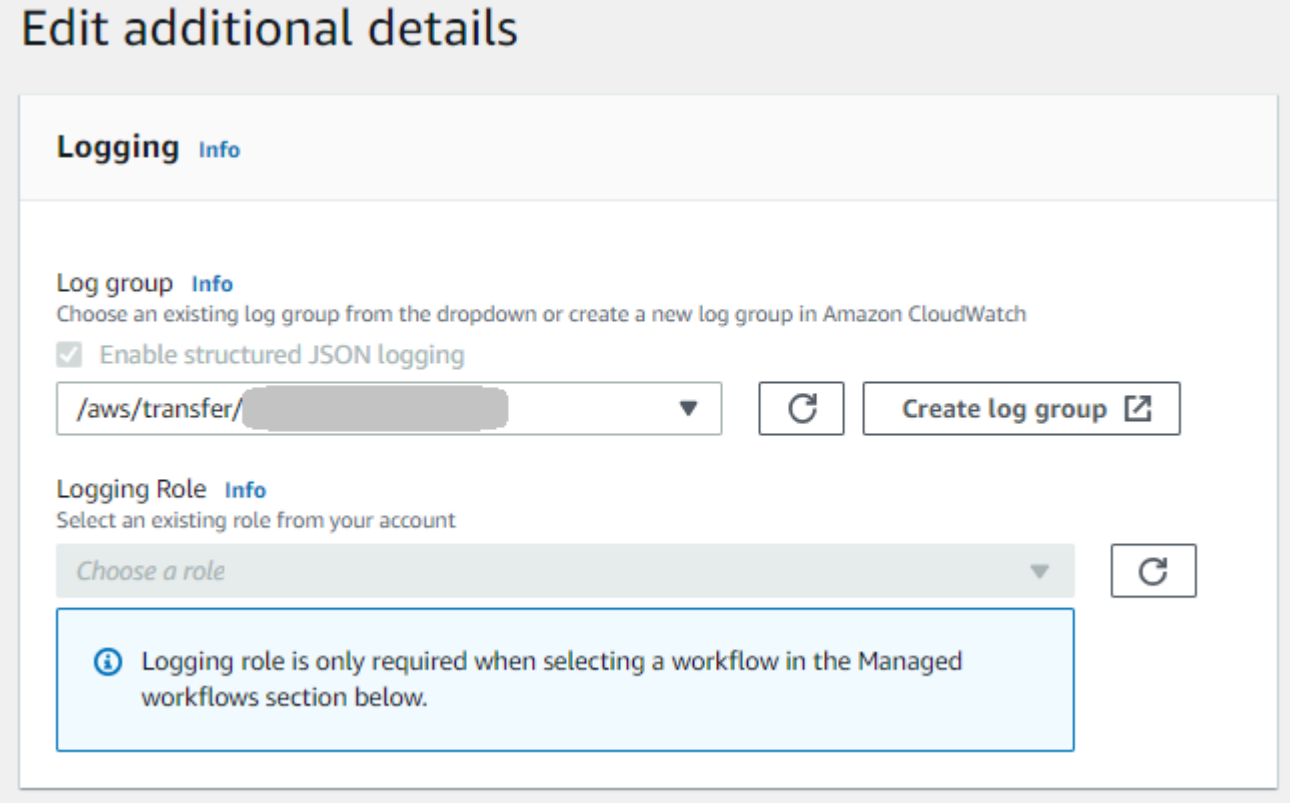
- Il server ha già un ruolo di registrazione abilitato, ma non ha la registrazione JSON strutturata abilitata.



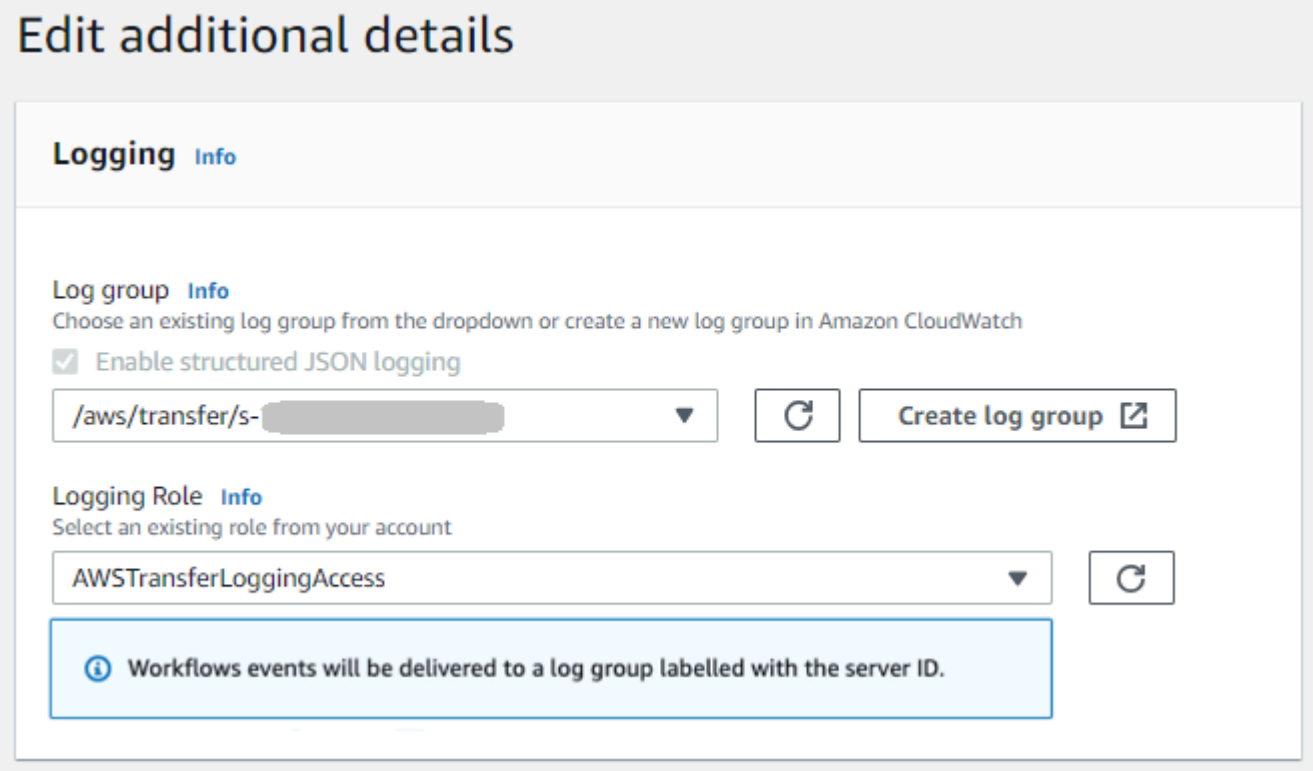
- Il server non ha alcuna registrazione abilitata.



- Nel server è già abilitata la registrazione JSON strutturata, ma non è stato specificato un ruolo di registrazione.



- Il server ha già abilitato la registrazione JSON strutturata e ha inoltre specificato un ruolo di registrazione.

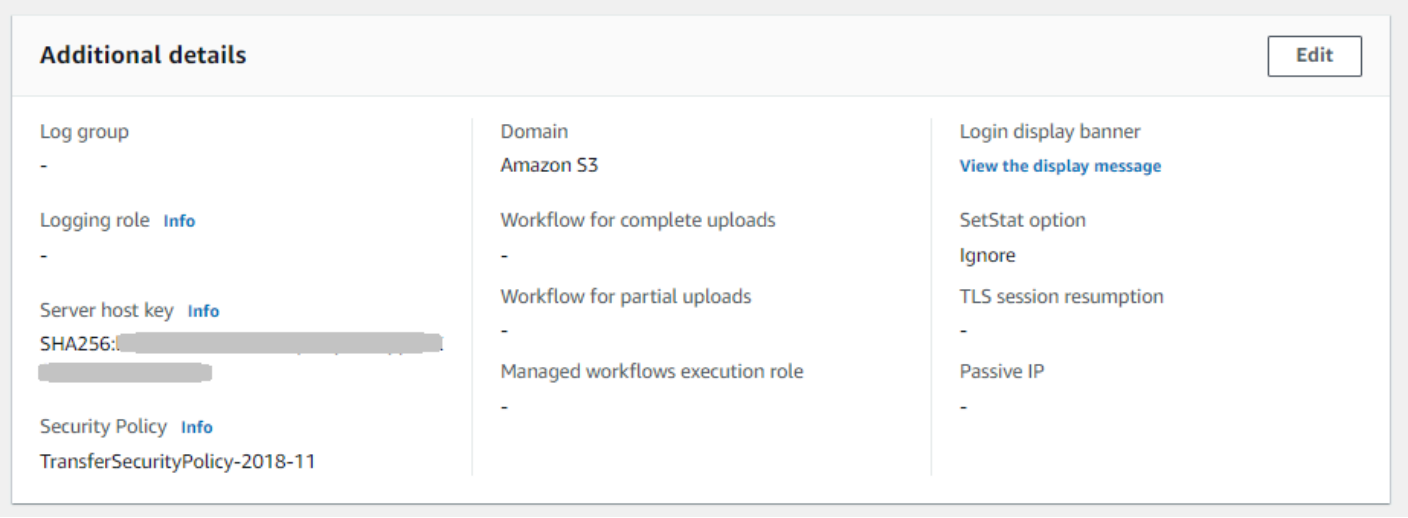


Visualizzazione della configurazione del server

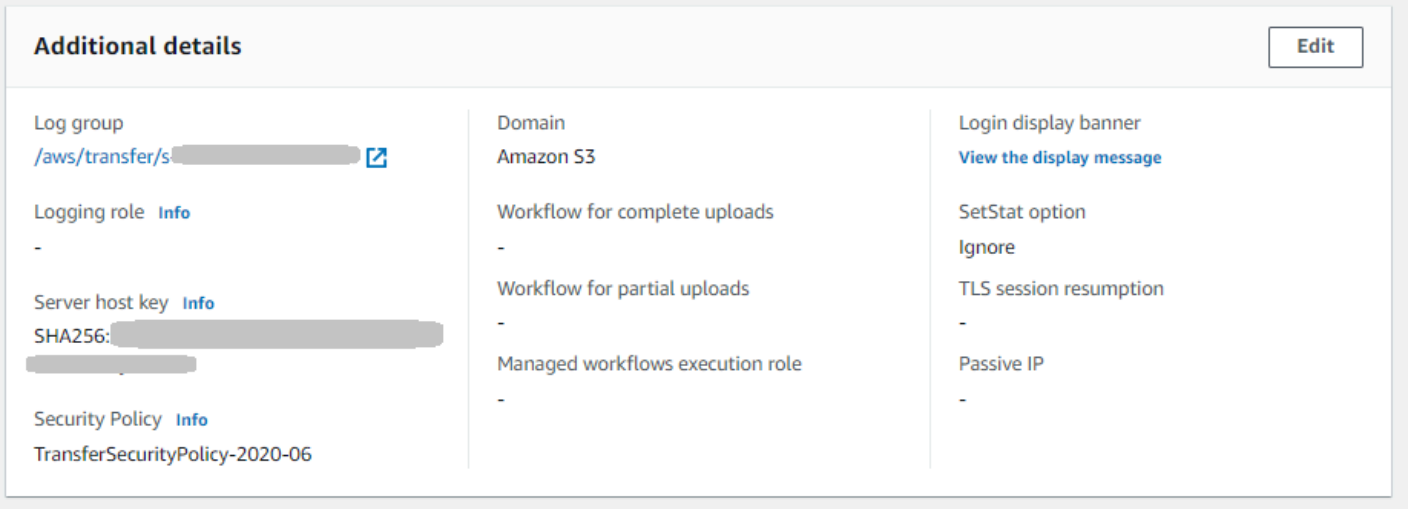
I dettagli per la pagina di configurazione del server dipendono dallo scenario in uso:

A seconda dello scenario, la pagina di configurazione del server potrebbe essere simile a uno dei seguenti esempi:

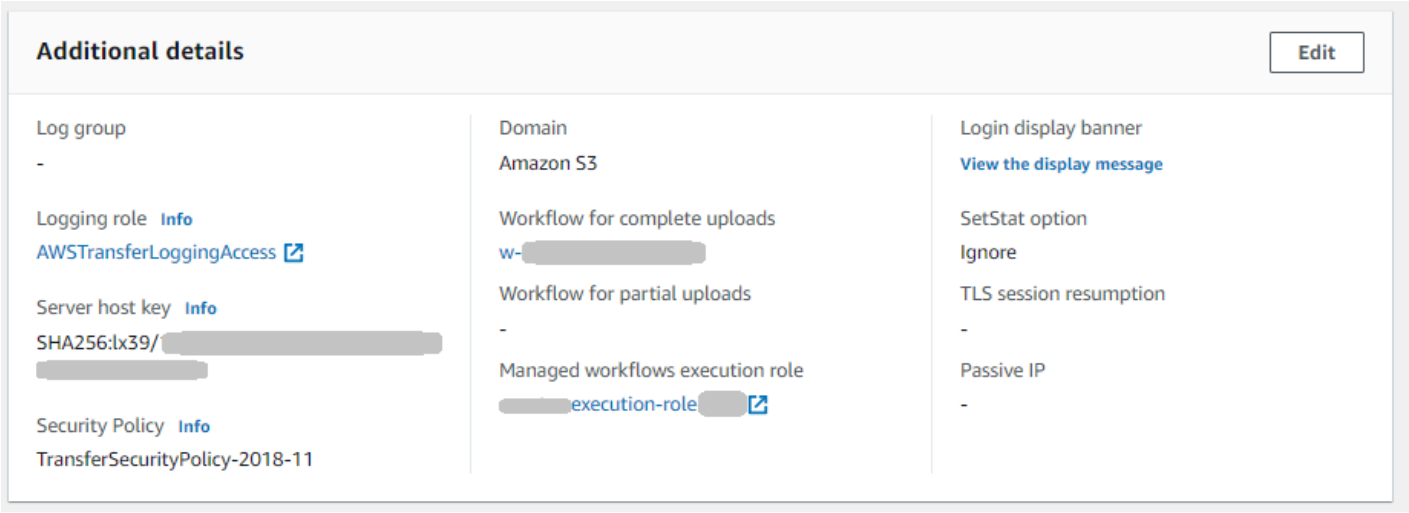
- Non è abilitata la registrazione.



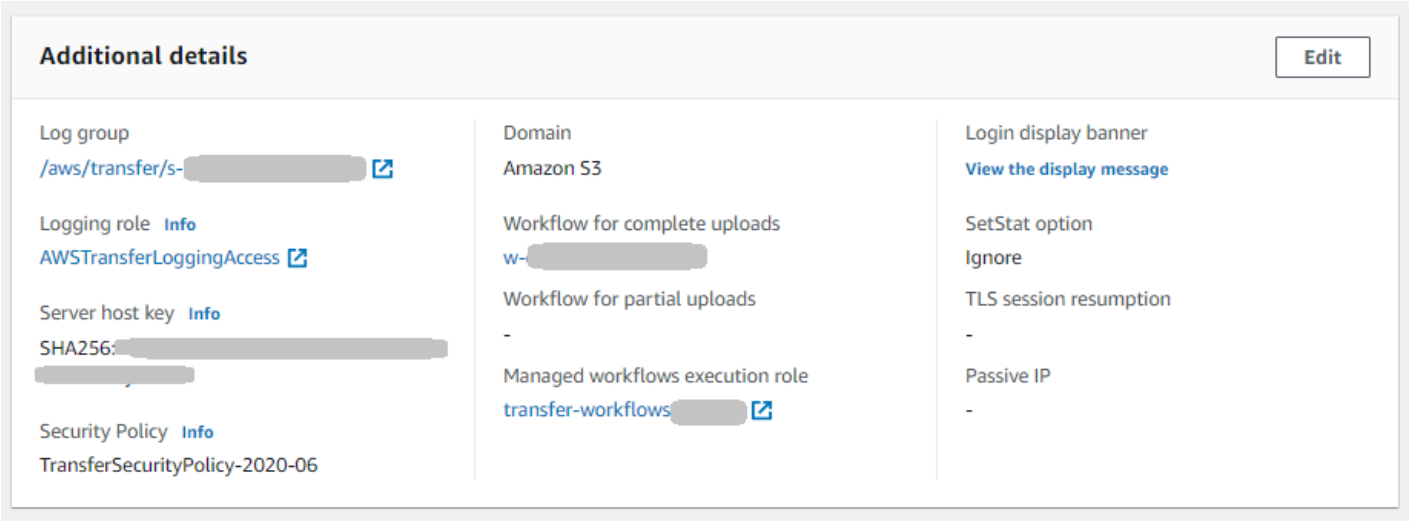
- La registrazione JSON strutturata è abilitata.



- Il ruolo di registrazione è abilitato, ma la registrazione JSON strutturata non è abilitata.



- Entrambi i tipi di registrazione (ruolo di registrazione e registrazione JSON strutturata) sono abilitati.



Gestione della registrazione per i flussi di lavoro

CloudWatch fornisce controlli e registrazioni consolidati per l'avanzamento e i risultati del flusso di lavoro. Inoltre, AWS Transfer Family fornisce diverse metriche per i flussi di lavoro. È possibile visualizzare le metriche relative al numero di esecuzioni di flussi di lavoro avviate, completate con successo e non riuscite nel minuto precedente. Tutte le CloudWatch metriche per Transfer Family sono descritte in[Utilizzo delle CloudWatch metriche per Transfer Family](#).

Visualizza i CloudWatch log di Amazon per i flussi di lavoro

1. Apri la CloudWatch console Amazon all'[indirizzo https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Nel riquadro di navigazione a sinistra, scegli Registri, quindi scegli Gruppi di log.

3. Nella pagina Gruppi di log, nella barra di navigazione, scegli la regione corretta per il tuo AWS Transfer Family server.
4. Scegli il gruppo di log corrispondente al tuo server.

   Ad esempio, se l'ID del tuo server è`s-1234567890abcdef0`, il tuo gruppo di log lo è`/aws/transfer/s-1234567890abcdef0`.
5. Nella pagina dei dettagli del gruppo di log relativa al server, vengono visualizzati i flussi di log più recenti. Esistono due flussi di log per l'utente che stai esplorando:

   - Uno per ogni sessione di Secure Shell (SSH) File Transfer Protocol (SFTP).
   - Uno per il flusso di lavoro che viene eseguito per il server. Il formato per il flusso di log per il flusso di lavoro è*`username`*`.`*`workflowID`*`.`*`uniqueStreamSuffix`*.

   Ad esempio, se il tuo utente è`mary-major`, hai i seguenti flussi di log:

   ```
   mary-major-east.1234567890abcdef0
   mary.w-abcdef01234567890.021345abcdef6789
   ```

   > **Note**
   >
   > Gli identificatori alfanumerici a 16 cifre elencati in questo esempio sono fittizi. I valori che vedi in Amazon CloudWatch sono diversi.

La pagina degli eventi di registro `mary-major-usa-east.1234567890abcdef0` mostra i dettagli di ogni sessione utente e il flusso di `mary.w-abcdef01234567890.021345abcdef6789` registro contiene i dettagli del flusso di lavoro.

Di seguito è riportato un esempio di flusso di log per`mary.w-abcdef01234567890.021345abcdef6789`, basato su un workflow (`w-abcdef01234567890`) che contiene una fase di copia.

```
{
    "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 il CloudWatch ruolo di registrazione

Per impostare l'accesso, crei una policy IAM basata sulle risorse e un ruolo IAM che fornisce tali informazioni di accesso.

Per abilitare Amazon CloudWatch Logging, devi iniziare creando una policy IAM che abiliti la CloudWatch registrazione. Quindi crei un ruolo IAM e alleghi la policy ad esso. Puoi farlo quando crei un server o modificando un server esistente. Per ulteriori informazioni su CloudWatch, consulta What is Amazon CloudWatch? e cosa sono i CloudWatch log di Amazon? nella Amazon CloudWatch User Guide.

Utilizza i seguenti esempi di policy IAM per consentire CloudWatch la registrazione.

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:Account AWS:log-group:/aws/transfer/
*"
        }
    ]
}
```

Nell'esempio precedente policy, for the**Resource**, sostituisci il *region-id* e *Account AWS*con i tuoi valori. Ad esempio, **"Resource": "arn:aws::logs:us-east-1:111122223333:log-group:/aws/transfer/*"**

Quindi crei un ruolo e CloudWatch alleghi la politica Logs che hai creato.

Per creare un ruolo IAM e collegare una policy

1. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.

   Nella pagina Crea ruolo, assicurati che sia selezionato AWS il servizio.
2. Scegliere Transfer (Trasferisci) dall'elenco di servizi, quindi selezionare Next: Permissions (Successivo: Autorizzazioni). Ciò stabilisce una relazione di fiducia tra AWS Transfer Family e il ruolo IAM. Inoltre, aggiungi `aws:SourceAccount` e `aws:SourceArn` condiziona le chiavi per proteggerti dal confuso problema del vice. Per ulteriori dettagli, consulta la seguente documentazione:

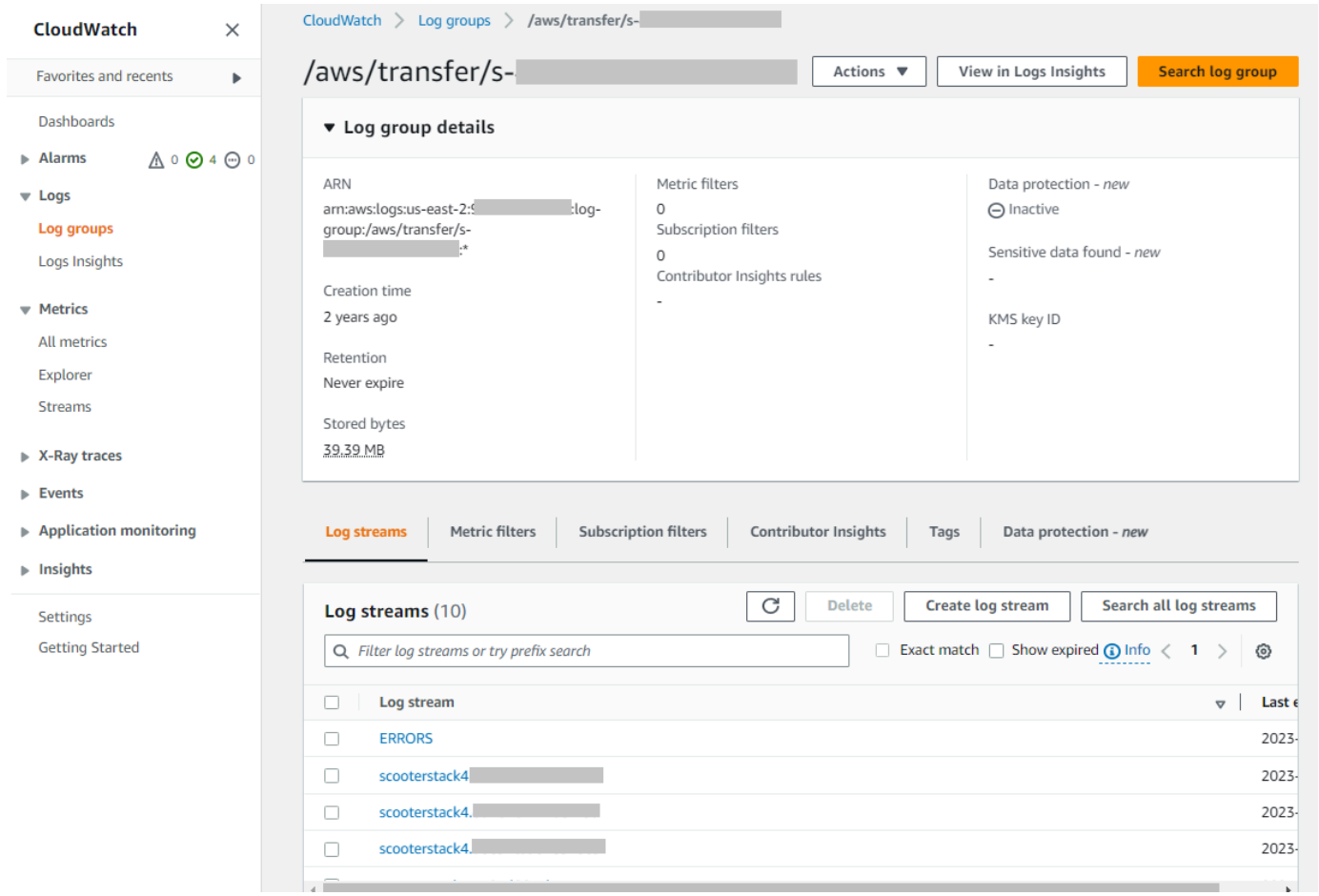
   - Procedura per stabilire un rapporto di fiducia con AWS Transfer Family: Per stabilire una relazione di trust
   - Descrizione del problema del deputato confuso: il problema del deputato confuso
3. Nella sezione Allega criteri di autorizzazione, individua e scegli la politica CloudWatch Logs che hai appena creato e scegli Avanti: Tag.
4. (Facoltativo) Immettere una chiave e un valore per un tag e scegliere Next: Review (Successivo: Rivedi).
5. Nella pagina Review (Rivedi), immettere un nome e una descrizione per il nuovo ruolo, quindi scegliere Create role (Crea ruolo).
6. Per visualizzare i log, scegli l'ID del server per aprire la pagina di configurazione del server e scegli Visualizza registri. Verrai reindirizzato alla CloudWatch console dove puoi vedere i tuoi flussi di log.

CloudWatch Nella pagina relativa al server, puoi visualizzare i record di autenticazione degli utenti (esito positivo e negativo), i caricamenti dei dati (`PUT`operazioni) e i download dei dati (`GET`operazioni).

Visualizzazione dei flussi di log di Transfer Family

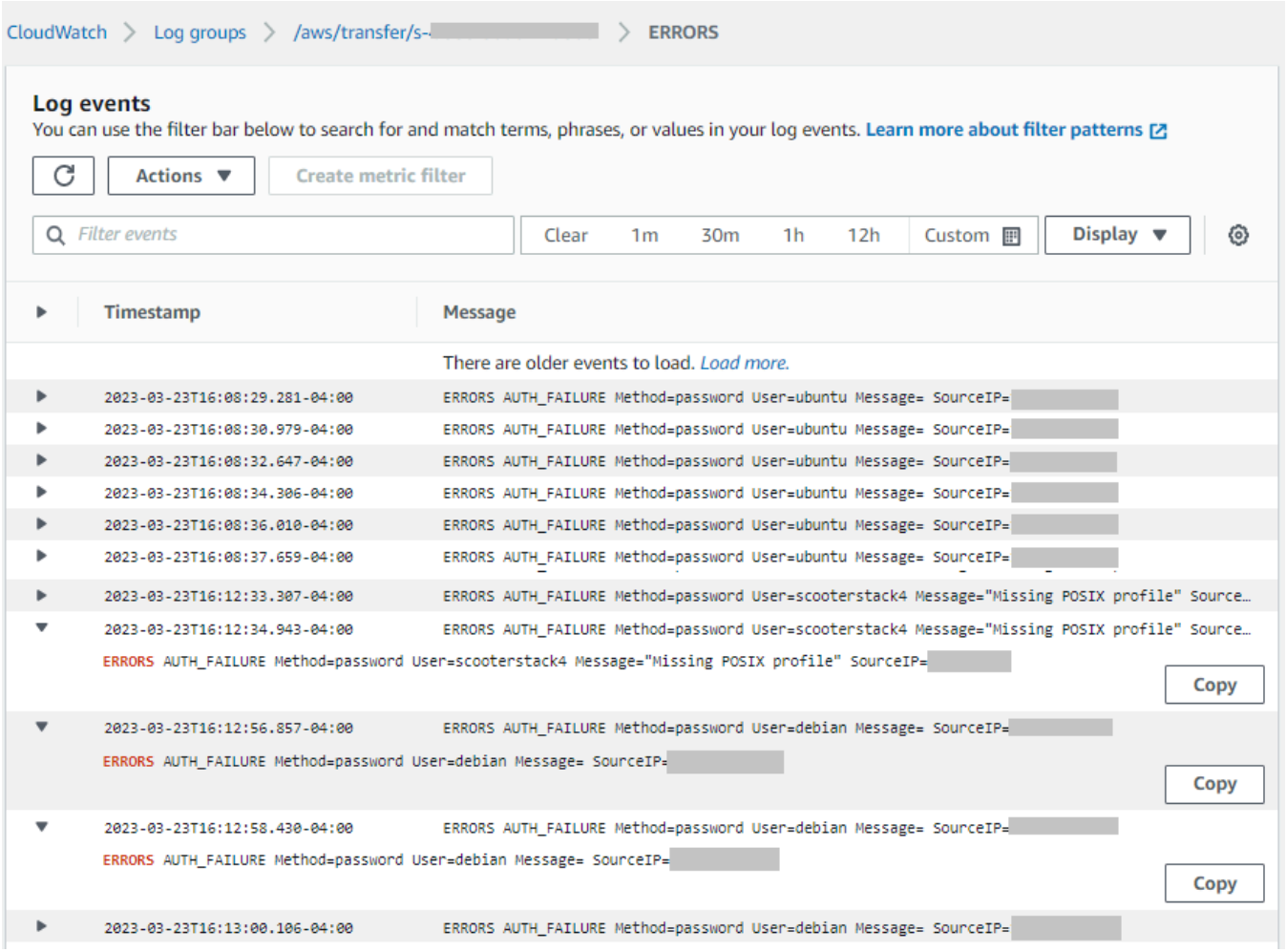
Per visualizzare i log del server Transfer Family

1. Vai alla pagina dei dettagli di un server.
2. Scegli Visualizza registri. Questo apre Amazon CloudWatch.
3. Viene visualizzato il gruppo di log per il server selezionato.

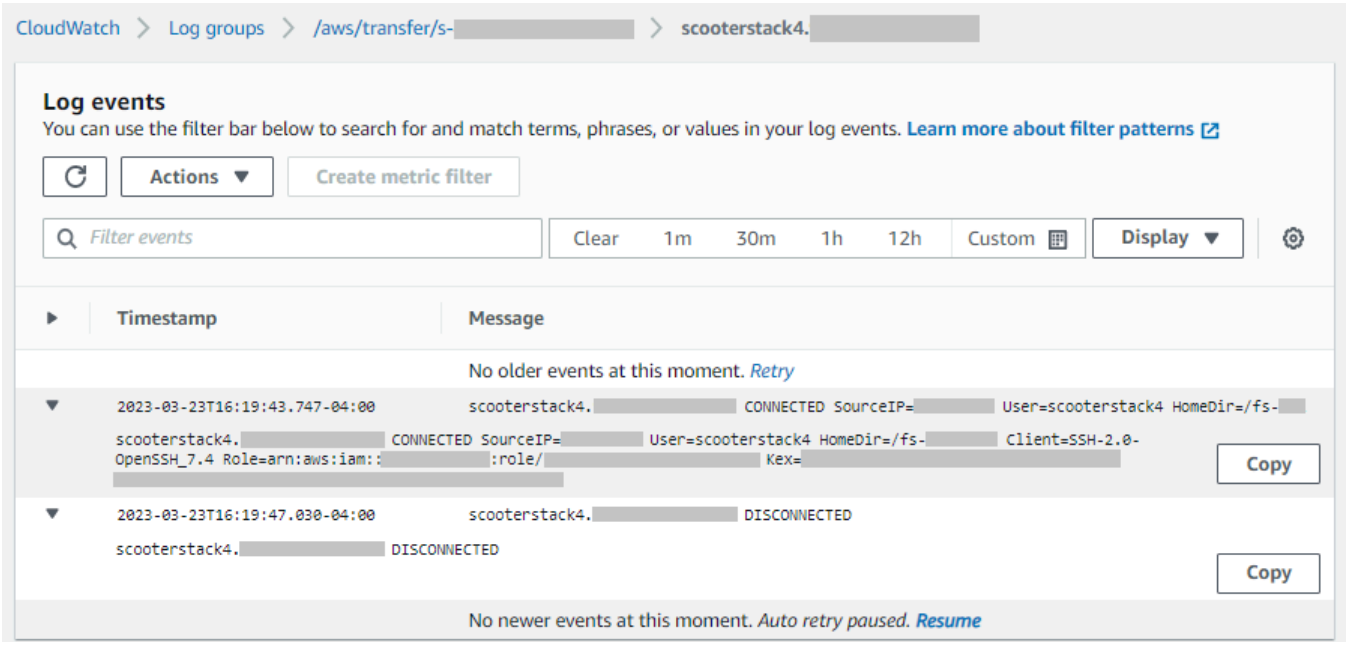


4. È possibile selezionare un flusso di log per visualizzare i dettagli e le singole voci relative allo stream.

   - Se è presente un elenco di ERRORI, puoi sceglierlo per visualizzare i dettagli degli errori più recenti relativi al server.

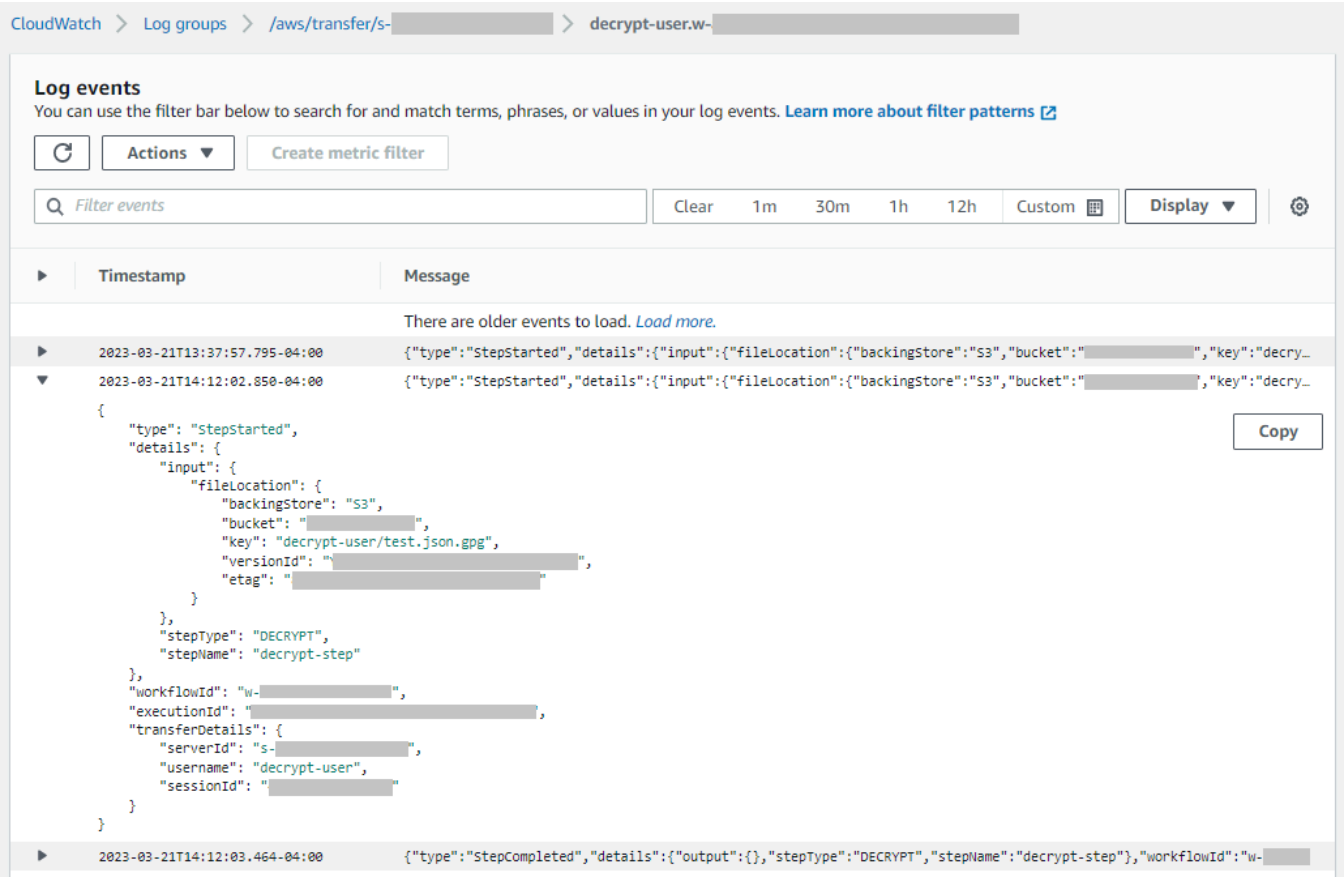


- Scegliete qualsiasi altra voce per vedere un esempio di flusso di log.



- Se al server è associato un flusso di lavoro gestito, è possibile visualizzare i registri relativi alle esecuzioni del flusso di lavoro.

> **Note**
>
> Il formato per il flusso di log per il flusso di lavoro è*username*.*workflowId*.*uniqueStreamSuffix*. Ad esempio, decrypt-user.w-a1111222233334444.aaaa1111bb2222 potrebbe essere il nome di un flusso di log per utente e flusso di lavoro. **`decrypt-user w-a1111222233334444`**



> **Note**
>
> Per qualsiasi voce di registro espansa, è possibile copiare la voce negli Appunti scegliendo Copia. Per maggiori dettagli sui CloudWatch log, consulta Visualizzazione dei dati di registro.

Creazione di CloudWatch allarmi Amazon

L'esempio seguente mostra come creare CloudWatch allarmi Amazon utilizzando la AWS Transfer Family metrica,. `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
```

Registrazione delle chiamate API di Amazon S3 nei log di accesso S3

Se utilizzi i log di accesso di Amazon S3 per identificare le richieste S3 effettuate per conto dei tuoi utenti di trasferimento file, viene utilizzato per mostrare quale ruolo IAM `RoleSessionName` è stato

assunto per gestire i trasferimenti di file. Visualizza anche informazioni aggiuntive come il nome utente, l'id di sessione e l'id del server utilizzati per i trasferimenti. Il formato è `[AWS:Role Unique Identifier]/username.sessionid@server-id` ed è contenuto nel campo Requester. Ad esempio, di seguito sono riportati i contenuti di un campo Requester di esempio da un log di accesso S3 per un file che è stato copiato nel bucket S3.

`arn:aws:sts::AWS-Account-ID:assumed-role/`*`IamRoleName`*`/username.sessionid@server-id`

Nel campo Requester riportato sopra, mostra il ruolo IAM chiamato. `IamRoleName` Per ulteriori informazioni sugli identificatori univoci dei ruoli IAM, consulta Identificatori univoci nella Guida per l'AWS Identity and Access Management utente.

Esempi per limitare il problema confuso dei deputati

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione tra servizi può portare al problema del vice confuso. Per ulteriori dettagli, consulta Prevenzione del problema "confused deputy" tra servizi.

> **Note**
>
> Negli esempi seguenti, sostituire ogni *`segnaposto dell'input utente`* con le proprie informazioni.
> In questi esempi, puoi rimuovere i dettagli ARN per un flusso di lavoro se al server non è collegato alcun flusso di lavoro.

Il seguente esempio di politica di registrazione/invocazione consente a qualsiasi server (e flusso di lavoro) dell'account di assumere il ruolo.

```
{
    "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/*"
                   ]
                }
            }
        }
    ]
}
```

Il seguente esempio di politica di registrazione/invocazione consente a un server (e a un flusso di lavoro) specifici di assumere il ruolo.

```
{
    "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 struttura di log per Transfer Family

Questo argomento descrive i campi che vengono compilati nei log Transfer Family: sia per le voci di registro strutturate JSON che per le voci di registro legacy.

Argomenti

Log strutturati JSON per Transfer Family

La tabella seguente contiene i dettagli per i campi di immissione del registro per le azioni SFTP/FTP/FTPS di Transfer Family, nel nuovo formato di registro strutturato JSON.

Campo	Descrizione	Esempio di inserimento
activity-type	The action by the user	APRI | CHIUDI | CHIUDI PARZIALMENTE | DISCONNESSO | CONNESSO
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 (available ciphers are listed in Algoritmi crittografici)	aes256-gcm@openssh.com
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	/user-home-bucket/test

Campo	Descrizione	Esempio di inserimento
	have a logical home directory, this value is always /	
kex	Specifies the negotiated SSH key exchange (KEX) for the connection (available KEX are listed in Algoritmi crittografici)	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
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

Campo	Descrizione	Esempio di inserimento
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

Log precedenti per Transfer Family

La tabella seguente contiene i dettagli delle voci di registro per varie azioni Transfer Family.

> **Note**
>
> Queste voci non sono nel nuovo formato di registro strutturato JSON.

La tabella seguente contiene i dettagli delle voci di registro per varie azioni Transfer Family, nel nuovo formato di registro strutturato JSON.

Azione	Log corrispondenti all'interno di Amazon CloudWatch Logs
Authentication failures (Errori di autenticazione)	ERRORI METODO AUTH_FAILURE =PublicKey user=LHR message="RSA SHA256:LFZ3R2NMLY4RAK+B7RB1RSVUIBAE+A+HXG0C7L1JIZ0" SourceIP=3.8.172.211
Flusso di lavoro COPIA/TAG/ELIMINA/DECRITTOGRAFA	{"type»:» StepStarted «, "details»: {"input»: {"fileLocation»: {"BackingStore» :"EFS», "fileSystemID» :"fs-12345678", "path»:» /lhr/regex.py «}}, "stepType» :"TAG», "stepName» :"successful_tag_step "}, "workflow ID» :"stepName» :"successful_tag_step "}, "workflowID» :"stepName» :"successful_tag_step» «w-1111aaaa2222bb3", "executio nID» :"81234abcd-1234-efgh-5678-ijklmnopq

Azione	Log corrispondenti all'interno di Amazon CloudWatch Logs
	r90", "transferDetails»: {"serverID» :"s-1234a bcd5678efghi», "username» :"lhr», "sessionI D» :"1234567890abcdef0"}}
Flusso di lavoro personalizzato in fasi	{"tipo»:» CustomStepInvoked «, "details»: {"output»: {"token» :"mzM4MJG5YWUTYT EzMy 00 YjIz LWI3OG MtYz U4OGI2 ZjQyMz E5"}, "stepType» :"CUSTOM», "stepName » :"efs-s3_copy_2"}, "workflowID» :"w-9283e 49d33297c3f7", "executionID» :"1234abc d-1234-efgh-5678-ijklmnopqr90", "transfer Details»: {"serverID» :"s-zz1111aaaa2222 3", "username» :"lhr», "sessionID» :"1234567 890abcdef0"}}
Eliminazioni	lhr.33a8fb495ffb383b ELIMINA PERCORSO=/ bucket/user/123.jpg
Download	lhr.33a8fb495ffb383b PERCORSO APERTO=/ bucket/user/123.jpg mode=Leggi llhr.33a8fb495ffb383b CHIUDI PERCORSO=/ bucket/user/123.jpg =3618546 BytesOut
Accessi/Logout	user.914984e553bcddb6 SORGENTE CONNESSA IP=1.22.111.222 utente=LHR =CLIENT LOGICO =SSH-2.0-OPENSSH_7.4 role=ARN:AWS: :iam: :123456789012:role/sftp-s3-access HomeDir user.914984e553bcddb6 DISCONNESSO
Rinomina	lhr.33a8fb495ffb383b RINOMINA PERCORSO=/bucket/user/lambo.png =/bucket/ user/ferrari.png NewPath

Azione	Log corrispondenti all'interno di Amazon CloudWatch Logs
Esempio di registro degli errori del workflow	{"type»:» StepErrored «, "details»: {"errorTy pe» :"BAD_REQUEST», "errorMes sage» :"Impossibile etichettare il file Efs», "stepType» :"TAG», "stepName» :"success ful_tag_step "}, "workflowID» :"w-1234a bcd5678efghi», "executionID» :"81234ab cd-1234-efgh-5678-ijklmnopqr90", "transfer Details»: {"serverID» :"s-1234abcd5678efghi», "username» :"lhr», "sessionId» :"1234567 890abcdef0"}}
Collegamenti simbolici	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK =/fs-12345678/lhr/pqr.jpg =abc.jpg LinkPath TargetPath
Caricamenti	lhr.33a8fb495ffb383b PERCORSO APERTO=/ bucket/user/123.jpg mode=create|truncate| scrivere lhr.33a8fb495ffb383b CHIUDI PERCORSO=/ bucket/user/123.jpg =3618546 BytesIn

Azione	Log corrispondenti all'interno di Amazon CloudWatch Logs
Flussi di lavoro	{"tipo»:» «, "details»: {"input»: {» Execution Started «: {" BackingStore» :"EFS», "fileSyst emID» :"fs-12345678", "path»:» /lhr/regex.py initialFileLocation «}}}, "workflowID» :"w-1111a aaa2222bbbb3", "executionID» :"1234abc d-123efgh-5678", "executionID» :"1234abc d-123efgh-5678" 8-ijklmnopqr90", "transfer Details»: {"serverID» :"s-zzzz1111aaaa22223", "username» :"lhr», "sessionID» :"1234567 890abcdef0"}} {"tipo»:» StepStarted «, "details»: {"input»: {"fileLocation»: {"BackingStore» :"EFS», "fileSystemID» :"fs-12345678", "path»:» / lhr/regex.py «}}, "stepType» :"CUSTOM» , "stepName» :"efs-s3_copy_2"}, "workflow .com» ID» :"w-9283e49d33297c3f7", "executio nID» :"1234abcd-1234-efgh-5678-ijklmnopqr 90", "transferDetails»: {"serverId» :"s-18ca4 9dce5d842e0b», "nome utente» :"lhr», "sessionID» :"12» 34567890abcdef0"}}

Esempi di voci di CloudWatch registro

Questo argomento presenta esempi di voci di registro.

Argomenti

- Esempio di voci del registro delle sessioni di trasferimento
- Esempi di voci di registro per i connettori SFTP
- Esempi di voci di registro relative agli errori dell'algoritmo di scambio di chiavi

Esempio di voci del registro delle sessioni di trasferimento

In questo esempio, un utente SFTP si connette a un server Transfer Family, carica un file, quindi si disconnette dalla sessione.

La seguente voce di registro riflette un utente SFTP che si connette a un server 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 seguente voce di registro indica l'utente SFTP che carica un file nel proprio bucket 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"
}
```

Le seguenti voci di registro indicano la disconnessione dell'utente SFTP dalla sessione SFTP. Innanzitutto, il client chiude la connessione al bucket, quindi disconnette la sessione 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"
}
```

Esempi di voci di registro per i connettori SFTP

Questa sezione contiene registri di esempio relativi a un trasferimento riuscito e a un trasferimento non riuscito. I log vengono generati in un gruppo di log denominato`/aws/transfer/`*`connector-id`*, dove *`connector-id`* è l'identificatore del connettore SFTP.

> **Note**
>
> Le voci di registro per i connettori SFTP vengono generate solo quando si esegue un comando. `StartFileTransfer`

Questa voce di registro si riferisce a un trasferimento completato con successo.

```
{
    "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
}
```

Questa voce di registro si riferisce a un trasferimento scaduto e che pertanto non è stato completato correttamente.

```
{
    "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"
}
```

Questa voce di registro è relativa a un'operazione SEND che ha esito positivo.

```
{
    "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
}
```

Descrizioni di alcuni campi chiave negli esempi di log precedenti.

- `timestamp`rappresenta quando viene aggiunto il registro a CloudWatch. `start-time`e `end-time` corrispondono a quando il connettore avvia e termina effettivamente un trasferimento.

- `transfer-id`è un identificatore univoco assegnato per ogni `start-file-transfer` richiesta. Se l'utente passa più percorsi di file in una singola chiamata `start-file-transfer` API, tutti i file condividono gli stessi `transfer-id` percorsi.
- `file-transfer-id`è un valore univoco generato per ogni file trasferito. Si noti che la parte iniziale di `file-transfer-id` è la stessa di`transfer-id`.

Esempi di voci di registro relative agli errori dell'algoritmo di scambio di chiavi

Questa sezione contiene log di esempio in cui l'algoritmo di scambio di chiavi (KEX) non è riuscito. Questi sono esempi tratti dal flusso di log ERRORS per i log strutturati.

Questa voce di registro è un esempio in cui si verifica un errore di tipo di chiave 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"
}
```

Questa voce di registro è un esempio di mancata corrispondenza con 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"
}
```

Utilizzo delle CloudWatch metriche per Transfer Family

> **Note**
>
> Puoi anche ottenere le metriche per Transfer Family direttamente dalla console Transfer Family stessa. Per maggiori dettagli, consulta Monitoraggio dell'utilizzo nella console .

Puoi ottenere informazioni sul tuo server utilizzando le CloudWatch metriche. Una metrica rappresenta un insieme di punti dati ordinati nel tempo su cui vengono pubblicati. CloudWatch Quando si utilizzano le metriche, è necessario specificare lo spazio dei nomi Transfer Family, il nome della metrica e la dimensione. Per ulteriori informazioni sui parametri, consulta Metrics nella Amazon CloudWatch User Guide.

La tabella seguente descrive le CloudWatch metriche per Transfer Family.

Spazio dei nomi	Parametro	Descrizione
`AWS/Transfer`	`BytesIn`	Il numero totale di byte trasferiti nel server. Unità: numero Periodo: 5 minuti
	`BytesOut`	Il numero totale di byte trasferiti dal server. Unità: numero Periodo: 5 minuti
	`FilesIn`	Il numero totale di file trasferiti nel server. Per i server che utilizzano il protocollo AS2, questa metrica rappresenta il numero di messaggi ricevuti. Unità: numero Periodo: 5 minuti
	`FilesOut`	Il numero totale di file trasferiti dal server.

Spazio dei nomi	Parametro	Descrizione
		Unità: numero Periodo: 5 minuti
	`InboundMessage`	Il numero totale di messaggi AS2 ricevuti con successo da un partner commerciale. Unità: numero Periodo: 5 minuti
	`InboundFailedMessage`	Il numero totale di messaggi AS2 ricevuti senza successo da un partner commerciale. Cioè, un partner commerciale ha inviato un messaggio, ma il server Transfer Family non è stato in grado di elaborarlo correttamente. Unità: numero Periodo: 5 minuti
	`OnUploadExecutionsStarted`	Il numero totale di esecuzioni del flusso di lavoro avviate sul server. Unità: numero Periodo: 1 minuto
	`OnUploadExecutionsSuccess`	Il numero totale di esecuzioni di workflow riuscite sul server. Unità: numero Periodo: 1 minuto

Spazio dei nomi	Parametro	Descrizione
	`OnUploadExecutionsFailed`	Il numero totale di esecuzioni di workflow non riuscite sul server. Unità: numero Periodo: 1 minuto

Dimensioni Transfer Family

Una dimensione è una coppia nome-valore che fa parte dell'identità di un parametro. Per ulteriori informazioni sulle dimensioni, consulta Dimensions nella Amazon CloudWatch User Guide.

La tabella seguente descrive la CloudWatch dimensione per Transfer Family.

Dimensione	Descrizione
`ServerId`	L'ID univoco del server.

Utilizzo Notifiche all'utente AWS con AWS Transfer Family

Per ricevere notifiche sugli AWS Transfer Family eventi, puoi Notifiche all'utente AWSimpostare vari canali di distribuzione. Quando un evento corrisponde a una regola specificata, ricevi una notifica.

È possibile ricevere notifiche per gli eventi tramite più canali, tra cui e-mail, notifiche chat AWS Chatbot o notifiche push AWS Console Mobile Application. Puoi anche visualizzare le notifiche nel Centro notifiche della console. Notifiche all'utente supporta l'aggregazione, che può ridurre il numero di notifiche ricevute durante eventi specifici.

Per ulteriori informazioni, consulta il post di blog Personalizzare le notifiche di recapito dei file utilizzando flussi di lavoro AWS Transfer Family gestiti e Cos'è? Notifiche all'utente AWS nella Guida per l'Notifiche all'utente AWS utente.

Utilizzo delle query per filtrare le voci di registro

È possibile utilizzare CloudWatch le query per filtrare e identificare le voci di registro per Transfer Family. Questa sezione contiene alcuni esempi.

1. Accedere AWS Management Console e aprire la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Puoi creare domande o regole.
   - Per creare una query di Logs Insights, scegli Logs Insights dal pannello di navigazione a sinistra, quindi inserisci i dettagli della tua query.
   - Per creare una regola Contributor Insights, scegli Insights > Contributor Insights dal pannello di navigazione a sinistra, quindi inserisci i dettagli della regola.
3. Esegui la query o la regola che hai creato.

Visualizza i principali contributori relativi agli errori di autenticazione

Nei log strutturati, una voce del log degli errori di autenticazione è simile alla seguente:

```
{
  "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"
}
```

Esegui la seguente query per visualizzare i principali fattori che contribuiscono agli errori di autenticazione.

```
filter @logStream = 'ERRORS'
| filter `activity-type` = 'AUTH_FAILURE'
| stats count() as AuthFailures by user, method
| sort by AuthFailures desc
| limit 10
```

Invece di utilizzare CloudWatch Logs Insights, puoi creare una regola di CloudWatch Contributors Insights per visualizzare gli errori di autenticazione. Crea una regola simile alla seguente.

```
{
    "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"
    ]
}
```

Visualizza le voci di registro in cui è stato aperto un file

Nei log strutturati, una voce del registro di lettura dei file è simile alla seguente:

```
{
  "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"
}
```

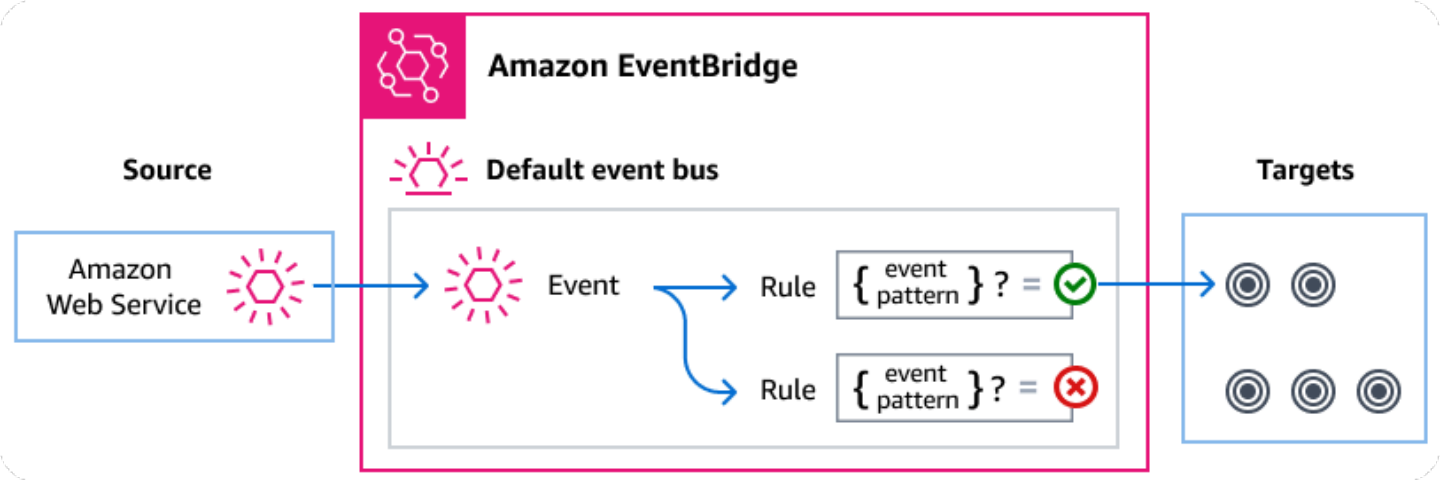
Esegui la seguente query per visualizzare le voci di registro che indicano che un file è stato aperto.

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

Gestione Transfer Family degli eventi tramite Amazon EventBridge

Amazon EventBridge è un servizio serverless che utilizza gli eventi per connettere tra loro i componenti dell'applicazione, il che può semplificare la creazione di applicazioni scalabili basate sugli eventi. L'architettura basata sugli eventi è uno stile di creazione di sistemi software liberamente accoppiati che interagiscono emettendo e rispondendo agli eventi. Gli eventi rappresentano un cambiamento in una risorsa o in un ambiente.

Come molti AWS servizi, Transfer Family genera e invia eventi al bus eventi EventBridge predefinito. Tieni presente che il bus degli eventi predefinito viene fornito automaticamente in ogni AWS account. Un router di eventi è un router che riceve eventi e li invia a nessuna o a più destinazioni o target. Si specificano le regole per il bus degli eventi che valuta gli eventi man mano che arrivano. Ogni regola verifica se un evento corrisponde al modello di eventi della regola. Se l'evento corrisponde, il bus degli eventi invia l'evento a uno o più obiettivi specificati.



Argomenti

- Transfer Family eventi
- Invio di Transfer Family eventi tramite regole EventBridge
- Amazon EventBridge autorizzazioni
- EventBridge Risorse aggiuntive
- Transfer Family riferimento ai dettagli degli eventi

Transfer Family eventi

Transfer Family invia automaticamente gli eventi al bus EventBridge eventi predefinito. È possibile creare regole sul bus degli eventi in cui ogni regola include un modello di eventi e uno o più obiettivi. Gli eventi che corrispondono allo schema di eventi di una regola vengono consegnati agli obiettivi specificati con il massimo impegno, tuttavia alcuni eventi potrebbero essere consegnati in modo errato.

I seguenti eventi sono generati da Transfer Family. Per ulteriori informazioni, consulta EventBridge gli eventi nella Guida Amazon EventBridge per l'utente.

Eventi dei server SFTP, FTPS e FTP

Tipo di dettaglio dell'evento	Descrizione
Download del file server FTP completato	Un file è stato scaricato correttamente per il protocollo FTP.
Scaricamento del file server FTP non riuscito	Un tentativo di scaricare un file non è riuscito per il protocollo FTP.
Caricamento del file server FTP completato	Un file è stato caricato correttamente per il protocollo FTP.
Caricamento del file server FTP non riuscito	Un tentativo di caricamento di un file non è riuscito per il protocollo FTP.
Download del file server FTPS completato	Un file è stato scaricato correttamente per il protocollo FTPS.
Scaricamento del file server FTPS non riuscito	Un tentativo di scaricare un file non è riuscito per il protocollo FTPS.
Caricamento del file server FTPS completato	Un file è stato caricato correttamente per il protocollo FTPS.
Caricamento del file server FTPS non riuscito	Un tentativo di caricamento di un file non è riuscito per il protocollo FTPS.

Tipo di dettaglio dell'evento	Descrizione
Download del file dal server SFTP completato	Un file è stato scaricato correttamente per il protocollo SFTP.
Scaricamento del file dal server SFTP non riuscito	Un tentativo di scaricare un file non è riuscito per il protocollo SFTP.
Caricamento del file sul server SFTP completato	Un file è stato caricato correttamente per il protocollo SFTP.
Caricamento del file sul server SFTP non riuscito	Un tentativo di caricamento di un file non è riuscito per il protocollo SFTP.

Eventi del connettore SFTP

Tipo di dettaglio dell'evento	Descrizione
Invio del file del connettore SFTP completato	Il trasferimento di file da un connettore a un server SFTP remoto è stato completato correttamente.
Invio del file del connettore SFTP non riuscito	Un trasferimento di file da un connettore a un server SFTP remoto non è riuscito.
Recupero dei file del connettore SFTP completato	Il trasferimento di file da un server SFTP remoto a un connettore è stato completato correttamente.
Recupero del file del connettore SFTP non riuscito	Un trasferimento di file da un server SFTP remoto a un connettore non è riuscito.
Elenco delle directory dei connettori SFTP completato	Una chiamata di avvio dell'elenco delle directory dei file completata con successo.
Elenco delle directory dei connettori SFTP non riuscito	Un elenco di directory di file di avvio non riuscito.

Eventi A2S

Tipo di dettaglio dell'evento	Descrizione
Ricezione del payload AS2 completata	Il payload per un messaggio AS2 è stato ricevuto.
Ricezione del payload AS2 non riuscita	Il payload per un messaggio AS2 non è stato ricevuto.
Invio del payload AS2 completato	Il payload per un messaggio AS2 è stato inviato correttamente.
Invio del payload AS2 non riuscito	Il payload per un messaggio AS2 non è stato inviato.
Ricezione MDN AS2 completata	La notifica di disposizione del messaggio per un messaggio AS2 è stata ricevuta.
Ricezione MDN AS2 non riuscita	La notifica di disposizione del messaggio per un messaggio AS2 non è stata ricevuta.
Invio MDN AS2 completato	La notifica di disposizione del messaggio per un messaggio AS2 è stata inviata correttamente.
Invio MDN AS2 non riuscito	La notifica di disposizione del messaggio per un messaggio AS2 non è stata inviata.

Invio di Transfer Family eventi tramite regole EventBridge

Se si desidera che il bus degli eventi EventBridge predefinito invii Transfer Family eventi a una destinazione, è necessario creare una regola che contenga uno schema di eventi che corrisponda ai dati degli Transfer Family eventi desiderati.

È possibile creare una regola seguendo questi passaggi generali:

1. Crea un modello di evento per la regola che specifica quanto segue:
   - Transfer Family è l'origine degli eventi valutati dalla regola.

- (Facoltativo) Qualsiasi altro dato relativo all'evento con cui confrontarlo.

Per ulteriori informazioni, consulta ???.

2. (Facoltativo) Crea un trasformatore di input che personalizzi i dati dell'evento prima di EventBridge inviare le informazioni alla destinazione della regola.

   Per ulteriori informazioni, consulta Input transformation nella Guida per l'EventBridge utente.

3. Specificate gli obiettivi a cui desiderate EventBridge fornire eventi che corrispondano allo schema degli eventi.

   Le destinazioni possono essere altri AWS servizi, applicazioni SaaS (Software as a Service), destinazioni API o altri endpoint personalizzati. Per ulteriori informazioni, consulta la sezione Destinazioni nella Guida per l'utente di EventBridge .

Per istruzioni complete sulla creazione di regole per i bus degli eventi, consulta Creazione di regole che reagiscono agli eventi nella Guida per l'EventBridge utente.

Creazione di modelli di Transfer Family eventi per eventi

Quando Transfer Family invia un evento al bus di eventi predefinito, EventBridge utilizza il modello di eventi definito per ogni regola per determinare se l'evento deve essere distribuito agli obiettivi della regola. Un modello di eventi corrisponde ai dati negli Transfer Family eventi desiderati. Ogni modello di evento è un oggetto JSON che contiene quanto segue:

- Un attributo `source` che identifica il servizio che invia l'evento. Per Transfer Family gli eventi, la fonte è`aws.transfer`.
- (Facoltativo) Un `detail-type` attributo che contiene una matrice dei tipi di eventi da abbinare.
- (Facoltativo) Un `detail` attributo contenente qualsiasi altro dato relativo all'evento su cui effettuare la corrispondenza.

Ad esempio, il seguente schema di eventi corrisponde a tutti gli eventi di Transfer Family:

```
{
  "source": ["aws.transfer"]
}
```

Il seguente esempio di pattern di eventi corrisponde a tutti gli eventi del connettore 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"]
}
```

Il seguente esempio di pattern di eventi corrisponde a tutti gli eventi non riusciti di Transfer Family:

```
{
  "source": ["aws.transfer"],
  "detail-type": [{"wildcard", "*Failed"}]
}
```

Il seguente esempio di pattern di eventi corrisponde ai download SFTP riusciti per il *nome utente dell'utente*:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Server File Download Completed"],
  "detail": {
    "username": [username]
  }
}
```

Per ulteriori informazioni sulla scrittura di modelli di eventi, consultate Event pattern nella Guida per l'EventBridge utente.

Test dei modelli di Transfer Family eventi per gli eventi in EventBridge

È possibile utilizzare EventBridge Sandbox per definire e testare rapidamente un modello di evento, senza dover completare il processo più ampio di creazione o modifica di una regola. Utilizzando la Sandbox, è possibile definire un pattern di eventi e utilizzare un evento di esempio per confermare che il pattern corrisponda agli eventi desiderati. EventBridge offre la possibilità di creare una nuova regola utilizzando quel pattern di eventi direttamente dalla sandbox.

Per ulteriori informazioni, consulta Testare un pattern di eventi utilizzando la EventBridge sandbox nella Guida per l'EventBridge utente.

Amazon EventBridge autorizzazioni

Transfer Family non richiede autorizzazioni aggiuntive per l'invio di eventi. Amazon EventBridge

Le destinazioni specificate potrebbero richiedere autorizzazioni o configurazioni specifiche. Per maggiori dettagli sull'utilizzo di servizi specifici per le destinazioni, consulta Amazon EventBridge gli obiettivi nella Guida per l'Amazon EventBridge utente.

EventBridge Risorse aggiuntive

Fate riferimento ai seguenti argomenti della Guida per Amazon EventBridge l'utente per ulteriori informazioni su come utilizzare EventBridge per elaborare e gestire gli eventi.

- Per informazioni dettagliate sul funzionamento degli event bus, consulta Amazon EventBridge Event Bus.
- Per informazioni sulla struttura degli eventi, consulta Eventi.
- Per informazioni sulla creazione di modelli di eventi EventBridge da utilizzare per abbinare gli eventi alle regole, consulta Modelli di eventi.
- Per informazioni sulla creazione di regole per specificare quali eventi vengono EventBridge elaborati, consulta Regole.
- Per informazioni su come specificare i servizi o le altre destinazioni a cui EventBridge inviare gli eventi corrispondenti, consulta Target.

Transfer Family riferimento ai dettagli degli eventi

Tutti gli eventi dei AWS servizi hanno un set comune di campi contenenti metadati sull'evento. Questi metadati possono includere il AWS servizio che è l'origine dell'evento, l'ora in cui l'evento è stato generato, l'account e la regione in cui si è verificato l'evento e altri. Per le definizioni di questi campi generali, consultate il riferimento alla struttura degli eventi nella Guida per l'Amazon EventBridge utente.

Inoltre, ogni evento ha un campo `detail` che contiene dati specifici per quel particolare evento. Il riferimento seguente definisce i campi di dettaglio per i vari Transfer Family eventi.

Quando utilizzate EventBridge per selezionare e gestire Transfer Family gli eventi, tenete presente quanto segue:

- Il `source` campo per tutti gli eventi da Transfer Family è impostato su`aws.transfer`.
- Il campo `detail-type` specifica il tipo di evento.

  Ad esempio, `FTP File Server Download Completed`.
- Il campo `detail` contiene i dati specifici di quel particolare evento.

Per informazioni sulla creazione di modelli di eventi che consentono alle regole di abbinare Transfer Family gli eventi, consulta Modelli di eventi nella Guida per l'Amazon EventBridge utente.

Per ulteriori informazioni sugli eventi e su come li EventBridge elabora, consulta Amazon EventBridge gli eventi nella Guida per l'Amazon EventBridge utente.

Argomenti

- Eventi dei server SFTP, FTPS e FTP
- Eventi del connettore SFTP
- Eventi AS2

Eventi dei server SFTP, FTPS e FTP

Di seguito sono riportati i campi di dettaglio per gli eventi dei server SFTP, FTPS e FTP:

- Download del file server FTP completato
- Scaricamento del file server FTP non riuscito
- Caricamento del file server FTP completato
- Caricamento del file server FTP non riuscito
- Download del file server FTPS completato
- Scaricamento del file server FTPS non riuscito
- Caricamento del file server FTPS completato
- Caricamento del file server FTPS non riuscito
- Scaricamento del file dal server SFTP completato
- Scaricamento del file dal server SFTP non riuscito
- Caricamento del file dal server SFTP completato
- Caricamento del file sul server SFTP non riuscito

I `detail-type` campi `source` e sono inclusi di seguito perché contengono valori specifici per Transfer Family gli eventi. Per le definizioni degli altri campi di metadati inclusi in tutti gli eventi, consulta il riferimento alla struttura degli eventi nella Guida per l'Amazon EventBridge utente.

```
{
  . . .,
  "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 il tipo di evento.

Per questo evento, il valore è uno dei nomi di evento del server SFTP, FTPS o FTP elencati in precedenza.

`source`

Identifica il servizio che ha generato l'evento. Per gli eventi Transfer Family, questo valore è`aws.transfer`.

`detail`

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per questo evento, i dati includono quanto segue:

`failure-code`

Categoria relativa al motivo per cui il trasferimento non è riuscito. Valori: `PARTIAL_UPLOAD | PARTIAL_DOWNLOAD | UNKNOWN_ERROR`

`status-code`

Se il trasferimento è andato a buon fine. Valori:`COMPLETED | FAILED`.

`protocol`

Il protocollo utilizzato per il trasferimento. Valori: `SFTP | FTPS | FTP`

`bytes`

Il numero di byte trasferiti.

`client-ip`

L'indirizzo IP del client coinvolto nel trasferimento

`failure-message`

Per i trasferimenti non riusciti, i dettagli del motivo per cui il trasferimento non è riuscito.

`end-timestamp`

Per i trasferimenti riusciti, il timestamp del termine dell'elaborazione del file.

`etag`

Il tag di entità (utilizzato solo per i file Amazon S3).

`file-path`

Il percorso del file da trasferire.

`server-id`

L'ID univoco per il server Transfer Family.

`username`

L'utente che sta eseguendo il trasferimento.

`session-id`

L'identificatore univoco per la sessione di trasferimento.

`start-timestamp`

Per trasferimenti riusciti, il timestamp di inizio dell'elaborazione dei file.

Example Esempio di evento SFTP Server File Download Failed

L'esempio seguente mostra un evento in cui un download non è riuscito su un server SFTP (Amazon EFS è lo storage utilizzato).


```
{
    "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 Esempio di evento FTP File Server Upload Completed

L'esempio seguente mostra un evento in cui un caricamento è stato completato correttamente su un server FTP (Amazon S3 è lo storage utilizzato).


```
{
    "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"
    }
}
```

Eventi del connettore SFTP

Di seguito sono riportati i campi di dettaglio per gli eventi del connettore SFTP:

- Invio del file del connettore SFTP completato
- Invio del file del connettore SFTP non riuscito
- Recupero del file del connettore SFTP completato
- Recupero del file del connettore SFTP non riuscito
- Elenco delle directory dei connettori SFTP completato
- Elenco delle directory dei connettori SFTP non riuscito

I `detail-type` campi `source` e sono inclusi di seguito perché contengono valori specifici per Transfer Family gli eventi. Per le definizioni degli altri campi di metadati inclusi in tutti gli eventi, consulta il riferimento alla struttura degli eventi nella Guida per l'Amazon EventBridge utente.

```
{
  . . .,
  "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 il tipo di evento.

Per questo evento, il valore è uno dei nomi di eventi del connettore SFTP elencati in precedenza.

`source`

Identifica il servizio che ha generato l'evento. Per Transfer Family gli eventi, questo valore è`aws.transfer`.

`detail`

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

Per questo evento, i dati includono quanto segue:

`max-items`

Il numero massimo di nomi di directory/file da restituire.

`operation`

Se la `StartFileTransfer` richiesta consiste nell'invio o nel recupero di un file. Valori:. `SEND|RETRIEVE`

`connector-id`

L'identificatore univoco per il connettore SFTP utilizzato.

`output-directory-path`

Il percorso (bucket e prefisso) in Amazon S3 per memorizzare i risultati dell'elenco di file/directory.

`listing-id`

Un identificatore univoco per la chiamata API. `StartDirectoryListing` Questo identificatore può essere usato per controllare CloudWatch i log e vedere lo stato della richiesta di inserzione.

`transfer-id`

L'identificatore univoco per l'evento di trasferimento (una `StartFileTransfer` richiesta).

`file-transfer-id`

L'identificatore univoco del file da trasferire.

`url`

L'URL dell'endpoint AS2 o SFTP del partner.

`file-path`

La posizione e il file che vengono inviati o recuperati.

`status-code`

Se il trasferimento ha esito positivo. Valori:`FAILED | COMPLETED`.

`failure-code`

Per i trasferimenti non riusciti, il codice del motivo per cui il trasferimento non è riuscito.

`failure-message`

Per i trasferimenti non riusciti, i dettagli del motivo per cui il trasferimento non è riuscito.

`start-timestamp`

Per trasferimenti riusciti, il timestamp di inizio dell'elaborazione dei file.

`end-timestamp`

Per trasferimenti riusciti, il timestamp del completamento dell'elaborazione del file.

`local-directory-path`

Per `RETRIEVE` le richieste, la posizione in cui inserire il file recuperato.

`remote-directory-path`

Per `SEND` le richieste, la directory dei file in cui inserire il file sul server SFTP del partner. Questo è il valore `RemoteDirectoryPath` che l'utente ha passato alla `StartFileTransfer` richiesta. È possibile specificare una directory predefinita sul server SFTP del partner. In tal caso, questo campo è vuoto.

`item-count`

Il numero di elementi (directory e file) restituiti per la richiesta di inserzione.

`truncated`

Se l'output dell'elenco contiene o meno tutti gli elementi contenuti nella directory remota.

`bytes`

Il numero di byte trasferiti. Il valore è 0 per i trasferimenti non riusciti.

`local-file-location`

Questo parametro contiene i dettagli della posizione del file di AWS archiviazione.

`domain`

Lo spazio di archiviazione utilizzato. Attualmente, l'unico valore è`S3`.

`bucket`

Il contenitore per l'oggetto in Amazon S3.

`key`

Il nome assegnato all'oggetto in Amazon S3.

`output-file-location`

Questo parametro contiene i dettagli della posizione in cui archiviare i risultati dell'elenco delle directory in AWS archiviazione.

`domain`

Lo spazio di archiviazione utilizzato. Attualmente, l'unico valore è`S3`.

`bucket`

Il contenitore per l'oggetto in Amazon S3.

`key`

Il nome assegnato all'oggetto in Amazon S3.

Example Esempio di evento SFTP Connector File Send Failed

L'esempio seguente mostra un evento in cui un connettore SFTP si è guastato durante il tentativo di inviare un file a un server 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 Evento di esempio SFTP Connector File Retrieve Completed

L'esempio seguente mostra un evento in cui un connettore SFTP ha recuperato con successo un file inviato da un server 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 Evento di esempio SFTP Connector Directory Listing Completed

L'esempio seguente mostra un evento in cui una chiamata Start Directory Listing ha recuperato un file di elenco da un server 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"
        }
    }
}
```

Eventi AS2

Di seguito sono riportati i campi di dettaglio per gli eventi AS2:

- Ricezione del payload AS2 completata
- Ricezione del payload AS2 non riuscita
- Invio del payload AS2 completato
- Invio del payload AS2 non riuscito
- Ricezione MDN AS2 completata
- Ricezione MDN AS2 non riuscita
- Invio MDN AS2 completato
- Invio MDN AS2 non riuscito

I `detail-type` campi `source` e sono inclusi di seguito perché contengono valori specifici per gli Transfer Family eventi. Per le definizioni degli altri campi di metadati inclusi in tutti gli eventi, consulta il riferimento alla struttura degli eventi nella Guida per l'Amazon EventBridge utente.

```
{
   . . .,
  "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 il tipo di evento.

Per questo evento, il valore è uno degli eventi AS2 elencati in precedenza.

`source`

Identifica il servizio che ha generato l'evento. Per Transfer Family gli eventi, questo valore è`aws.transfer`.

`detail`

Un oggetto JSON contenente informazioni sull'evento. Il servizio che genera l'evento determina il contenuto di questo campo.

`s3-attributes`

Identifica il bucket e la chiave Amazon S3 per il file da trasferire. Per gli eventi MDN, identifica anche il bucket e la chiave per il file MDN.

`file-bucket`

Il contenitore per l'oggetto in Amazon S3.

`file-key`

Il nome assegnato all'oggetto in Amazon S3.

`json-bucket`

Per i trasferimenti COMPLETATI o NON RIUSCITI, il contenitore per il file JSON.

`json-key`

Per i trasferimenti COMPLETATI o NON RIUSCITI, il nome assegnato al file JSON in Amazon S3.

`mdn-bucket`

Per gli eventi MDN, il contenitore per il file MDN.

`mdn-key`

Per gli eventi MDN, il nome assegnato al file MDN in Amazon S3.

`mdn-subject`

Per gli eventi MDN, una descrizione testuale della disposizione dei messaggi.

`mdn-message-id`

Per gli eventi MDN, un ID univoco per il messaggio MDN.

`disposition`

Per gli eventi MDN, la categoria per la disposizione.

`bytes`

Il numero di byte nel messaggio.

`as2-from`

Il partner commerciale AS2 che invia il messaggio.

`as2-message-id`

Un identificatore univoco per il messaggio AS2 che viene trasferito.

`as2-to`

Il partner commerciale AS2 che riceve il messaggio.

`connector-id`

Per i messaggi AS2 inviati da un server Transfer Family a un partner commerciale, viene utilizzato l'identificatore univoco del connettore AS2.

`client-ip`

Per gli eventi del server (trasferimenti da un partner commerciale a un server Transfer Family), l'indirizzo IP del client coinvolto nel trasferimento.

`agreement-id`

Per gli eventi del server, l'identificatore univoco per l'accordo AS2.

`server-id`

Per gli eventi del server, un ID univoco solo per il server Transfer Family.

`requester-file-name`

Per gli eventi di payload, il nome originale del file ricevuto durante il trasferimento.

`message-subject`

Una descrizione testuale dell'oggetto del messaggio.

`start-timestamp`

Per trasferimenti riusciti, il timestamp di inizio dell'elaborazione dei file.

`end-timestamp`

Per trasferimenti riusciti, il timestamp del completamento dell'elaborazione del file.

`status-code`

Il codice che corrisponde allo stato del processo di trasferimento dei messaggi AS2. Valori validi: `COMPLETED | FAILED | PROCESSING`.

`failure-code`

Per i trasferimenti non riusciti, la categoria relativa al motivo per cui il trasferimento non è riuscito.

`failure-message`

Per i trasferimenti non riusciti, i dettagli del motivo per cui il trasferimento non è riuscito.

`transfer-id`

L'identificatore univoco dell'evento di trasferimento.

Example Evento di esempio 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 Esempio di 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"
  }
}
```

Sicurezza in AWS Transfer Family

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Ambito per programma di conformitàServizi AWS di conformità e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of

Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).

- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Transfer Family. Negli argomenti seguenti viene illustrato come eseguire la configurazione AWS Transfer Family per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS Transfer Family le tue risorse.

Offriamo un workshop che fornisce indicazioni prescrittive e un laboratorio pratico su come creare un'architettura di trasferimento dei file scalabile e sicura AWS senza dover modificare le applicazioni esistenti o gestire l'infrastruttura server. Puoi visualizzare i dettagli di questo workshop qui.

Argomenti

- Sicurezza dell'infrastruttura in AWS Transfer Family
- Aggiungi un firewall per applicazioni Web
- Prevenzione del problema "confused deputy" tra servizi
- AWS politiche gestite per AWS Transfer Family

Politiche di sicurezza per AWS Transfer Family i server

Le politiche di sicurezza del server AWS Transfer Family consentono di limitare l'insieme di algoritmi crittografici (codici di autenticazione dei messaggi (MAC), scambi di chiavi (KEX) e suite di crittografia) associati al server. Per un elenco degli algoritmi crittografici supportati, vedere. Algoritmi crittografici Per un elenco degli algoritmi a chiave supportati da utilizzare con le chiavi dell'host del server e le chiavi utente gestite dal servizio, vedere. Algoritmi supportati per chiavi utente e server

> **Note**
>
> Consigliamo vivamente di aggiornare i server alla nostra politica di sicurezza più recente. La nostra politica di sicurezza più recente è quella predefinita. A qualsiasi cliente che crea un server Transfer Family utilizzando CloudFormation e accetta la politica di sicurezza predefinita verrà assegnata automaticamente la politica più recente. Se sei preoccupato per la compatibilità dei client, indica affermativamente quale politica di sicurezza desideri utilizzare durante la creazione o l'aggiornamento di un server anziché utilizzare la politica predefinita, che è soggetta a modifiche.
> Per modificare la politica di sicurezza di un server, consulta. Modifica la politica di sicurezza

Per ulteriori informazioni sulla sicurezza in Transfer Family, consulta il post del blog, Come Transfer Family può aiutarti a costruire una soluzione di trasferimento di file gestita sicura e conforme.

Argomenti

- Algoritmi crittografici
- TransferSecurityPolitica - 2024-01
- TransferSecurityPolitica - 2023-05
- TransferSecurityPolitica - 2022-03
- TransferSecurityPolitica-2020-06
- TransferSecurityPolitica - 2018-11

- TransferSecurityPolicy-FIPS-2024-01/ Policy-FIPS-2024-05 TransferSecurity
- TransferSecurityPolitica-FIPS-2023-05
- TransferSecurityPolitica-FIPS-2020-06
- Politiche di sicurezza post-quantistiche

> **Note**
>
> `TransferSecurityPolicy-2024-01`è la politica di sicurezza predefinita allegata al server quando si crea un server utilizzando la console, l'API o la CLI.

Algoritmi crittografici

Per le chiavi host, supportiamo i seguenti algoritmi:

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`
- `ssh-ed25519`

Inoltre, le seguenti politiche di sicurezza consentono`ssh-rsa`:

- TransferSecurityPolitica-2018-11
- TransferSecurityPolitica-2020-06
- TransferSecurityPolitica-FIPS-2020-06
- TransferSecurityPolitica - FIPS-2023-05
- TransferSecurityPolitica-FIPS-2024-01
- TransferSecurityPolitica-PQ-SSH-FIPS-Sperimentale-2023-04

> **Note**
>
> È importante comprendere la distinzione tra il tipo di chiave RSA, che è sempre, e l'algoritmo della chiave host RSA, che può essere uno qualsiasi degli algoritmi supportati. `ssh-rsa`

Di seguito è riportato un elenco di algoritmi crittografici supportati per ogni policy di sicurezza.

> **Note**
>
> Nella tabella e nelle politiche seguenti, si noti il seguente utilizzo dei tipi di algoritmo.
>
> - I server SFTP utilizzano solo algoritmi nelle sezioni SshCiphersSshKexs, e SshMacs.
> - I server FTPS utilizzano solo gli algoritmi presenti nella sezione. TlsCiphers
> - I server FTP, poiché non utilizzano la crittografia, non utilizzano nessuno di questi algoritmi.
> - Le politiche di sicurezza FIPS-2024-05 e FIPS-2024-01 sono identiche, tranne per il fatto che FIPS-2024-05 non supporta l'algoritmo. `ssh-rsa`

Policy di sicurezza	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-gcm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦
aes192-ctr	♦	♦	♦	♦	♦	♦	♦	♦

Policy di sicurezza	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
aes256-ctr	♦	♦	♦	♦	♦	♦	♦	♦
aes256-gcm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦
chacha20-poly1305@openssh.com				♦				♦
SshKexs								
curva25519-sha256	♦	♦	♦					♦
curve25519-sha256@libssh.org	♦	♦	♦					♦
diffie-hellman-group14-sha1								♦

Policy di sicurezza	2024-01	2023-05	2022-03	2020-06	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
diffie-hellman-group-ppo14-sha256				♦			♦	♦
diffie-hellman-group-ppo16-sha512	♦	♦	♦	♦	♦	♦	♦	♦
diffie-hellman-group-ppo18-sha512	♦	♦	♦	♦	♦	♦	♦	♦
diffie-hellman-group-exchange-sha256		♦	♦	♦		♦	♦	♦

Policy di sicurezza	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	♦				♦			

Policy di sicurezza	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	♦							

Policy di sicurezza	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	♦	♦	♦	♦	♦	♦	♦	♦

Policy di sicurezza	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	♦	♦	♦	♦	♦	♦	♦	♦

Policy di sicurezza	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	♦	♦	♦	♦	♦	♦	♦	♦

Policy di sicurezza	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								♦

TransferSecurityPolitica - 2024-01

Di seguito viene illustrata la politica di sicurezza -2024-01 TransferSecurityPolicy.

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

TransferSecurityPolitica - 2023-05

Di seguito viene illustrata la politica di sicurezza 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"
        ]
    }
}
```

TransferSecurityPolitica - 2022-03

Di seguito viene illustrata la politica di sicurezza -2022-03 TransferSecurityPolicy.

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

TransferSecurityPolitica-2020-06

Di seguito viene illustrata la politica di sicurezza -2020-06 TransferSecurityPolicy.

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

TransferSecurityPolitica - 2018-11

Di seguito viene illustrata la politica di sicurezza 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"
    ]
  }
}
```

TransferSecurityPolicy-FIPS-2024-01/ Policy-FIPS-2024-05 TransferSecurity

Di seguito vengono illustrate le politiche di sicurezza -FIPS-2024-01 e -FIPS-2024-05. TransferSecurityPolicy TransferSecurityPolicy

> **Note**
>
> L'endpoint del servizio FIPS e le politiche di sicurezza -FIPS-2024-01 e -FIPS-2024-05 sono disponibili solo in alcune regioni. TransferSecurityPolicy TransferSecurityPolicy AWS Per ulteriori informazioni, consulta Endpoint e quote AWS Transfer Family nella Riferimenti generali di AWS.
>
> L'unica differenza tra queste due politiche di sicurezza è che -FIPS-2024-01 supporta l'algoritmo e -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"
        ]
    }
}
```

TransferSecurityPolitica-FIPS-2023-05

I dettagli della certificazione FIPS per sono disponibili all'indirizzo AWS Transfer Family https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all

Di seguito viene illustrata la politica di sicurezza TransferSecurityPolicy -FIPS-2023-05.

> **Note**
>
> L'endpoint del servizio FIPS e la politica di sicurezza TransferSecurityPolicy -FIPS-2023-05 sono disponibili solo in alcune regioni. AWS Per ulteriori informazioni, consulta Endpoint e quote AWS Transfer Family nella Riferimenti generali di 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"
        ]
    }
}
```

TransferSecurityPolitica-FIPS-2020-06

I dettagli della certificazione FIPS per sono disponibili all'indirizzo AWS Transfer Family https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all

Di seguito viene mostrata la politica di sicurezza TransferSecurityPolicy -FIPS-2020-06.

> **Note**
>
> L'endpoint del servizio FIPS e la politica di sicurezza TransferSecurityPolicy -FIPS-2020-06 sono disponibili solo in alcune regioni. AWS Per ulteriori informazioni, consulta Endpoint e quote AWS Transfer Family nella Riferimenti generali di 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"
    ]
  }
}
```

Politiche di sicurezza post-quantistiche

Questa tabella elenca gli algoritmi per le politiche di sicurezza post-quantistiche di Transfer Family. Queste politiche sono descritte in dettaglio in. Utilizzo dello scambio di chiavi post-quantistiche ibrido con AWS Transfer Family

Gli elenchi delle politiche seguono la tabella.

Policy di sicurezza	TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	TransferSecurityPolitica-PQ-SSH-FIPS-Sperimentale-2023-04
SSH ciphers		
aes128-ctr		♦
aes128-gcm@openssh.com	♦	♦
aes192-ctr	♦	♦

Policy di sicurezza	TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	TransferSecurityPolitica-PQ-SSH-FIPS-Sperimentale-2023-04
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-gruppo16-sha512	♦	♦
diffie-hellman-gruppo18-sha512	♦	♦
ecdh-sha2-nistp384		♦
ecdh-sha2-nistp521		♦
diffie-hellman-group-exchange-sha256	♦	♦

Policy di sicurezza	TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	TransferSecurityPolitica-PQ-SSH-FIPS-Sperimentale-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	♦	♦

Policy di sicurezza	TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	TransferSecurityPolitica-PQ-SSH-FIPS-Sperimentale-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	♦	♦

TransferSecurityPolitica-pq-ssh-sperimentale-2023-04

Di seguito viene illustrata la politica di sicurezza -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"
        ]
    }
}
```

TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04

Di seguito viene illustrata la politica di sicurezza -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"
        ]
    }
}
```

Politiche AWS Transfer Family di sicurezza per i connettori SFTP

Le politiche di sicurezza dei connettori SFTP AWS Transfer Family consentono di limitare l'insieme di algoritmi crittografici (codici di autenticazione dei messaggi (MAC), scambi di chiavi (KEX) e suite di crittografia) associati al connettore SFTP. Di seguito è riportato un elenco di algoritmi crittografici supportati per ogni politica di sicurezza del connettore SFTP.

> **Note**
>
> `TransferSFTPConnectorSecurityPolicy-2024-03`è la politica di sicurezza predefinita applicata ai connettori SFTP.

È possibile modificare la politica di sicurezza per il connettore. Seleziona Connettori dal riquadro di navigazione a sinistra di Transfer Family e seleziona il tuo connettore. Quindi seleziona Modifica nella sezione di configurazione Sftp. Nella sezione Opzioni dell'algoritmo di crittografia, scegli qualsiasi politica di sicurezza disponibile dall'elenco a discesa nel campo Politica di sicurezza.

Policy di sicurezza	Politica SFTP dei trasferimenti - 2024-03 ConnectorSecurity	Trasferisce la Connector Security politica SFTP-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-gruppo16-sha512	♦	♦
diffie-hellman-gruppo18-sha512	♦	♦
diffie-hellman-group-exchange-sha256	♦	♦
Macs		
hmac-sha2-512-etm@openssh.com	♦	♦
hmac-sha2-256-etm@openssh.com	♦	♦

Policy di sicurezza	Politica SFTP dei trasferimenti - 2024-03 ConnectorSecurity	Trasferisce la Connector Security politica SFTP-2023 -07
hmac-sha2-512	♦	♦
hmac-sha2-256	♦	♦
hmac-sha1		♦
hmac-sha-196		♦
Host Key Algorithms		
rsa-sha2-256	♦	♦
rsa-sha2-512	♦	♦
ecdsa-sha2-nistp256	♦	♦
ecdsa-sha2-nistp384	♦	♦
ecdsa-sha2-nistp521	♦	♦
ssh rsa		♦

Utilizzo dello scambio di chiavi post-quantistiche ibrido con AWS Transfer Family

AWS Transfer Family supporta un'opzione ibrida di creazione di chiavi post-quantistiche per il protocollo Secure Shell (SSH). La creazione di chiavi post-quantistiche è necessaria perché è già possibile registrare il traffico di rete e salvarlo per la decrittografia in futuro da parte di un computer quantistico, il cosiddetto attacco store-now-harvest-later.

Puoi utilizzare questa opzione quando ti connetti a Transfer Family per trasferimenti sicuri di file da e verso lo storage Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS). La creazione di chiavi ibride post-quantistiche in SSH introduce meccanismi di creazione di chiavi post-quantistici, che utilizza in combinazione con i classici algoritmi di scambio di chiavi. Le chiavi SSH create con le suite di crittografia classiche sono protette dagli attacchi di forza

bruta con la tecnologia attuale. Tuttavia, non si prevede che la crittografia classica rimanga sicura dopo l'emergere dell'informatica quantistica su larga scala in futuro.

Se la tua organizzazione si affida alla riservatezza a lungo termine dei dati trasmessi tramite una connessione Transfer Family, dovresti prendere in considerazione un piano per migrare alla crittografia post-quantistica prima che i computer quantistici su larga scala diventino disponibili per l'uso.

Per proteggere i dati crittografati oggi da potenziali attacchi futuri, AWS partecipa con la comunità crittografica allo sviluppo di algoritmi quantistici resistenti o post-quantistici. Abbiamo implementato suite di cifratura ibride post-quantistiche a scambio di chiavi in Transfer Family che combinano elementi classici e post-quantistici.

Queste suite di crittografia ibride sono disponibili per l'uso con i carichi di lavoro di produzione nella maggior parte delle regioni. AWS Tuttavia, poiché le caratteristiche prestazionali e i requisiti di larghezza di banda delle suite di crittografia ibride sono diversi da quelli dei classici meccanismi di scambio di chiavi, ti consigliamo di testarli sulle tue connessioni Transfer Family.

Scopri di più sulla crittografia post-quantistica nel post del blog sulla sicurezza di Post-Quantum Cryptography.

Indice

Informazioni sullo scambio di chiavi ibride post-quantistiche in SSH

Transfer Family supporta suite di cifratura a scambio di chiavi ibride post-quantistiche, che utilizzano sia il classico algoritmo di scambio di chiavi Elliptic Curve Diffie-Hellman (ECDH) che CRYSTALS Kyber. Kyber è un algoritmo post-quantistico di crittografia a chiave pubblica e di definizione delle

chiavi che il National Institute for Standards and Technology (NIST) ha designato come primo algoritmo di accordo di chiavi post-quantistiche standard.

Il client e il server effettuano ancora uno scambio di chiavi ECDH. Inoltre, il server incapsula un segreto condiviso post-quantistico nella chiave pubblica KEM post-quantistica del client, pubblicizzata nel messaggio di scambio di chiavi SSH del client. Questa strategia combina l'elevata garanzia di uno scambio di chiavi classico con la sicurezza degli scambi di chiavi post-quantistici proposti, per contribuire a garantire che le strette di mano siano protette finché l'ECDH o il segreto condiviso post-quantistico non possono essere violati.

Come funziona la creazione di chiavi ibride post-quantistiche in Transfer Family

AWS ha recentemente annunciato il supporto per lo scambio di chiavi post-quantistiche nei trasferimenti di file SFTP in. AWS Transfer Family Transfer Family ridimensiona in modo sicuro i trasferimenti di business-to-business file ai servizi di AWS archiviazione utilizzando SFTP e altri protocolli. SFTP è una versione più sicura del File Transfer Protocol (FTP) che funziona su SSH. Il supporto post-quantistico per lo scambio di chiavi di Transfer Family innalza il livello di sicurezza per i trasferimenti di dati tramite SFTP.

Il supporto SFTP per lo scambio di chiavi ibrido post-quantistico in Transfer Family include la combinazione di algoritmi post-quantistici Kyber-512, Kyber-768 e Kyber-1024, con ECDH su curve P256, P384, P521 o Curve25519. I seguenti metodi di scambio di chiavi SSH corrispondenti sono specificati nella bozza di scambio di chiavi SSH ibrida post-quantistica.

- `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**
>
> Questi nuovi metodi di scambio di chiavi possono cambiare man mano che la bozza evolve verso la standardizzazione o quando il NIST ratificherà l'algoritmo Kyber.

Perché Kyber?

AWS si impegna a supportare algoritmi standardizzati e interoperabili. Kyber è il primo algoritmo di crittografia post-quantistica selezionato per la standardizzazione dal progetto NIST Post-Quantum Cryptography. Alcuni enti di normazione stanno già integrando Kyber nei protocolli. AWS supporta già Kyber in TLS in alcuni endpoint API. AWS

Come parte di questo impegno, AWS ha presentato una bozza di proposta all'IETF per la crittografia post-quantistica che combina Kyber con curve approvate dal NIST come P256 per SSH. Per contribuire a migliorare la sicurezza dei nostri clienti, l' AWS implementazione dello scambio di chiavi post-quantistiche in SFTP e SSH segue quella bozza. Abbiamo intenzione di supportarne i futuri aggiornamenti fino a quando la nostra proposta non sarà adottata dall'IETF e diventerà uno standard.

I nuovi metodi di scambio delle chiavi (elencati nella sezioneCome funziona la creazione di chiavi ibride post-quantistiche in Transfer Family) potrebbero cambiare man mano che la bozza evolverà verso la standardizzazione o quando il NIST ratificherà l'algoritmo Kyber.

> **Note**
>
> Il supporto di algoritmi post-quantistici è attualmente disponibile per lo scambio di chiavi ibride post-quantistiche in TLS AWS KMS (vedi Utilizzo del TLS ibrido post-quantistico con) e per gli endpoint API. AWS KMSAWS Certificate Manager AWS Secrets Manager

Scambio di chiavi SSH ibrido post-quantistico e requisiti crittografici (FIPS 140)

Per i clienti che richiedono la conformità FIPS, Transfer Family fornisce crittografia approvata FIPS in SSH utilizzando la libreria crittografica open source certificata AWS FIPS 140, -LC. AWSI metodi di scambio di chiavi ibridi post-quantistici supportati nel TransferSecurityPolicy -PQ-SSH-FIPS-Experimental-2023-04 in Transfer Family sono approvati FIPS secondo lo SP 800-56Cr2 del NIST (sezione 2). Anche l'Ufficio federale tedesco per la sicurezza delle informazioni (BSI) e l'Agence nationale de la sécurité des systèmes d'information (ANSSI) della Francia raccomandano tali metodi di scambio di chiavi ibridi post-quantistici.

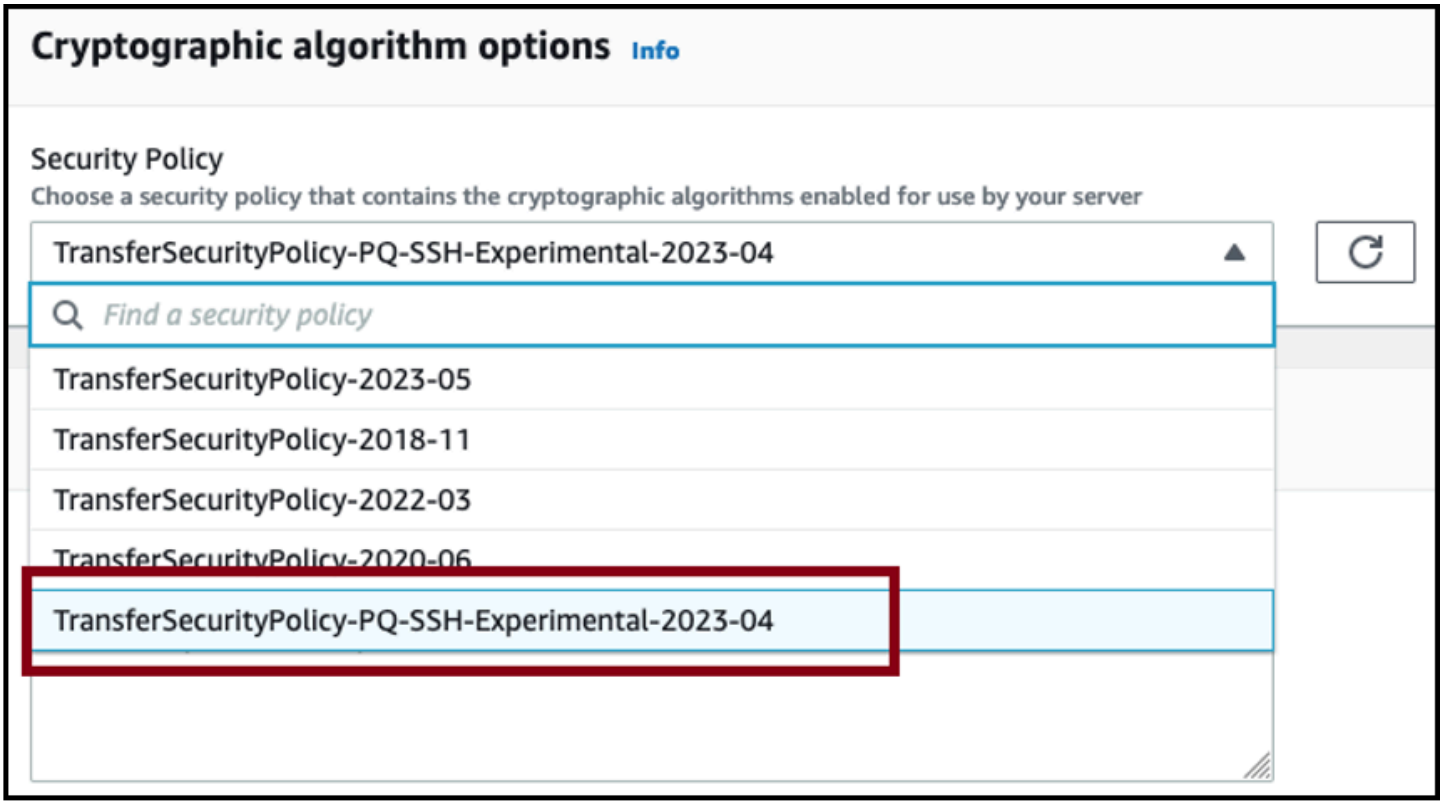
Test dello scambio di chiavi ibride post-quantistiche in Transfer Family

Questa sezione descrive i passaggi da seguire per testare lo scambio di chiavi ibride post-quantistiche.

1. Abilita lo scambio di chiavi ibride post-quantistiche sul tuo endpoint SFTP.
2. Utilizzate un client SFTP (ad esempioConfigura un client SFTP che supporti lo scambio di chiavi ibride post-quantistiche) che supporti lo scambio di chiavi ibride post-quantistiche seguendo le indicazioni contenute nella bozza di specifica sopra menzionata.
3. Trasferisci un file utilizzando un server Transfer Family.
4. Conferma lo scambio di chiavi ibride post-quantistiche in SFTP.

Abilita lo scambio di chiavi ibride post-quantistiche sul tuo endpoint SFTP

È possibile scegliere la politica SSH quando si crea un nuovo endpoint server SFTP in Transfer Family o modificando le opzioni dell'algoritmo crittografico in un endpoint SFTP esistente. L'istantanea seguente mostra un esempio di come si aggiorna la AWS Management Console policy SSH.



I nomi delle policy SSH che supportano lo scambio di chiavi post-quantistiche sono Policy-PQ-SSH-Experimental-2023-04 e Policy-PQ-SSH-FIPS-Experimental-2023-04. TransferSecurity TransferSecurity Per maggiori dettagli sulle politiche di Transfer Family, consultaPolitiche di sicurezza per AWS Transfer Family i server.

Configura un client SFTP che supporti lo scambio di chiavi ibride post-quantistiche

Dopo aver selezionato la politica SSH post-quantistica corretta nell'endpoint SFTP Transfer Family, puoi sperimentare l'SFTP post-quantistico in Transfer Family. È possibile utilizzare un client SFTP (come OQS OpenSSH) che supporti lo scambio di chiavi ibride post-quantistiche seguendo le indicazioni contenute nella bozza di specifica sopra menzionata.

OQS OpenSSH è un fork open source di OpenSSH che aggiunge la crittografia quantistica sicura a SSH utilizzando. `liboqs` `liboqs`è una libreria C open source che implementa algoritmi crittografici a resistenza quantistica. OQS OpenSSH `liboqs` e fanno parte del progetto Open Quantum Safe (OQS).

Per testare lo scambio di chiavi ibride post-quantistiche in Transfer Family SFTP con OQS OpenSSH, devi creare OQS OpenSSH come spiegato nel README del progetto. Dopo aver creato OQS OpenSSH, è possibile eseguire il client SFTP di esempio per connettersi all'endpoint SFTP (ad esempio`s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com`,) utilizzando i metodi di scambio di chiavi ibridi post-quantistici, come illustrato nel comando seguente.

```
./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
```

Nel comando precedente, sostituisci i seguenti elementi con le tue informazioni:

- Sostituite *`username_private_key_PEM_File con la chiave privata dell'utente SFTP con codifica PEM`*
- Sostituisci *`il nome utente`* con il nome utente SFTP
- Sostituisci *`server-id con l'ID`* del server Transfer Family
- Sostituisci *`region-id`* con la regione effettiva in cui si trova il tuo server Transfer Family

Conferma lo scambio di chiavi ibride post-quantistiche in SFTP

Per confermare che lo scambio di chiavi ibride post-quantistiche è stato utilizzato durante una connessione SSH per SFTP a Transfer Family, controlla l'output del client. Facoltativamente, è possibile utilizzare un programma di acquisizione di pacchetti. Se si utilizza il client Open Quantum Safe OpenSSH, l'output dovrebbe essere simile al seguente (omettendo informazioni irrilevanti per brevità):

```
$./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>
```

L'output mostra che la negoziazione con il cliente è avvenuta utilizzando il metodo ibrido post-quantistico e ha stabilito con successo una sessione SFTP. `ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org`

Protezione dei dati in AWS Transfer Family

Il modello di responsabilità AWS condivisa Modello di di si applica alla protezione dei dati in AWS Transfer Family (Transfer Family). Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutto il AWS Cloud. L'utente è responsabile di mantenere il controllo sui contenuti ospitati su questa infrastruttura. Questo contenuto include le attività di configurazione e gestione della sicurezza per i AWS servizi che utilizzi. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il modello di responsabilitàAWS condivisa e il post sul blog sul GDPR sul AWS Security Blog.

Ai fini della protezione dei dati, ti consigliamo di proteggere le credenziali degli AWS account e di configurare account utente individuali con AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il proprio lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse. AWS Supportiamo TLS 1.2.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS dei servizi.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati personali archiviati in Amazon S3.
- Se si richiedono moduli crittografici convalidati FIPS 140-2 quando si accede ad AWS tramite una CLI o un'API, utilizzare un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Consigliamo di non inserire mai informazioni identificative sensibili, ad esempio i numeri di account dei clienti, in campi a formato libero come un campo Nome. Ciò include quando lavori con Transfer Family o altri AWS servizi utilizzando la console, l'API o AWS gli SDK. AWS CLI Tutti i dati di configurazione inseriti nella configurazione del servizio Transfer Family o nelle configurazioni di altri servizi potrebbero essere raccolti per essere inclusi nei registri di diagnostica. Quando fornisci un

URL a un server esterno, non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta a tale server.

Al contrario, i dati delle operazioni di caricamento e download da e verso i server Transfer Family vengono trattati come completamente privati e non esistono mai al di fuori dei canali crittografati, come una connessione SFTP o FTPS. Questi dati sono sempre accessibili solo alle persone autorizzate.

Argomenti

Crittografia dei dati in Amazon S3

AWS Transfer Family utilizza le opzioni di crittografia predefinite impostate per il bucket Amazon S3 per crittografare i dati. Quando abiliti la crittografia in un bucket, tutti gli oggetti vengono crittografati quando vengono archiviati nel bucket. Gli oggetti vengono crittografati utilizzando la crittografia lato server con chiavi gestite Amazon S3 (SSE-S3) AWS Key Management Service o () chiavi gestite (SSE-KMS AWS KMS). Per informazioni sulla crittografia lato server, consulta Protezione dei dati utilizzando la crittografia lato server nella Guida per l'utente di Amazon Simple Storage Service.

I passaggi seguenti mostrano come crittografare i dati in. AWS Transfer Family

Per consentire la crittografia in AWS Transfer Family

1. Abilita la crittografia predefinita per il tuo bucket Amazon S3. Per istruzioni, consulta la crittografia predefinita di Amazon S3 per i bucket S3 nella Guida per l'utente di Amazon Simple Storage Service.
2. Aggiorna la policy del ruolo AWS Identity and Access Management (IAM) allegata all'utente per concedere le autorizzazioni richieste AWS Key Management Service ()AWS KMS.
3. Se si utilizza una politica di sessione per l'utente, la politica di sessione deve concedere le AWS KMS autorizzazioni richieste.

L'esempio seguente mostra una policy IAM che concede le autorizzazioni minime richieste quando si utilizza AWS Transfer Family con un bucket Amazon S3 abilitato per la crittografia. AWS KMS Includi questa policy di esempio sia nella policy del ruolo IAM dell'utente che nella policy di sessione, se ne utilizzi una.

```
{
 "Sid": "Stmt1544140969635",
 "Action": [
  "kms:Decrypt",
  "kms:Encrypt",
  "kms:GenerateDataKey"
 ],
 "Effect": "Allow",
 "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

> **Note**
>
> L'ID della chiave KMS specificato in questa politica deve essere lo stesso specificato per la crittografia predefinita nel passaggio 1.
> Root, o il ruolo IAM utilizzato per l'utente, deve essere consentito nella policy AWS KMS chiave. Per informazioni sulla politica AWS KMS chiave, consulta Using key policy in AWS KMS nella AWS Key Management Service Developer Guide.

Gestione delle chiavi SSH e PGP in Transfer Family

In questa sezione, puoi trovare informazioni sulle chiavi SSH, incluso come generarle e come ruotarle. Per i dettagli sull'utilizzo di Transfer Family with AWS Lambda per gestire le chiavi, consulta il post del blog Enabling user self-service key management with A AWS Transfer Family and AWS Lambda.

> **Note**
>
> AWS Transfer Family accetta le chiavi RSA, ECDSA ed ED25519.

Questa sezione spiega anche come generare e gestire le chiavi Pretty Good Privacy (PGP).

Argomenti

- Algoritmi supportati per chiavi utente e server
- Genera chiavi SSH per gli utenti gestiti dal servizio
- Ruota le chiavi SSH

- Genera e gestisci le chiavi PGP
- Client PGP supportati

Algoritmi supportati per chiavi utente e server

I seguenti algoritmi chiave sono supportati per le coppie di chiavi utente e server all'interno. AWS Transfer Family

> **Note**
>
> Per gli algoritmi da utilizzare con la decrittografia PGP nei flussi di lavoro, vedere Algoritmi supportati per le coppie di chiavi PGP.

- Per ED25519: `ssh-ed25519`
- Per RSA:
  - `rsa-sha2-256`
  - `rsa-sha2-512`
- Per ECDSA:
  - `ecdsa-sha2-nistp256`
  - `ecdsa-sha2-nistp384`
  - `ecdsa-sha2-nistp521`

> **Note**
>
> `ssh-rsa`Supportiamo SHA1 per le nostre vecchie politiche di sicurezza. Per informazioni dettagliate, vedi Algoritmi crittografici.

Genera chiavi SSH per gli utenti gestiti dal servizio

È possibile configurare il server per autenticare gli utenti utilizzando il metodo di autenticazione gestita dal servizio, in cui i nomi utente e le chiavi SSH sono archiviati all'interno del servizio. La chiave SSH pubblica dell'utente viene caricata sul server come proprietà dell'utente. Questa chiave viene utilizzata dal server come parte di un processo di autenticazione standard basato su chiavi.

Ogni utente può avere più chiavi SSH pubbliche su file con un singolo server. Per i limiti al numero di chiavi che possono essere archiviate per utente, consulta AWS Transfer Family endpoint e quote in. Riferimenti generali di Amazon Web Services

In alternativa al metodo di autenticazione gestita dal servizio, puoi autenticare gli utenti utilizzando un provider di identità personalizzato oppure. AWS Directory Service for Microsoft Active Directory Per ulteriori informazioni, consulta Lavorare con provider di identità personalizzati o Utilizzo del provider di identità AWS Directory Service.

Un server può autenticare gli utenti solo utilizzando un metodo (servizio gestito, servizio di directory o provider di identità personalizzato) e tale metodo non può essere modificato dopo la creazione del server.

Argomenti

- Creazione di chiavi SSH su macOS, Linux o Unix
- Creazione di chiavi SSH su Microsoft Windows
- Convertire una chiave pubblica SSH2 in formato PEM

Creazione di chiavi SSH su macOS, Linux o Unix

Nei sistemi operativi macOS, Linux o Unix, si utilizza il `ssh-keygen` comando per creare una chiave pubblica SSH e una chiave privata SSH, nota anche come coppia di chiavi.

Per creare chiavi SSH su un sistema operativo macOS, Linux o Unix

1. Sui sistemi operativi macOS, Linux o Unix, apri un terminale di comando.
2. AWS Transfer Family accetta chiavi in formato RSA, ECDSA ed ED25519. Scegliete il comando appropriato in base al tipo di coppia di chiavi che state generando.

> **Note**
>
> Negli esempi seguenti, non viene specificata una passphrase: in questo caso, lo strumento chiede di inserire la passphrase e quindi di ripeterla per verificare. La creazione di una passphrase offre una protezione migliore per la chiave privata e potrebbe anche migliorare la sicurezza generale del sistema. Non è possibile recuperare la passphrase: se la si dimentica, è necessario creare una nuova chiave.
> Tuttavia, se state generando una chiave host del server, dovete specificare una passphrase vuota, specificando l'`-N ""`opzione nel comando (o premendo **`Enter`** due

volte quando richiesto), perché i server Transfer Family non possono richiedere una password all'avvio.

- Per generare una coppia di chiavi RSA 4096 bit:

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Per generare una coppia di chiavi ECDSA a 521 bit (ECDSA ha dimensioni in bit di 256, 384 e 521):

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Per generare una coppia di chiavi ED25519:

```
ssh-keygen -t ed25519 -f key_name
```

Note

*key_name*è il nome del file della coppia di chiavi SSH.

Di seguito viene illustrato un esempio dell'`ssh-keygen`output.

```
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**
>
> Quando si esegue il comando `ssh-keygen` come mostrato in precedenza, le chiavi pubblica e privata vengono create come file nella directory corrente.

La tua coppia di chiavi SSH è ora pronta per l'uso. Segui i passaggi 3 e 4 per archiviare la chiave pubblica SSH per gli utenti gestiti dal servizio. Questi utenti utilizzano le chiavi quando trasferiscono file sugli endpoint del server Transfer Family.

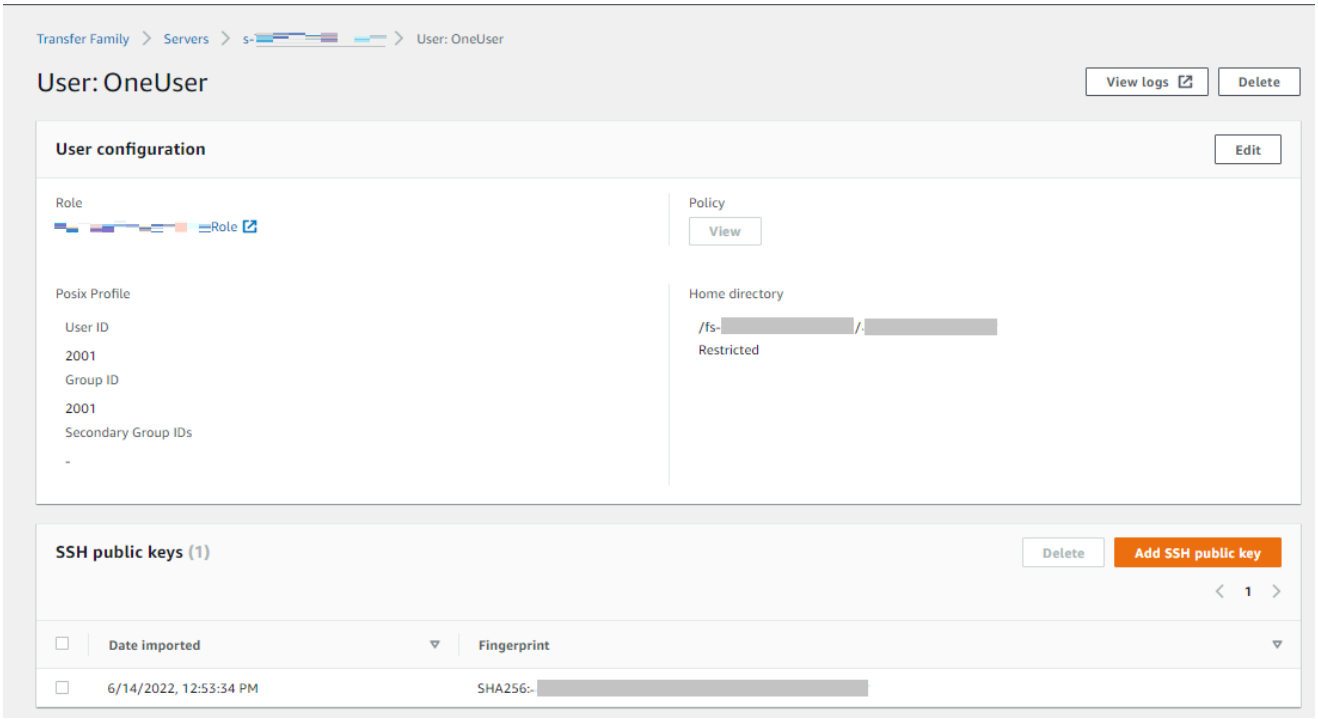
3. Accedere al *`key_name`*`.pub` file e aprirlo.
4. Copia il testo e incollalo nella chiave pubblica SSH per l'utente gestito dal servizio.

   a. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/, quindi seleziona Server dal pannello di navigazione.

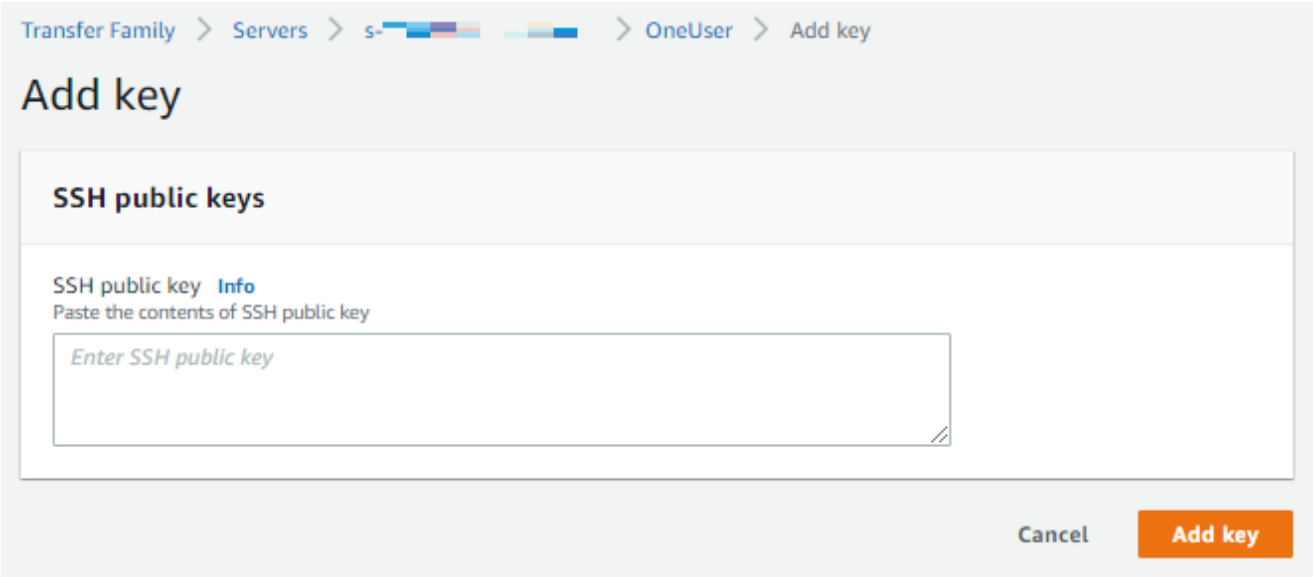
   b. Nella pagina Server, seleziona l'ID server per il server che contiene l'utente che desideri aggiornare.

   c. Seleziona l'utente per il quale stai aggiungendo una chiave pubblica.

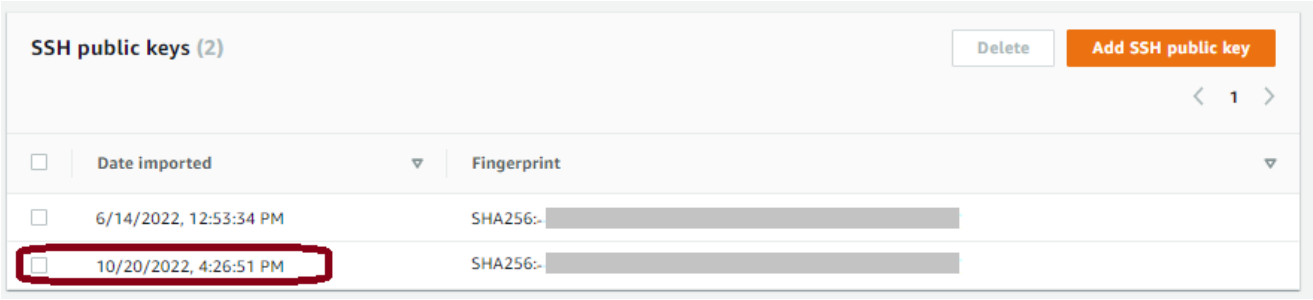
   d. Nel riquadro delle chiavi pubbliche SSH, scegli Aggiungi chiave pubblica SSH.



e. Incolla il testo della chiave pubblica che hai generato nella casella di testo della chiave pubblica SSH, quindi scegli Aggiungi chiave.



La nuova chiave è elencata nel riquadro delle chiavi pubbliche SSH.



Creazione di chiavi SSH su Microsoft Windows

Windows utilizza un formato della coppia di chiavi SSH leggermente diverso. La chiave pubblica deve essere nel formato PUB e la chiave privata deve essere nel formato PPK. In Windows, puoi utilizzare PuTTYgen per creare una coppia di chiavi SSH nei formati appropriati. Puoi anche utilizzare PuTTYgen per convertire una chiave privata generata utilizzando `ssh-keygen` in un file `.ppk`.

> **Note**
>
> Se si presenta a WinSCP un file di chiave privata non `.ppk` in formato, quel client offre la possibilità di convertire la chiave `.ppk` in formato per voi.

Per un tutorial sulla creazione di chiavi SSH utilizzando PuTTYgen su Windows, consulta il sito Web SSH.com.

Convertire una chiave pubblica SSH2 in formato PEM

AWS Transfer Family accetta solo chiavi pubbliche in formato PEM. Se hai una chiave pubblica SSH2, devi convertirla. Una chiave pubblica SSH2 ha il seguente formato:

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

Una chiave pubblica PEM ha il seguente formato:

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

Esegui il comando seguente per convertire una chiave pubblica in formato SSH2 in una chiave pubblica in formato PEM. *Sostituisci ssh2-key con il nome della tua chiave SSH2 e la chiave PEM con il nome della tua chiave PEM.*

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

Ruota le chiavi SSH

Per motivi di sicurezza, consigliamo la migliore pratica di ruotare le chiavi SSH. Di solito, questa rotazione viene specificata come parte di una politica di sicurezza e viene implementata in modo automatico. A seconda del livello di sicurezza, per una comunicazione altamente sensibile, una coppia di chiavi SSH potrebbe essere utilizzata una sola volta. In tal modo si elimina qualsiasi rischio causato da chiavi archiviate. Tuttavia, è molto più comune archiviare le credenziali SSH per un periodo di tempo e impostare un intervallo che non imponga un onere eccessivo agli utenti. Un intervallo di tempo di tre mesi è la norma.

Sono disponibili due metodi per eseguire la rotazione di chiavi SSH:

- Sulla console, puoi caricare una nuova chiave pubblica SSH ed eliminare una chiave pubblica SSH esistente.
- Utilizzando l'API, è possibile aggiornare gli utenti esistenti utilizzando l'DeleteSshPublicKeyAPI per eliminare la chiave pubblica Secure Shell (SSH) di un utente e l'ImportSshPublicKeyAPI per aggiungere una nuova chiave pubblica Secure Shell (SSH) all'account dell'utente.

Console

Per eseguire una rotazione dei tasti nella console

1. Apri la AWS Transfer Family console all'indirizzo https://console.aws.amazon.com/transfer/.
2. Vai alla pagina Server.
3. Scegli l'identificatore nella colonna Server ID per visualizzare la pagina dei dettagli del server.
4. In Utenti, seleziona la casella di controllo dell'utente di cui desideri ruotare la chiave pubblica SSH, quindi scegli Azioni, quindi scegli Aggiungi chiave per visualizzare la pagina Aggiungi chiave.

   oppure

Scegli il nome utente per visualizzare la pagina dei dettagli dell'utente, quindi scegli Aggiungi chiave pubblica SSH per visualizzare la pagina Aggiungi chiave.

5. Inserisci la nuova chiave pubblica SSH e scegli Aggiungi chiave.

> **Important**
>
> Il formato della chiave pubblica SSH dipende dal tipo di chiave generata.
>
> - Per le chiavi RSA, il formato è. `ssh-rsa` *`string`*
> - Per le chiavi ED25519, il formato è. `ssh-ed25519` *`string`*
> - Per le chiavi ECDSA, la chiave inizia con`ecdsa-sha2-nistp256`, o `ecdsa-sha2-nistp384``ecdsa-sha2-nistp521`, a seconda della dimensione della chiave generata. La stringa iniziale viene quindi seguita da*`string`*, in modo simile agli altri tipi di chiave.

Si torna alla pagina dei dettagli utente e la nuova chiave pubblica SSH appena inserita viene visualizzata nella sezione Chiavi pubbliche SSH.

6. Seleziona la casella di controllo della vecchia chiave you che desideri eliminare, quindi scegli Elimina.
7. Conferma l'operazione di eliminazione inserendo la parola`delete`, quindi scegli Elimina.

API

Per eseguire una rotazione delle chiavi utilizzando l'API

1. Sui sistemi operativi macOS, Linux o Unix, apri un terminale di comando.
2. Recupera la chiave SSH che desideri eliminare inserendo il seguente comando. Per utilizzare questo comando, *`serverID`* sostituiscilo con l'ID del server Transfer Family e sostituiscilo *`username`* con il tuo nome utente.

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

Il comando restituisce dettagli sull'utente. Copia il contenuto del `"SshPublicKeyId":` campo. Sarà necessario immettere questo valore più avanti in questa procedura.

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":
 "keyID",
   "DateImported": 1621969331.072 } ],
```

3. Quindi, importa una nuova chiave SSH per il tuo utente. Al prompt , immettere il comando di seguito. Per utilizzare questo comando, sostituiscilo *serverID* con l'ID del server Transfer Family, sostituiscilo *username* con il tuo nome utente e sostituiscilo *public-key* con l'impronta digitale della tua nuova chiave pubblica.

   ```
   aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'
      --ssh-public-key-body='public-key'
   ```

   Se il comando ha esito positivo, non viene restituito alcun output.

4. Infine, elimina la vecchia chiave eseguendo il comando seguente. Per utilizzare questo comando, sostituiscilo *serverID* con l'ID del server Transfer Family, sostituiscilo *username* con il tuo nome utente e *keyID-from-step-2* sostituiscilo con il valore dell'ID chiave che hai copiato nel passaggio 2 di questa procedura

   ```
   aws transfer delete-ssh-public-key --server-id='serverID' --user-name='username'
      --ssh-public-key-id='keyID-from-step-2'
   ```

5. (Facoltativo) Per confermare che la vecchia chiave non esiste più, ripetete il passaggio 2.

Genera e gestisci le chiavi PGP

È possibile utilizzare la decrittografia Pretty Good Privacy (PGP) con i file che Transfer Family elabora con i flussi di lavoro. Per utilizzare la decrittografia in una fase del flusso di lavoro, fornite una chiave PGP.

Il blog AWS sullo storage ha un post che descrive come decrittografare semplicemente i file senza scrivere alcun codice utilizzando i flussi di lavoro Transfer Family Managed, crittografare e decrittografare i file con PGP e. AWS Transfer Family

Genera chiavi PGP

L'operatore utilizzato per generare le chiavi PGP dipende dal sistema operativo e dalla versione del software di generazione delle chiavi in uso.

Se usi Linux o Unix, usa il programma di installazione del pacchetto per l'installazione. `gpg` A seconda della distribuzione Linux in uso, uno dei seguenti comandi dovrebbe funzionare correttamente.

```
sudo yum install gnupg
```

```
sudo apt-get install gnupg
```

Per Windows o macOS, puoi scaricare ciò che ti serve da https://gnupg.org/download/.

Dopo aver installato il software generatore di chiavi PGP, si esegue il `gpg --gen-key` comando `gpg --full-gen-key` o per generare una coppia di chiavi.

> **Note**
>
> Se utilizzi la GnuPG versione 2.3.0 o successiva, devi eseguire. `gpg --full-gen-key` Quando viene richiesto il tipo di chiave da creare, scegli RSA o ECC. Tuttavia, se scegli ECC, assicurati di scegliere uno dei due NIST o BrainPool per la curva ellittica. Non scegliete. Curve 25519

Algoritmi supportati per le coppie di chiavi PGP

Supportiamo i seguenti algoritmi per le coppie di chiavi PGP:

- RSA
- Elgamal
- ECC.:
  - NIST
  - BrainPool

> **Note**
>
> Non supportiamo le chiavi CCurve25519.

gpgSottocomandi utili

Di seguito sono riportati alcuni sottocomandi utili per: gpg

- `gpg --help`— Questo comando elenca le opzioni disponibili e potrebbe includere alcuni esempi.
- `gpg --list-keys`— Questo comando elenca i dettagli di tutte le coppie di chiavi create.
- `gpg --fingerprint`— Questo comando elenca i dettagli di tutte le coppie di chiavi, inclusa l'impronta digitale di ogni chiave.
- `gpg --export -a` *`user-name`*— Questo comando esporta la parte della chiave pubblica relativa alla *`user-name`* chiave utilizzata al momento della generazione della chiave.

Gestire le chiavi PGP

Per gestire le tue chiavi PGP, usa. AWS Secrets Manager

> **Note**
>
> Il tuo nome segreto include l'ID del server Transfer Family. Ciò significa che dovreste aver già identificato o creato un server prima di poter memorizzare le informazioni della chiave PGP. AWS Secrets Manager

Se desideri utilizzare una chiave e una passphrase per tutti i tuoi utenti, puoi memorizzare le informazioni sul blocco delle chiavi PGP sotto il nome segretoaws/transfer/*`server-id`*/@pgp-default, dove si *`server-id`* trova l'ID del tuo server Transfer Family. Transfer Family utilizza questa chiave predefinita se non esiste una chiave in cui *`user-name`* corrisponde all'utente che sta eseguendo il flusso di lavoro.

È possibile creare una chiave per un utente specifico. In questo caso, il formato per il nome segreto èaws/transfer/*`server-id`*/*`user-name`*, dove *`user-name`* corrisponde all'utente che esegue il flusso di lavoro per un server Transfer Family.

> **Note**
>
> È possibile memorizzare un massimo di 3 chiavi private PGP, per server Transfer Family, per utente.

Per configurare le chiavi PGP da utilizzare con la decrittografia

1. A seconda della versione di GPG che stai utilizzando, esegui uno dei seguenti comandi per generare una coppia di chiavi PGP che non utilizzi un algoritmo di crittografia Curve 25519.

   - Se utilizzi la **GnuPG** versione 2.3.0 o successiva, esegui il seguente comando:

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

     Puoi scegliere o**RSA**, se lo desideri, puoi scegliere **ECC** uno dei due **NIST** o **BrainPool** per la curva ellittica. Se `gpg --gen-key` invece esegui, crei una coppia di chiavi che utilizza l'algoritmo di crittografia ECC Curve 25519, che attualmente non supportiamo per le chiavi PGP.

   - Per le versioni **GnuPG** precedenti alla 2.3.0, puoi utilizzare il seguente comando, poiché RSA è il tipo di crittografia predefinito.

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

   > **Important**
   >
   > Durante il processo di generazione delle chiavi, è necessario fornire una passphrase e un indirizzo e-mail. Assicurati di prendere nota di questi valori. È necessario fornire la passphrase quando si inseriscono i dettagli della chiave in una fase AWS Secrets Manager successiva di questa procedura. Inoltre, è necessario fornire lo stesso indirizzo e-mail per esportare la chiave privata nel passaggio successivo.

2. Esegui il comando seguente per esportare la chiave privata. Per utilizzare questo comando, sostituiscilo *`private.pgp`* con il nome del file in cui salvare il blocco di chiave privata e *`marymajor@example.com`* con l'indirizzo email che hai usato quando hai generato la coppia di chiavi.

   ```
   gpg --output private.pgp --armor --export-secret-key marymajor@example.com
   ```

3. AWS Secrets Manager Utilizzatelo per memorizzare la vostra chiave PGP.

   a. Accedi AWS Management Console e apri la AWS Secrets Manager console all'indirizzo https://console.aws.amazon.com/secretsmanager/.

b. Nel pannello di navigazione a sinistra, seleziona Segreti.

c. Nella pagina Segreti, scegli Memorizza un nuovo segreto.

d. Nella pagina Scegli il tipo di segreto, per Tipo segreto, seleziona Altro tipo di segreto.

e. Nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.

- Chiave: Invio. **`PGPPrivateKey`**

> **Note**
>
> È necessario immettere la **`PGPPrivateKey`** stringa esattamente: non aggiungere spazi prima o tra i caratteri.

- value — Incolla il testo della tua chiave privata nel campo del valore. È possibile trovare il testo della chiave privata nel file (ad esempio,`private.pgp`) specificato al momento dell'esportazione della chiave in precedenza in questa procedura. La chiave inizia con `-----BEGIN PGP PRIVATE KEY BLOCK-----` e finisce con`-----END PGP PRIVATE KEY BLOCK-----`.

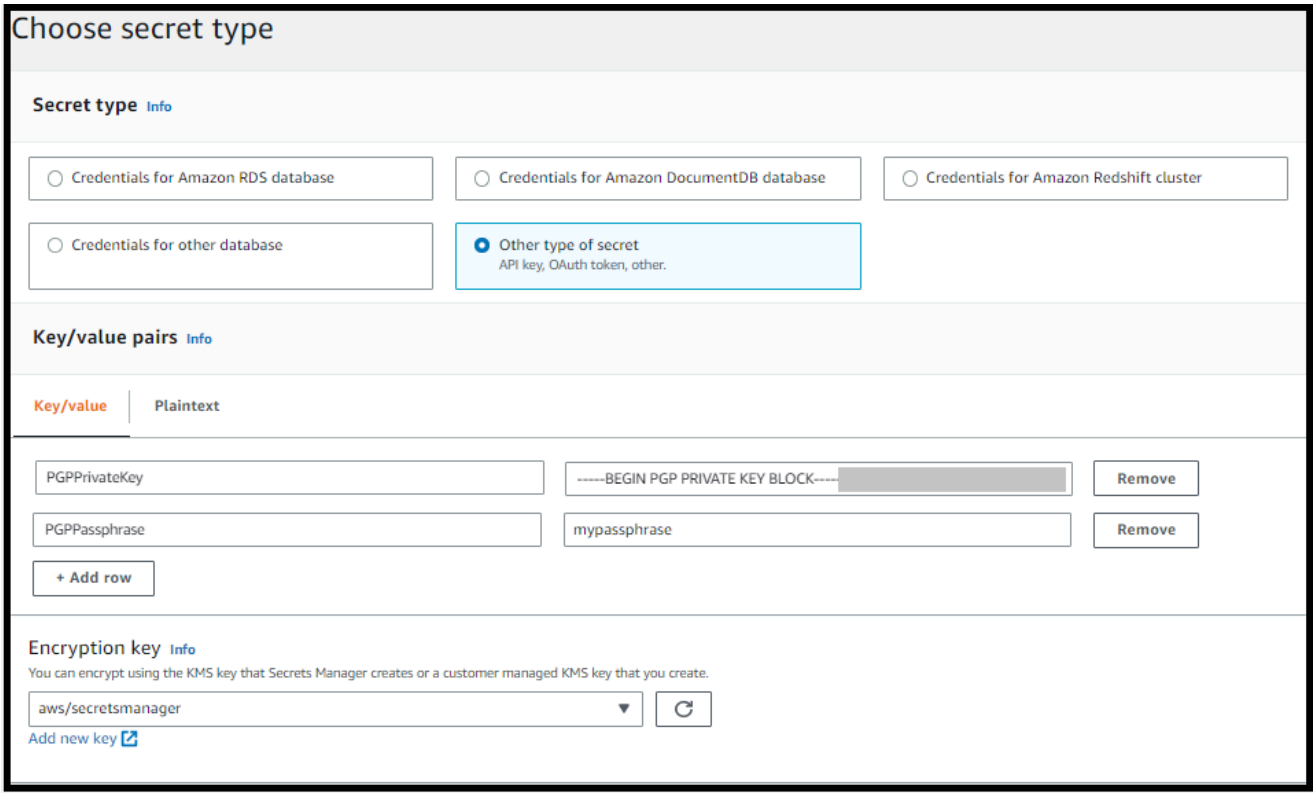
> **Note**
>
> Assicurati che il blocco di testo contenga solo la chiave privata e non contenga anche la chiave pubblica.

f. Seleziona Aggiungi riga e nella sezione Coppie chiave/valore, scegli la scheda Chiave/valore.

- Chiave: Invio. **`PGPPassphrase`**

> **Note**
>
> È necessario immettere la **`PGPPassphrase`** stringa esattamente: non aggiungere spazi prima o tra i caratteri.

- value — Inserisci la passphrase che hai usato quando hai generato la tua coppia di key pair PGP.



> **Note**
>
> Puoi aggiungere fino a 3 set di chiavi e passphrase. Per aggiungere un secondo set, aggiungi due nuove righe e inserisci e **`PGPPassphrase2`** per le chiavi **`PGPPrivateKey2`** e incolla un'altra chiave privata e passphrase. Per aggiungere un terzo set, i valori chiave devono essere e. **`PGPPrivateKey3 PGPPassphrase3`**

g. Seleziona Successivo.

h. Nella pagina Configura segreto, inserisci un nome e una descrizione per il tuo segreto.

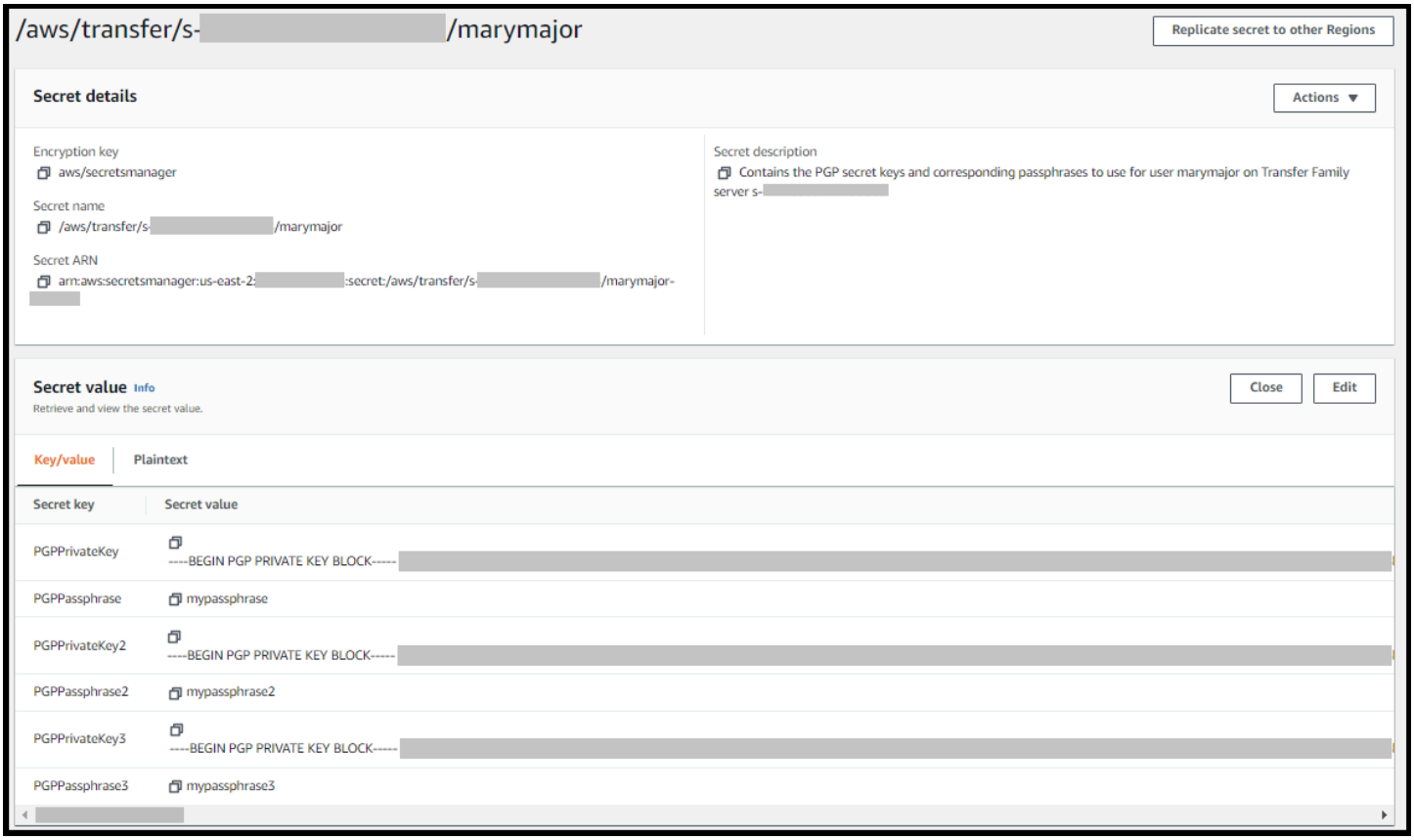
- Se stai creando una chiave predefinita, ovvero una chiave che può essere utilizzata da qualsiasi utente di Transfer Family, inserisci**`aws/transfer/`*`server-id`*`/@pgp-default`**. Sostituiscila *`server-id`* con l'ID del server che contiene il flusso di lavoro che prevede una fase di decrittografia.
- Se stai creando una chiave che deve essere utilizzata da un utente Transfer Family specifico, inserisci**`aws/transfer/`*`server-id`*`/`*`user-name`**. Sostituiscilo *`server-id`* con l'ID del server che contiene il flusso di lavoro con una fase di decrittografia e

sostituiscilo *`user-name`* con il nome dell'utente che esegue il flusso di lavoro. *`user-name`*Viene memorizzato nel provider di identità utilizzato dal server Transfer Family.

i. Scegli Avanti e accetta le impostazioni predefinite nella pagina Configura rotazione. Quindi scegli Successivo.

j. Nella pagina Revisione, scegli Store per creare e archiviare il segreto.

La schermata seguente mostra i dettagli dell'utente **`marymajor`** per uno specifico server Transfer Family. Questo esempio mostra tre tasti e le relative passphrase corrispondenti.



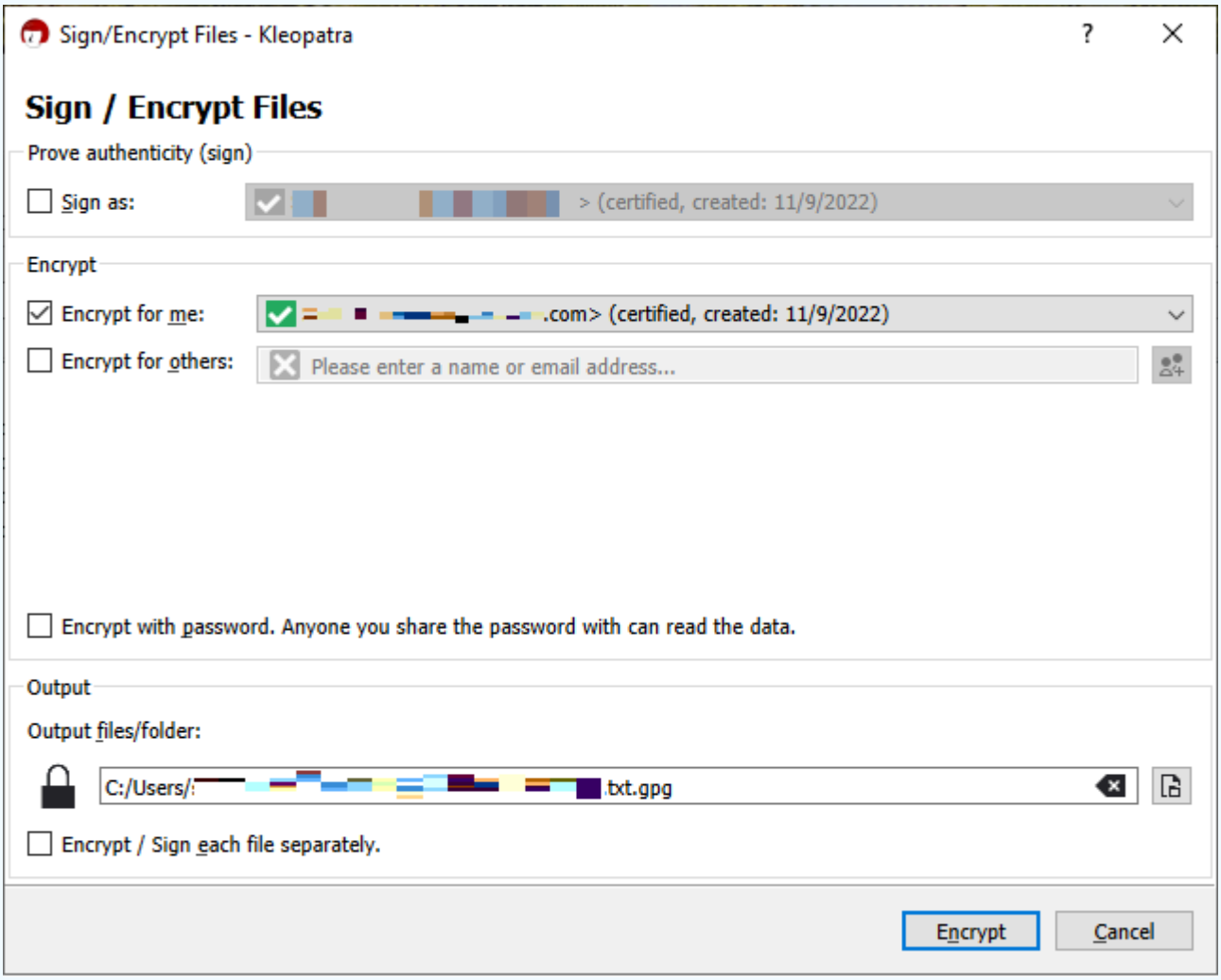
Client PGP supportati

I seguenti client sono stati testati con Transfer Family e possono essere utilizzati per generare chiavi PGP e per crittografare i file che si intende decrittografare con un flusso di lavoro.

- GPG4win+ Kleopatra.

Note

Quando selezioni Firma/Crittografa i file, assicurati di deselezionare l'opzione Sign as: attualmente non supportiamo la firma per i file criptati.



Se firmi il file crittografato e tenti di caricarlo su un server Transfer Family con un flusso di lavoro di decrittografia, ricevi il seguente errore:

```
Encrypted file with signed message unsupported
```

- Principali versioni di GnuPG: 2.4, 2.3, 2.2, 2.0 e 1.4.

Nota che potrebbero funzionare anche altri client PGP, ma solo i client qui menzionati sono stati testati con Transfer Family.

Gestione delle identità e degli accessi per AWS Transfer Family

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS Transfer Family IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS Transfer Family svolgi.

Utente del servizio: se utilizzi il AWS Transfer Family servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS Transfer Family funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS Transfer Family, consulta Risoluzione dei problemi di AWS Transfer Family identità e accesso.

Amministratore del servizio: se sei responsabile delle AWS Transfer Family risorse della tua azienda, probabilmente hai pieno accesso a AWS Transfer Family. È tuo compito determinare a quali AWS Transfer Family funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AWS Transfer Family, consultaCome AWS Transfer Family funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS Transfer Family. Per visualizzare esempi di policy AWS Transfer Family basate sull'identità che puoi utilizzare in IAM, consulta. AWS Transfer Family esempi di politiche basate sull'identità

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

Utente root dell'account AWS

Quando ne crei un Account AWS, inizi con un'unica identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account.

Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli

utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La

maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire

da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come AWS Transfer Family funziona con IAM

Prima di utilizzare AWS Identity and Access Management (IAM) per gestire l'accesso a AWS Transfer Family, è necessario comprendere con quali funzionalità IAM è disponibile l'uso AWS Transfer Family. Per avere una visione di alto livello di come AWS Transfer Family e altri AWS servizi funzionano con IAM, consulta AWS i servizi che funzionano con IAM nella Guida per l'utente IAM.

Argomenti

- Policy AWS Transfer Family basate su identità
- Policy di AWS Transfer Family basate sulle risorse
- Autorizzazione basata su tag AWS Transfer Family
- AWS Transfer Family Ruoli IAM

Policy AWS Transfer Family basate su identità

Con le policy basate su identità IAM, puoi specificare operazioni e risorse consentite o rifiutate, nonché le condizioni in base alle quali le operazioni sono consentite o rifiutate. AWS Transfer Family supporta operazioni, risorse e chiavi di condizione specifiche. Per conoscere tutti gli elementi che usi in una policy JSON, consulta il riferimento agli elementi della policy JSON di IAM nella Guida per l'AWS Identity and Access Management utente.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione

AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le azioni politiche AWS Transfer Family utilizzano il seguente prefisso prima dell'azione:`transfer:`. Ad esempio, per concedere a qualcuno l'autorizzazione a creare un server, con l'operazione Transfer Family `CreateServer` API, includi l'`transfer:CreateServer`azione nella sua politica. Le istruzioni delle policy devono includere un elemento `Action` o `NotAction`. AWS Transfer Family definisce un proprio set di operazioni che descrivono le attività che puoi eseguire con questo servizio.

Per specificare più operazioni in una singola istruzione, separarle con una virgola come mostrato di seguito.

```
"Action": [
      "transfer:action1",
      "transfer:action2"
```

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Describe`, includi la seguente operazione.

```
"Action": "transfer:Describe*"
```

Per visualizzare un elenco di AWS Transfer Family azioni, consulta Azioni definite da AWS Transfer Family nel Service Authorization Reference.

Risorse

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

La risorsa del server Transfer Family ha il seguente ARN.

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

Ad esempio, per specificare il server `s-01234567890abcdef` Transfer Family nella dichiarazione, utilizzare il seguente ARN.

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Names (ARNs) nel Service Authorization Reference o IAM ARNs nella IAM User Guide.

Per specificare tutte le istanze database che appartengono a un account specifico, utilizza il carattere jolly (*).

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/*"
```

Alcune AWS Transfer Family azioni vengono eseguite su più risorse, come quelle utilizzate nelle policy IAM. In questi casi, è necessario utilizzare il carattere jolly (*).

```
"Resource": "arn:aws:transfer:*:123456789012:server/*"
```

In alcuni casi è necessario specificare più di un tipo di risorsa, ad esempio se si crea una politica che consente l'accesso ai server e agli utenti di Transfer Family. Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

```
"Resource": [
      "resource1",
      "resource2"
            ]
```

Per visualizzare un elenco di AWS Transfer Family risorse, vedere Tipi di risorse definiti da AWS Transfer Family nel Service Authorization Reference.

Chiavi di condizione

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

AWS Transfer Family definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare un elenco di chiavi di AWS Transfer Family condizione, vedere Condition keys for AWS Transfer Family nel Service Authorization Reference.

Esempi

Per visualizzare esempi di politiche AWS Transfer Family basate sull'identità, vedere. AWS Transfer Family esempi di politiche basate sull'identità

Policy di AWS Transfer Family basate sulle risorse

Le politiche basate sulle risorse sono documenti di policy JSON che specificano quali azioni uno specifico principale può eseguire sulla risorsa e in quali condizioni. AWS Transfer Family *Amazon S3 supporta politiche di autorizzazione basate sulle risorse per i bucket Amazon S3.* Le policy basate su risorse consentono di concedere l'autorizzazione all'utilizzo ad altri

account per ogni risorsa. *Puoi anche utilizzare una policy basata sulle risorse per consentire a un AWS servizio di accedere ai tuoi bucket Amazon S3.*

Per consentire l'accesso a più account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata su risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa si trovano in AWS account diversi, devi inoltre concedere all'entità principale l'autorizzazione ad accedere alla risorsa. Concedi l'autorizzazione collegando una policy basata sull'identità all'entità. Tuttavia, se una policy basata su risorse concede l'accesso a un'entità principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta In che modo i ruoli IAM differiscono dalle politiche basate sulle risorse nella Guida per l'AWS Identity and Access Management utente.

Il servizio Amazon S3 supporta solo un tipo di policy basata sulle risorse chiamata bucket policy, che è collegata a un bucket. Questa policy definisce quali entità principali (account, utenti, ruoli e utenti federati) possono eseguire azioni sull'oggetto.

Esempi

Per visualizzare esempi di politiche AWS Transfer Family basate sulle risorse, vedere. AWS Transfer Family esempi di policy basate su tag

Autorizzazione basata su tag AWS Transfer Family

È possibile allegare tag alle AWS Transfer Family risorse o passare tag in una richiesta a. AWS Transfer Family Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `transfer:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`. Per informazioni su come utilizzare i tag per controllare l'accesso alle AWS Transfer Family risorse, consultaAWS Transfer Family esempi di policy basate su tag.

AWS Transfer Family Ruoli IAM

Un ruolo IAM è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con AWS Transfer Family

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo GetFederation Token.

AWS Transfer Family supporta l'utilizzo di credenziali temporanee.

AWS Transfer Family esempi di politiche basate sull'identità

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse AWS Transfer Family . Inoltre, non possono eseguire attività utilizzando l'API AWS Management Console AWS CLI, o. AWS Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi collegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

Per scoprire come creare una policy basata sull'identità IAM utilizzando questi esempi di documenti di policy JSON, consulta Creazione di policy nella scheda JSON nella Guida per l'utente.AWS Identity and Access Management

Argomenti

- Best practice per le policy
- Utilizzo della console di AWS Transfer Family
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse nel tuo account. AWS Transfer Family Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console di AWS Transfer Family

Per accedere alla AWS Transfer Family console, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle AWS Transfer Family risorse del tuo AWS account. Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti e ruoli IAM) associate a tale policy. Per ulteriori informazioni, consulta Aggiungere autorizzazioni a un utente nella Guida per l'AWS Identity and Access Management utente.

Non è necessario consentire autorizzazioni minime di console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, puoi accedere solo alle operazioni che soddisfano l'operazione API che stai cercando di eseguire.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica

include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI 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 esempi di policy basate su tag

Di seguito sono riportati alcuni esempi di come controllare l'accesso alle AWS Transfer Family risorse in base ai tag.

Utilizzo dei tag per controllare l'accesso alle risorse AWS Transfer Family

Le condizioni nelle policy IAM fanno parte della sintassi utilizzata per specificare le autorizzazioni alle AWS Transfer Family risorse. Puoi controllare l'accesso alle AWS Transfer Family risorse (come utenti, server, ruoli e altre entità) in base ai tag presenti su tali risorse. I tag sono coppie chiave-valore. Per ulteriori informazioni sull'etichettatura delle risorse, consulta Tagging AWS resources in. Riferimenti generali di AWS

Nel AWS Transfer Family, le risorse possono avere tag e alcune azioni possono includere tag. Quando si crea una policy IAM, è possibile utilizzare le chiavi di condizione di tag per controllare:

- Quali utenti possono eseguire azioni su una AWS Transfer Family risorsa, in base ai tag presenti nella risorsa.
- Quali tag possono essere passati in una richiesta di operazione;
- Se delle chiavi di tag specifiche possono essere utilizzate in una richiesta.

Utilizzando il controllo degli accessi basato su tag, puoi applicare un controllo più preciso rispetto a livello di API. È inoltre possibile applicare un controllo più dinamico rispetto al controllo degli accessi basato sulle risorse. Puoi creare policy IAM che consentano o rifiutino un'operazione in base ai tag forniti nella richiesta (tag di richiesta). Puoi anche creare policy IAM basate su tag sulla risorsa su cui viene gestita (tag di risorsa). In generale, i tag di risorsa sono per i tag che sono già presenti sulle risorse, i tag di richiesta servono per aggiungere o rimuovere tag da una risorsa.

Per la sintassi e la semantica complete delle chiavi di condizione dei tag, consulta Controlling access to AWS resources using resource tags nella IAM User Guide. Per dettagli sulla specificazione delle policy IAM con API Gateway, consulta Controllare l'accesso a un'API con autorizzazioni IAM nella API Gateway Developer Guide.

Esempio 1: nega le azioni basate sui tag delle risorse

Puoi negare l'esecuzione di un'azione su una risorsa in base ai tag. La politica di esempio seguente nega`TagResource`,`UntagResource`, `StartServer` `StopServer`e `DescribeServer`, e `DescribeUser` le operazioni se la risorsa utente o del server è contrassegnata con la chiave `stage` e il valore. `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"
                }
            }
        }
    ]
}
```

Esempio 2: consentire azioni basate sui tag delle risorse

Puoi consentire l'esecuzione di un'azione su una risorsa in base ai tag. La seguente politica di esempio consente `TagResourceUntagResource`,`StartServer`, `StopServerDescribeServer`, e `DescribeUser` operazioni se la risorsa utente o del server è contrassegnata con la chiave `stage` e il valore`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"
                }
            }
        }
    ]
}
```

Esempio 3: nega la creazione di un utente o di un server in base ai tag di richiesta

La seguente politica di esempio contiene due istruzioni. La prima istruzione nega l'`CreateServer`operazione su tutte le risorse se la chiave del centro di costo per il tag non ha un valore.

La seconda istruzione nega l'`CreateServer`operazione se la chiave del centro di costo per il tag contiene qualsiasi altro valore oltre a 1, 2 o 3.

> **Note**
>
> Questa politica consente di creare o eliminare una risorsa che contiene una chiave chiamata `costcenter` e un valore di 12, 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"
                    ]
                }
            }
        }
    ]
}
```

Risoluzione dei problemi di AWS Transfer Family identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS Transfer Family un IAM.

Argomenti

- Non sono autorizzato a eseguire alcuna azione in AWS Transfer Family
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS Transfer Family risorse

Non sono autorizzato a eseguire alcuna azione in AWS Transfer Family

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` cerca di utilizzare la console per visualizzare i dettagli relativi a un *`widget`* ma non dispone di autorizzazioni `transfer:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 transfer:GetWidget on resource: my-example-widget
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le sue policy per poter accedere alla risorsa *my-example-widget* utilizzando l'operazione `transfer;:GetWidget`.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS Transfer Family.

Alcuni Servizi AWS consentono di passare un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS Transfer Family. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

La seguente politica di esempio contiene l'autorizzazione a passare un ruolo a AWS Transfer Family.

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

Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS Transfer Family risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Transfer Family supporta queste funzionalità, consultaCome AWS Transfer Family funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Convalida della conformità per AWS Transfer Family

I revisori di terze parti valutano la sicurezza e la conformità nell' AWS Transfer Family ambito di più programmi di AWS conformità. Sono inclusi SOC, PCI e HIPAA. Per l'elenco completo, consulta AWS Services in Scope by Compliance Program.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, consulta la sezione AWS Servizi rientranti nell'ambito del programma di conformità. Per informazioni generali, consultare Programmi per la conformità di AWS.

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact.

La vostra responsabilità di conformità durante l'utilizzo AWS Transfer Family è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- Whitepaper sull'architettura per la sicurezza e la conformità HIPAA: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi allo standard HIPAA. AWS
- Risorse per la conformità di AWS: questa raccolta di workbook e guide potrebbe essere utile al tuo settore e alla tua posizione.
- AWS Config— Questo AWS servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente AWS di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza in AWS Transfer Family

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

AWS Transfer Family supporta fino a 3 zone di disponibilità ed è supportato da una flotta ridondante con scalabilità automatica per le richieste di connessione e trasferimento.

Tieni presente quanto segue:

- Per gli endpoint pubblici:
  - La ridondanza a livello di zona di disponibilità è integrata nel servizio
  - Esistono flotte ridondanti per ogni AZ.
  - Questa ridondanza viene fornita automaticamente

- Per gli endpoint in un Virtual Private Cloud (VPC), vedi. Crea un server in un cloud privato virtuale

Consulta anche

- Per ulteriori informazioni sulle Regioni AWS zone di disponibilità, consulta l'infrastruttura AWS globale.
- Per un esempio su come creare una maggiore ridondanza e ridurre al minimo la latenza di rete utilizzando il routing basato sulla latenza, consulta il post sul blog Minimizza la latenza di rete con i server. AWS Transfer Family

Sicurezza dell'infrastruttura in AWS Transfer Family

In quanto servizio gestito, AWS Transfer Family è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS Transfer Family attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Aggiungi un firewall per applicazioni Web

AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le API dagli attacchi. È possibile utilizzarlo per configurare una serie di regole note come elenco di controllo degli accessi Web (Web ACL) che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. Per ulteriori informazioni, consulta Utilizzare AWS WAF per proteggere le API.

Per aggiungere AWS WAF

1. Aprire la console Gateway API all'indirizzo https://console.aws.amazon.com/apigateway/.
2. Nel riquadro di navigazione delle API, quindi scegli il modello di provider di identità personalizzato.
3. Scegliere Stages (Fasi).
4. Nel riquadro Stages (Fasi), selezionare il nome della fase.
5. Nel riquadro Stage Editor(Editor fasi) scegliere la scheda Settings (Impostazioni).
6. Esegui una di queste operazioni:

   - In Web Application Firewall (WAF), per Web ACL, scegli l'ACL Web che desideri associare a questa fase.
   - Se l'ACL Web di cui hai bisogno non esiste, dovrai crearne uno effettuando le seguenti operazioni:

     1. Scegli Crea ACL Web.
     2. Nella home page del servizio AWS WAF, scegli Crea ACL web.
     3. Nei dettagli dell'ACL Web, in Nome, digita il nome dell'ACL Web.
     4. In Regole, scegli Aggiungi regole, quindi scegli Aggiungi le mie regole e i miei gruppi di regole.
     5. Per Tipo di regola, scegli IP set per identificare un elenco specifico di indirizzi IP.
     6. Per Regola, inserisci il nome della regola.
     7. Per il set IP, scegliete un set IP esistente. Per creare un set IP, vedere Creazione di un set IP.
     8. Per utilizzare l'indirizzo IP come indirizzo di origine, scegli l'indirizzo IP nell'intestazione.
     9. Per il nome del campo Header, immettere. `SourceIP`
     10. Per Posizione all'interno dell'intestazione, scegli Primo indirizzo IP.
     11. Per Fallback for missing IP address, scegli Match o No Match a seconda di come desideri gestire un indirizzo IP non valido (o mancante) nell'intestazione.
     12. Per Azione, scegli l'azione del set IP.
     13. Per l'azione ACL web predefinita per le richieste che non corrispondono a nessuna regola, scegli Consenti o Blocca, quindi fai clic su Avanti.
     14. Per i passaggi 4 e 5, scegli Avanti.
     15. In Rivedi e crea, esamina le tue scelte, quindi scegli Crea ACL web.

7. Seleziona Salva modifiche.
8. Scegliere Resources (Risorse).
9. Per Azioni, scegli Deploy API.

Per informazioni sulla sicurezza AWS Transfer Family con il firewall delle applicazioni AWS Web, consulta Securing AWS Transfer Family with AWS Application Firewall e Amazon API Gateway nel blog sullo AWS storage.

Prevenzione del problema "confused deputy" tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione tra servizi può portare al confuso problema del sostituto. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio di chiamata può essere manipolato in modo da utilizzare le sue autorizzazioni per agire sulle risorse di un altro cliente in un modo a cui altrimenti non dovrebbe avere l'autorizzazione di accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account. Per una descrizione dettagliata di questo problema, consulta il confuso problema secondario nella Guida per l'utente di IAM.

Ti consigliamo di utilizzare `aws:SourceArn`le chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche delle risorse per limitare le autorizzazioni di cui AWS Transfer Family dispone per la risorsa. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` devono utilizzare lo stesso ID account nella stessa istruzione di policy.

Il modo più efficace per proteggersi dal problema "confused deputy" è utilizzare il nome della risorsa Amazon (ARN) esatto della risorsa che vuoi autorizzare. Se state specificando più risorse, utilizzate la chiave di condizione di contesto `aws:SourceArn` globale con caratteri jolly (`*`) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:transfer::`*`region`*`::`*`account-id`*`:server/*`.

AWS Transfer Family utilizza i seguenti tipi di ruoli:

- Ruolo utente: consente agli utenti gestiti dal servizio di accedere alle risorse Transfer Family necessarie. AWS Transfer Family assume questo ruolo nel contesto dell'ARN di un utente Transfer Family.

- Ruolo di accesso: fornisce l'accesso solo ai file Amazon S3 che vengono trasferiti. Per i trasferimenti AS2 in entrata, il ruolo di accesso utilizza l'Amazon Resource Name (ARN) per l'accordo. Per i trasferimenti AS2 in uscita, il ruolo di accesso utilizza l'ARN per il connettore.
- Ruolo di chiamata: da utilizzare con Amazon API Gateway come provider di identità personalizzato del server. Transfer Family assume questo ruolo nel contesto di un ARN del server Transfer Family.
- Ruolo di registrazione: utilizzato per registrare le voci in Amazon CloudWatch. Transfer Family utilizza questo ruolo per registrare i dettagli relativi al successo e all'errore insieme alle informazioni sui trasferimenti di file. Transfer Family assume questo ruolo nel contesto di un ARN del server Transfer Family. Per i trasferimenti AS2 in uscita, il ruolo di registrazione utilizza il connettore ARN.
- Ruolo di esecuzione: consente a un utente Transfer Family di chiamare e avviare flussi di lavoro. Transfer Family assume questo ruolo nel contesto di un flusso di lavoro Transfer Family ARN.

Per ulteriori informazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM .

> **Note**
>
> Negli esempi seguenti, sostituire ogni *`segnaposto dell'input utente`* con le proprie informazioni.

> **Note**
>
> Nei nostri esempi, utilizziamo entrambi `ArnLike` e. `ArnEquals` Sono identici dal punto di vista funzionale e pertanto è possibile utilizzarli entrambi quando si creano le proprie politiche. La documentazione di Transfer Family utilizza `ArnLike` quando la condizione contiene un carattere jolly e `ArnEquals` indica una condizione di corrispondenza esatta.

AWS Transfer Family, ruolo utente, prevenzione confusa tra diversi servizi

La seguente politica di esempio consente a qualsiasi utente di qualsiasi server dell'account di assumere il ruolo.

```
{
    "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/*"
                }
            }
        }
    ]
}
```

La seguente politica di esempio consente a qualsiasi utente di un server specifico di assumere il ruolo.

```
{
    "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/*"
                }
            }
        }
    ]
```

```
}
```

La seguente politica di esempio consente a un utente specifico di un server specifico di assumere il ruolo.

```
{
    "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 Transfer Family, ruolo del flusso di lavoro, prevenzione confusa tra diversi servizi

La seguente politica di esempio consente a qualsiasi flusso di lavoro dell'account di assumere il ruolo.

```
{
    "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 seguente politica di esempio consente a un flusso di lavoro specifico di assumere il ruolo.

```
{
    "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, ruolo di registrazione e invocazione, prevenzione confusa tra diversi servizi

> **Note**
>
> I seguenti esempi possono essere utilizzati sia nei ruoli di registrazione che di invocazione. In questi esempi, puoi rimuovere i dettagli ARN per un flusso di lavoro se al server non è collegato alcun flusso di lavoro.

Il seguente esempio di politica di registrazione/invocazione consente a qualsiasi server (e flusso di lavoro) dell'account di assumere il ruolo.

```
{
    "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/*"
                   ]
                }
            }
        }
    ]
}
```

Il seguente esempio di politica di registrazione/invocazione consente a un server (e a un flusso di lavoro) specifici di assumere il ruolo.

```
{
    "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 politiche gestite per AWS Transfer Family

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite che scrivere le politiche da soli. Ci vogliono tempo ed esperienza per creare policy gestite dai clienti AWS Identity and Access Management (IAM) che forniscano al team solo le autorizzazioni di cui ha bisogno. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy gestite da AWS , consulta Policy gestite da AWS nella Guida per l'utente di IAM. Per un elenco dettagliato di tutte le policy AWS gestite, consulta la guida di riferimento per le policy AWS gestite.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy `ReadOnlyAccess` AWS gestita fornisce l'accesso in sola lettura a tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: AWSTransferConsoleFullAccess

La `AWSTransferConsoleFullAccess` politica fornisce l'accesso completo a Transfer Family tramite la console di AWS gestione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `acm:ListCertificates`— Concede l'autorizzazione a recuperare un elenco del certificato Amazon Resource Names (ARNs) e il nome di dominio per ogni ARN.
- `ec2:DescribeAddresses`— Concede l'autorizzazione a descrivere uno o più indirizzi IP elastici.
- `ec2:DescribeAvailabilityZones`— Concede l'autorizzazione a descrivere una o più zone di disponibilità disponibili.
- `ec2:DescribeNetworkInterfaces`— Concede l'autorizzazione a descrivere una o più interfacce di rete elastiche.
- `ec2:DescribeSecurityGroups`— Concede l'autorizzazione a descrivere uno o più gruppi di sicurezza.
- `ec2:DescribeSubnets`— Concede l'autorizzazione a descrivere una o più sottoreti.
- `ec2:DescribeVpcs`— Concede l'autorizzazione a descrivere uno o più cloud privati virtuali (VPC).
- `ec2:DescribeVpcEndpoints`— Concede l'autorizzazione a descrivere uno o più endpoint VPC.
- `health:DescribeEventAggregates`— Restituisce il numero di eventi di ogni tipo di evento (problema, modifica pianificata e notifica all'account).
- `iam:GetPolicyVersion`— Concede l'autorizzazione a recuperare informazioni su una versione della politica gestita specificata, incluso il documento relativo alla policy.
- `iam:ListPolicies`— Concede l'autorizzazione a elencare tutte le politiche gestite.
- `iam:ListRoles`— Concede l'autorizzazione a elencare i ruoli IAM con il prefisso di percorso specificato.
- `iam:PassRole`— Concede l'autorizzazione a trasferire un ruolo IAM a Transfer Family. Per maggiori dettagli, consulta Concedere a un utente le autorizzazioni per passare un ruolo a un Servizio AWS.
- `route53:ListHostedZones`— Concede l'autorizzazione per ottenere un elenco delle zone ospitate pubbliche e private associate all'attuale. Account AWS

- `s3:ListAllMyBuckets`— Concede l'autorizzazione a elencare tutti i bucket di proprietà del mittente autenticato della richiesta.
- `transfer:*`— Garantisce l'accesso alle risorse di Transfer Family. L'asterisco (*) consente l'accesso a tutte le risorse.

```
{
    "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 politica gestita: AWSTransferFullAccess

La `AWSTransferFullAccess` politica offre l'accesso completo ai servizi Transfer Family.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `transfer:*`— Concede il permesso di accedere alle risorse di Transfer Family. L'asterisco (*) consente l'accesso a tutte le risorse.
- `iam:PassRole`— Concede l'autorizzazione a trasferire un ruolo IAM a Transfer Family. Per maggiori dettagli, consulta Concedere a un utente le autorizzazioni per passare un ruolo a un Servizio AWS.
- `ec2:DescribeAddresses`— Concede l'autorizzazione a descrivere uno o più indirizzi IP elastici.
- `ec2:DescribeNetworkInterfaces`— Concede l'autorizzazione a descrivere una o più interfacce di rete.
- `ec2:DescribeVpcEndpoints`— Concede l'autorizzazione a descrivere uno o più endpoint 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 politica gestita: AWSTransferLoggingAccess

La `AWSTransferLoggingAccess` politica concede a AWS Transfer Family l'accesso completo per creare flussi e gruppi di log e inserire eventi di registro nel tuo account.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni per. Amazon CloudWatch Logs

- `CreateLogStream`— Concede le autorizzazioni ai responsabili per creare un flusso di log.
- `DescribeLogStreams`— Concede le autorizzazioni ai principali per elencare i flussi di log per il gruppo di log.
- `CreateLogGroup`— Concede le autorizzazioni ai responsabili per creare gruppi di log.
- `PutLogEvents`— Concede le autorizzazioni ai principali per caricare un batch di eventi di registro in un flusso di log.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politica gestita: AWSTransferReadOnlyAccess

La `AWSTransferReadOnlyAccess` politica fornisce l'accesso in sola lettura ai servizi Transfer Family.

Dettagli dell'autorizzazione

Questa politica include le seguenti autorizzazioni per Transfer Family.

- `DescribeUser`— Concede ai mandanti le autorizzazioni per visualizzare le descrizioni per gli utenti.
- `DescribeServer`— Concede le autorizzazioni ai principali per visualizzare le descrizioni dei server.
- `ListUsers`— Concede le autorizzazioni ai principali per elencare gli utenti di un server.
- `ListServers`— Concede i permessi ai principali per elencare i server dell'account.
- `TestIdentityProvider`— Concede le autorizzazioni ai responsabili per verificare se il provider di identità configurato è configurato correttamente.
- `ListTagsForResource`— Concede le autorizzazioni ai responsabili per elencare i tag di una risorsa.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "transfer:DescribeUser",
                "transfer:DescribeServer",
                "transfer:ListUsers",
                "transfer:ListServers",
                "transfer:TestIdentityProvider",
                "transfer:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Trasferisci gli aggiornamenti di Transfer Family alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per AWS Transfer Family da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina Cronologia dei documenti per AWS Transfer Family.

Modifica	Descrizione	Data
Aggiornamento della documentazione	Sono state aggiunte sezioni per ciascuna delle politiche gestite da Transfer Family.	27 gennaio 2022
AWSTransferReadOnlyAccess: aggiornamento a una policy esistente	AWS Transfer Family ha aggiunto nuove autorizzazioni per consentire la lettura AWS Managed Microsoft AD della politica.	30 settembre 2021
AWS Transfer Family ha iniziato a tenere traccia delle modifiche	AWS Transfer Family ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	15 giugno 2021

Risoluzione dei problemi AWS Transfer Family

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con. AWS Transfer Family

Per problemi con IAM in Transfer Family, consultaRisoluzione dei problemi di AWS Transfer Family identità e accesso.

Argomenti

Risolvi i problemi relativi agli utenti gestiti dal servizio

Questa sezione descrive le possibili soluzioni per i seguenti problemi.

Argomenti

Risolvi i problemi relativi agli utenti gestiti dal servizio Amazon EFS

Descrizione

Esegui il `sftp` comando e il prompt non viene visualizzato, ma viene visualizzato il seguente messaggio:

```
Couldn't canonicalize: Permission denied
           Need cwd
```

Causa

Il ruolo del tuo utente AWS Identity and Access Management (IAM) non è autorizzato ad accedere ad Amazon Elastic File System (Amazon EFS).

Soluzione

Aumenta le autorizzazioni relative alle policy per il ruolo del tuo utente. Puoi aggiungere una policy AWS gestita, ad esempio`AmazonElasticFileSystemClientFullAccess`.

Risolvi i problemi relativi al corpo della chiave pubblica per un periodo troppo lungo

Descrizione

Quando si tenta di creare un utente gestito dal servizio, viene visualizzato il seguente errore:

```
Failed to create user (1 validation error detected:
'sshPublicKeyBody' failed to satisfy constraint: Member must have length less than or
 equal to 2048)
```

Causa

È possibile che stiate inserendo una chiave PGP per il corpo della chiave pubblica e che AWS Transfer Family non supporti le chiavi PGP per gli utenti gestiti dal servizio.

Soluzione

Se la chiave PGP è basata su RSA, è possibile convertirla in formato PEM. Ad esempio, Ubuntu fornisce uno strumento di conversione qui: https://manpages.ubuntu.com/manpages/xenial/man1/openpgp2ssh.1.html

Risoluzione dei problemi: impossibile aggiungere la chiave pubblica SSH

Descrizione

Quando si tenta di aggiungere una chiave pubblica per un utente gestito dal servizio, viene visualizzato il seguente errore:

```
Failed to add SSH public key (Unsupported or invalid SSH public key format)
```

Causa

È possibile che si stia tentando di importare una chiave pubblica in formato SSH2 e che AWS Transfer Family non supporti le chiavi pubbliche in formato SSH2 per gli utenti gestiti dal servizio.

Soluzione

È necessario convertire la chiave in formato OpenSSH. Questo processo è descritto in. Convertire una chiave pubblica SSH2 in formato PEM

Risolvi i problemi relativi ad Amazon API Gateway

Questa sezione descrive le possibili soluzioni per i seguenti problemi di API Gateway.

Argomenti

Troppi errori di autenticazione

Descrizione

Quando si tenta di connettersi al server utilizzando Secure Shell (SSH) File Transfer Protocol (SFTP), viene visualizzato il seguente errore:

```
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

È possibile che tu abbia inserito una password errata per il tuo utente. Riprova a inserire la password corretta.

Se la password è corretta, il problema potrebbe essere causato da un ruolo Amazon Resource Name (ARN) non valido. Per confermare che si tratta del problema, verifica il provider di identità del tuo server. Se viene visualizzata una risposta simile alla seguente, il ruolo ARN è solo un segnaposto, come indicato dal valore ID del ruolo di tutti gli zeri:

```
{
    "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"
}
```

Soluzione

Sostituisci il ruolo segnaposto ARN con un ruolo effettivo che dispone dell'autorizzazione per accedere al server.

Per aggiornare il ruolo

1. Apri la AWS CloudFormation console all'indirizzo https://console.aws.amazon.com/cloudformation.
2. Nel riquadro di navigazione a sinistra, selezionare Stacks (Stack).
3. Nell'elenco Stack, scegli il tuo stack, quindi scegli la scheda Parametri.
4. Scegli Aggiorna. Nella pagina Aggiorna stack, scegli Usa il modello corrente, quindi scegli Avanti.
5. Sostituiscilo UserRoleArncon un ruolo ARN con autorizzazioni sufficienti per accedere al tuo server Transfer Family.

> **Note**
>
> Per concedere le autorizzazioni necessarie, puoi aggiungere le politiche `AmazonAPIGatewayAdministrator` `AmazonS3FullAccess` gestite al tuo ruolo.

6. Scegli Avanti, quindi scegli nuovamente Avanti. Nella pagina Review ***stack***, seleziona Riconosco che AWS CloudFormation potrebbe creare risorse IAM, quindi scegli Update stack.

Connessione chiusa

Descrizione

Quando si tenta di connettersi al server utilizzando Secure Shell (SSH) File Transfer Protocol (SFTP), viene visualizzato il seguente errore:

```
Connection closed
```

Causa

Una possibile causa di questo problema è che il tuo ruolo di CloudWatch registrazione di Amazon non ha una relazione di fiducia con Transfer Family.

Soluzione

Assicurati che il ruolo di registrazione del server abbia una relazione di fiducia con Transfer Family. Per ulteriori informazioni, consulta Per stabilire una relazione di trust.

Risolvi i problemi relativi alle politiche per i bucket Amazon S3 crittografati

Descrizione

Hai un bucket Amazon S3 crittografato che stai utilizzando come storage per il tuo server Transfer Family. Se provi a caricare un file sul server, ricevi l'errore. `Couldn't close file: Permission denied`

Inoltre, se si visualizzano i log del server, vengono visualizzati i seguenti errori:

```
ERROR Message="Access denied" Operation=CLOSE Path=/bucket/user/test.txt BytesIn=13
ERROR Message="Access denied"
```

Causa

La policy per il tuo utente IAM non dispone dell'autorizzazione per accedere al bucket crittografato.

Soluzione

Devi specificare autorizzazioni aggiuntive nella tua policy per concedere le autorizzazioni richieste AWS Key Management Service (AWS KMS). Per informazioni dettagliate, vedi Crittografia dei dati in Amazon S3.

Risolvi i problemi di autenticazione

Questa sezione descrive le possibili soluzioni per i seguenti problemi di autenticazione.

Argomenti

- Errori di autenticazione: SSH/SFTP
- Problema relativo ai realms non corrispondenti di AD gestito
- Problemi di autenticazione vari

Errori di autenticazione: SSH/SFTP

Descrizione

Quando tenti di connetterti al server utilizzando Secure Shell (SSH) File Transfer Protocol (SFTP), ricevi un messaggio simile al seguente:

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
  Authentication failed.
```

> **Note**
>
> Se utilizzi un API Gateway e ricevi questo errore, consultaTroppi errori di autenticazione.

Causa

Non hai aggiunto una coppia di key pair RSA per il tuo utente, quindi devi invece autenticarti utilizzando una password.

Soluzione

Quando esegui il `sftp` comando, specifica l'`-o PubkeyAuthentication=no`opzione. Questa opzione impone al sistema di richiedere la password. Per esempio:

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

Problema relativo ai realms non corrispondenti di AD gestito

Descrizione

Il realm di un utente e il relativo realm di gruppo devono corrispondere. Devono essere entrambi nell'area di default oppure devono trovarsi entrambe nell'area di fiducia.

Causa

Se un utente e il relativo gruppo non coincidono, l'utente non può essere autenticato da Transfer Family. Se si esegue il test del provider di identità dell'utente, viene visualizzato l'errore Nessun accesso associato trovato per i gruppi di utenti.

Soluzione

Fai riferimento a un gruppo nell'area dell'utente che corrisponde all'area di autenticazione del gruppo (impostazione predefinita o affidabile).

Problemi di autenticazione vari

Descrizione

Viene visualizzato un errore di autenticazione e nessuna delle altre soluzioni di risoluzione dei problemi funziona

Causa

È possibile che sia stata specificata una destinazione per una directory logica che contiene una barra iniziale o finale (/).

Soluzione

Aggiorna la destinazione della directory logica, per assicurarti che inizi con una barra e non contenga una barra finale. Ad esempio, `/DOC-EXAMPLE-BUCKET/images` è accettabile, ma non lo `DOC-EXAMPLE-BUCKET/images` è. `/DOC-EXAMPLE-BUCKET/images/`

Risolvi i problemi relativi ai flussi di lavoro gestiti

Questa sezione descrive le possibili soluzioni per i seguenti problemi di flusso di lavoro.

Argomenti

Risolvi gli errori relativi al flusso di lavoro utilizzando Amazon CloudWatch

Descrizione

Se riscontri problemi con i flussi di lavoro, puoi utilizzare Amazon CloudWatch per indagare sulla causa.

Causa

Le cause possono essere diverse. Usa Amazon CloudWatch Logs per indagare.

Soluzione

Transfer Family emette lo stato di esecuzione del flusso di lavoro in CloudWatch Logs. Nei CloudWatch registri possono comparire i seguenti tipi di errori del flusso di lavoro:

- `"type": "StepErrored"`
- `"type": "ExecutionErrored"`
- `"type": "ExecutionThrottled"`
- `"Service failure on starting workflow"`

È possibile filtrare i registri di esecuzione del flusso di lavoro utilizzando diverse sintassi di filtri e pattern. Ad esempio, è possibile creare un filtro di registro nei registri per acquisire CloudWatch i registri di esecuzione del flusso di lavoro che contengono il messaggio. ExecutionErrored Per maggiori dettagli, consulta Elaborazione in tempo reale dei dati di log con abbonamenti e sintassi di filtri e pattern nella Amazon CloudWatch Logs User Guide.

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"}
```

Qui `StepErrored` indica che una fase del flusso di lavoro ha generato un errore. In un unico flusso di lavoro, è possibile configurare più passaggi. Questo errore indica in quale fase si è verificato l'errore e fornisce un messaggio di errore. In questo particolare esempio, la fase è stata configurata per etichettare un file; tuttavia, l'etichettatura di un file in un file system Amazon EFS non è supportata, quindi la fase ha generato un errore.

ExecutionErrored

```
2021-10-29T12:57:26.618-05:00
            {"type":"ExecutionErrored","details":{},"workflowId":"w-w-
abcdef01234567890",
            "executionId":"1234abcd-56ef-78gh-90ij-1234klmno567","transferDetails":
{"serverId":"s-1234567890abcdef0",
            "username":"lhr","sessionId":"1234567890abcdef0"}}
```

Quando un flusso di lavoro non è in grado di eseguire alcun passaggio, genera un `ExecutionErrored` messaggio. Ad esempio, se è stato configurato un singolo passaggio in un determinato flusso di lavoro e se il passaggio non può essere eseguito, l'intero flusso di lavoro ha esito negativo.

Esecuzione limitata

L'esecuzione viene limitata se un flusso di lavoro viene attivato a una velocità superiore a quella supportata dal sistema. Questo messaggio di registro indica che è necessario rallentare la velocità di esecuzione dei flussi di lavoro. Se non riesci a ridurre la velocità di esecuzione del flusso di lavoro, contatta Contact. AWS SupportAWS

Errore di servizio all'avvio del flusso di lavoro

Ogni volta che si rimuove un flusso di lavoro da un server e lo si sostituisce con uno nuovo o si aggiorna la configurazione del server (il che influisce sul ruolo di esecuzione di un flusso di lavoro), è necessario attendere circa 10 minuti prima di eseguire il nuovo flusso di lavoro. Il server

Transfer Family memorizza nella cache i dettagli del flusso di lavoro e il server impiega 10 minuti per aggiornare la cache.

Inoltre, è necessario disconnettersi da tutte le sessioni SFTP attive e quindi riconnettersi dopo il periodo di attesa di 10 minuti per visualizzare le modifiche.

Risolvete gli errori di copia del flusso di lavoro

Descrizione

Se stai eseguendo un flusso di lavoro che contiene un passaggio per copiare il file caricato, potresti riscontrare il seguente errore:

```
{
  "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

Il file di origine si trova in un bucket Amazon S3 che si trova in un bucket Regione AWS diverso da quello di destinazione.

Soluzione

Se stai eseguendo un flusso di lavoro che include una fase di copia, assicurati che i bucket di origine e di destinazione siano gli stessi. Regione AWS

Risolvi i problemi di decrittografia del flusso di lavoro

Questa sezione descrive le possibili soluzioni per i seguenti problemi relativi ai flussi di lavoro crittografati.

Argomenti

Risolvi l'errore relativo al file di crittografia firmato

Descrizione

Il flusso di lavoro di decrittografia non riesce e viene visualizzato il seguente errore:

```
"Encrypted file with signed message unsupported"
```

Causa

Transfer Family attualmente non supporta la firma per i file crittografati.

Soluzione

Nel tuo client PGP, se esiste un'opzione per firmare il file crittografato, assicurati di deselezionare la selezione, poiché Transfer Family attualmente non supporta la firma per i file crittografati.

Risolvete l'errore relativo a un algoritmo FIPS

Descrizione

Il flusso di lavoro di decrittografia non riesce e il messaggio di registro è simile al seguente:

```
{
   "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

Il server Transfer Family ha la modalità FIPS abilitata e una fase del flusso di lavoro Decrypt associata. Quando si crittografano i file prima del caricamento sul server Transfer Family, il client di crittografia potrebbe generare file crittografati che utilizzano algoritmi di crittografia simmetrica non approvati dalla FIPS. In tale scenario, il flusso di lavoro non è in grado di decrittografare i file. Nell'esempio seguente, la versione 2.4.0 di GnuPG utilizza OCB (una modalità di cifratura a blocchi non FIPS) per crittografare i file: questo causa il fallimento del flusso di lavoro.

Soluzione

È necessario modificare la chiave GPG utilizzata per crittografare i file e poi ricrittografarli. La procedura seguente descrive i passaggi da eseguire.

Per modificare le chiavi PGP

1. Identifica la chiave da modificare eseguendo `gpg --list-keys`

   Questo restituisce un elenco di chiavi. Ogni chiave ha dettagli simili ai seguenti:

   ```
   pub   ed25519 2022-07-07 [SC]
         wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
   uid           [ultimate] Mary Major <marymajor@example.com>
   sub   cv25519 2022-07-07 [E]
   ```

2. Identifica la chiave che desideri modificare. Nell'esempio mostrato nel passaggio precedente, l'ID è`wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.
3. Esegui `gpg --edit-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.

   Il sistema risponde con dettagli sul programma GnuPG e sulla chiave specificata.
4. Al `gpg>` prompt, inserisci. `showpref` Vengono restituiti i seguenti dettagli:

   ```
   [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
```

Si noti che sono elencati gli algoritmi preferiti memorizzati nella chiave.

5. Vogliamo modificare la chiave per conservare tutti gli algoritmi tranne OCB. Esegui il `setpref` comando, specificando tutti gli algoritmi da conservare:

```
gpg> setpref AES256, AES192,AES,3DES,SHA512, SHA384, SHA256, SHA224, SHA1,ZLIB,
 BZIP2, ZIP, Uncompressed
```

Ciò restituisce i seguenti dettagli:

```
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. Inserisci y per aggiornare, quindi inserisci la password quando ti viene richiesto di confermare la modifica.
7. Salvare le modifiche.

```
gpg> save
```

Prima di rieseguire il flusso di lavoro di decrittografia, è necessario crittografare nuovamente i file utilizzando la chiave modificata.

Risolvi i problemi di Amazon EFS

Questa sezione descrive le possibili soluzioni per i seguenti problemi di Amazon EFS.

Argomenti

- Risolvi i problemi relativi al profilo POSIX mancante
- Risoluzione dei problemi relativi alle directory logiche con Amazon EFS

Risolvi i problemi relativi al profilo POSIX mancante

Descrizione

Se utilizzi lo storage Amazon EFS per il tuo server e utilizzi un provider di identità personalizzato, devi fornire alla tua AWS Lambda funzione un profilo POSIX.

Causa

Una possibile causa è che i modelli che forniamo per creare un metodo Amazon API Gateway AWS Lambda supportato attualmente non contengono informazioni POSIX.

Se hai fornito informazioni POSIX, il formato che hai usato per fornire le informazioni POSIX potrebbe non essere analizzato correttamente da Transfer Family.

Soluzione

Assicurati di fornire un elemento JSON a Transfer Family per il `PosixProfile` parametro.

Ad esempio, se si utilizza Python, è possibile aggiungere la riga seguente in cui si analizza il parametro: `PosixProfile`

```
if PosixProfile:
        response_data["PosixProfile"] = json.loads(PosixProfile)
```

Oppure, in JavaScript, puoi aggiungere la riga seguente, dove *`uid-value`* e *`gid-value`* sono numeri interi, pari o superiori a 0, che rappresentano rispettivamente l'ID utente (UID) e l'ID del gruppo (GID):

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

Questi esempi di codice inviano il `PosixProfile` parametro a Transfer Family come oggetto JSON, anziché come stringa.

Inoltre, all'interno AWS Secrets Manager, è necessario memorizzare il `PosixProfile` parametro come segue. Sostituisci *`your-uid`* e *`your-gid`* con i tuoi valori effettivi per GID e UID.

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

Risoluzione dei problemi relativi alle directory logiche con Amazon EFS

Descrizione

Se la directory home dell'utente non esiste e l'utente esegue un `ls` comando, il sistema risponde come segue:

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Causa

Se il tuo server Transfer Family utilizza Amazon EFS, la home directory dell'utente deve essere creata con accesso in lettura e scrittura prima che l'utente possa lavorare nella sua home directory logica. L'utente non può creare questa directory da solo, poiché non avrebbe le autorizzazioni per la `mkdir` sua home directory logica.

Soluzione

Un utente con accesso amministrativo alla directory principale deve creare la home directory logica dell'utente.

Risolvi i problemi relativi al test del tuo provider di identità

Descrizione

Se esegui il test del tuo provider di identità utilizzando la console o la chiamata `TestIdentityProvider` API, il `Response` campo è vuoto. Per esempio:

```
{
    "Response": "{}",
    "StatusCode": 200,
    "Message": ""
}
```

Causa

La causa più probabile è che l'autenticazione non sia riuscita a causa di un nome utente o di una password errati.

Soluzione

Assicurati di utilizzare le credenziali corrette per il tuo utente e, se necessario, aggiorna il nome utente o la password.

Risolvi i problemi relativi all'aggiunta di chiavi host affidabili per il connettore SFTP

Descrizione

Quando si crea o si modifica un connettore SFTP e si aggiunge una chiave host affidabile, viene visualizzato il seguente errore: `Failed to edit connector details (Invalid host key format.)`

Causa

Se incollate una chiave pubblica corretta, il problema potrebbe essere che avete incluso la `comment` parte della chiave. AWS Transfer Family attualmente non accetta la parte di commento della chiave.

Soluzione

Elimina la parte di commento della chiave, quando la incolli nel campo di testo. Ad esempio, supponiamo che la chiave sia simile alla seguente:

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

Rimuovi il testo che segue i == caratteri e incolla solo la parte della chiave fino a includere il==.

```
ssh-rsa AAAA...==
```

Risolvi i problemi di caricamento dei file

Questa sezione descrive le possibili soluzioni per i seguenti problemi di caricamento dei file.

Argomenti

- Risolvi gli errori di caricamento dei file di Amazon S3
- Risolvi i problemi relativi ai nomi di file illeggibili

Risolvi gli errori di caricamento dei file di Amazon S3

Descrizione

Quando tenti di caricare un file sullo storage Amazon S3 utilizzando Transfer Family, ricevi il seguente messaggio di errore AWS : Transfer does not support random access write to S3 objects.

Causa

Quando utilizzi Amazon S3 per lo storage del tuo server, Transfer Family non supporta connessioni multiple per un singolo trasferimento.

Soluzione

Se il tuo server Transfer Family utilizza Amazon S3 per lo storage, disattiva tutte le opzioni del software client che prevedono l'utilizzo di più connessioni per un singolo trasferimento.

Risolvi i problemi relativi ai nomi di file illeggibili

Descrizione

In alcuni dei file caricati sono presenti nomi di file danneggiati. Gli utenti a volte incontrano problemi con i trasferimenti FTP e SFTP che alterano determinati caratteri nei nomi dei file, come dieresi, lettere accentate o determinati script, come il cinese o l'arabo.

Causa

Sebbene i protocolli FTP e SFTP consentano ai client di negoziare la codifica dei caratteri dei nomi dei file, Amazon S3 e Amazon EFS non lo fanno. Richiedono invece la codifica dei caratteri UTF-8. Di conseguenza, alcuni caratteri non vengono renderizzati correttamente.

Soluzione

Per risolvere questo problema, esaminate l'applicazione client per la codifica dei caratteri dei nomi di file e assicuratevi che sia impostata su UTF-8.

`ResourceNotFound`Risolvi i problemi relativi all'eccezione

Descrizione

Viene visualizzato un errore in cui la risorsa non può essere trovata. Ad esempio, se corri`UpdateServer`, potresti ricevere il seguente errore:

```
An error occurred (ResourceNotFoundException) when calling the UpdateServer operation:
 Unknown server
```

Causa

Esistono diversi motivi per cui si riceve un ResourceNotFoundExceptionmessaggio. Nella maggior parte dei casi, la risorsa specificata nel comando API non esiste. Se hai specificato una risorsa esistente, la causa più probabile è che la tua regione predefinita sia diversa da quella della risorsa. Ad esempio, se la tua regione predefinita è us-east-1 e il tuo server Transfer Family è in us-east-2, riceverai un'eccezione per le risorse Unknown.

Per i dettagli sull'impostazione di una regione predefinita, consulta Configurazione rapida con. `aws configure`

Soluzione

Aggiungi un parametro region al tuo comando API per specificare in modo esplicito dove trovare una particolare risorsa.

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

Risolvi i problemi relativi al connettore SFTP

Questa sezione descrive le possibili soluzioni per i seguenti problemi del connettore SFTP.

Argomenti

- La negoziazione chiave fallisce
- Problemi vari del connettore SFTP

La negoziazione chiave fallisce

Descrizione

Quando la negoziazione sullo scambio di chiavi fallisce, viene visualizzato un errore. Per esempio:

```
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

Questo errore è dovuto al fatto che non vi è alcuna sovrapposizione tra gli algoritmi delle chiavi host supportati dal server e quelli supportati dal connettore.

Soluzione

Assicurati che il server remoto supporti almeno uno degli algoritmi chiave dell'host client elencati nel messaggio di errore. Per l'elenco degli algoritmi supportati, vedere. Politiche AWS Transfer Family di sicurezza per i connettori SFTP

Problemi vari del connettore SFTP

Descrizione

Dopo l'esecuzione viene visualizzato un errore`StartFileTransfer`, ma non si conosce la causa del problema e dopo la chiamata API viene restituito solo l'ID del connettore.

Causa

Questo errore può avere diverse cause. Per risolvere i problemi, ti consigliamo di testare il connettore e di cercare nei log. CloudWatch

Soluzione

- Testa il tuo connettore: Vedi. Provate un connettore SFTP Se il test fallisce, il sistema fornisce un messaggio di errore in base al motivo per cui il test non è riuscito. Questa sezione descrive come testare il connettore dalla console o utilizzando il comando TestConnectionAPI.
- Visualizza CloudWatch i log del tuo connettore: VediEsempi di voci di registro per i connettori SFTP. Questo argomento fornisce esempi di voci di registro del connettore SFTP e la convenzione di denominazione per aiutarvi a trovare i log appropriati.

Risolvi i problemi relativi a AS2

I messaggi di errore e i suggerimenti per la risoluzione dei problemi per i server abilitati all'Applicability Statement 2 (AS2) sono descritti qui:. Codici di errore AS2

Riferimento API

Le seguenti sezioni documentano le chiamate al servizio AWS Transfer Family API, i tipi di dati, i parametri e gli errori.

Argomenti

Benvenuto nell' AWS Transfer Family API

AWS Transfer Family è un servizio di trasferimento sicuro che puoi utilizzare per trasferire file da e verso lo storage di Amazon Simple Storage Service (Amazon S3) tramite i seguenti protocolli:

- Protocollo di trasferimento file (SFTP) Secure Shell (SSH)
- Protocollo di trasferimento file sicuro (FTPS)
- Protocollo di trasferimento file (FTP)
- Dichiarazione di applicabilità 2 (AS2)

I protocolli di trasferimento dei file vengono utilizzati nei flussi di lavoro per lo scambio di dati in diversi settori come i servizi finanziari, la sanità, la pubblicità e la vendita al dettaglio, tra gli altri. AWS Transfer Family semplifica la migrazione dei flussi di lavoro di trasferimento dei file verso. AWS

Per utilizzare il AWS Transfer Family servizio, devi creare un'istanza di un server nella AWS regione di tua scelta. È possibile creare il server, elencare i server disponibili e aggiornare ed eliminare i server. Il server è l'entità a cui richiede le operazioni sui file AWS Transfer Family. I server dispongono di diverse proprietà importanti. Il server è un'istanza denominata come identificato da un identificatore `ServerId` assegnato dal sistema. Facoltativamente, puoi assegnare un nome host o anche un nome host personalizzato a un server. Le fatture del servizio per tutti i server istanziati (anche quelli`OFFLINE`) e per la quantità di dati trasferiti.

Gli utenti devono essere noti al server che richiede le operazioni sui file. Un utente identificato tramite il nome utente viene assegnato a un server. I nomi utente vengono utilizzati per autenticare le richieste. Un server può avere un solo metodo di autenticazione:`AWS_DIRECTORY_SERVICE`, `SERVICE_MANAGEDAWS_LAMBDA`, o. `API_GATEWAY`

È possibile utilizzare uno dei seguenti tipi di provider di identità per autenticare gli utenti:

- Infatti`SERVICE_MANAGED`, una chiave pubblica SSH viene archiviata con le proprietà dell'utente su un server. Un utente può avere una o più chiavi pubbliche SSH in archivio per il `SERVICE_MANAGED` metodo di autenticazione. Quando un client richiede un'operazione su file per `SERVICE_MANAGED` method, fornisce il nome utente e la chiave privata SSH, che vengono autenticati e viene fornito l'accesso.
- È possibile gestire l'autenticazione e l'accesso degli utenti con i gruppi di Microsoft Active Directory selezionando il metodo di `AWS_DIRECTORY_SERVICE` autenticazione.
- È possibile connettersi a un provider di identità personalizzato utilizzando AWS Lambda. Scegli il metodo `AWS_LAMBDA` di autenticazione.
- Puoi anche autenticare le richieste utente utilizzando un metodo di autenticazione personalizzato che fornisce autenticazione utente e accesso. Questo metodo si basa su Amazon API Gateway per utilizzare la chiamata API dal tuo provider di identità per convalidare le richieste degli utenti. Questo metodo viene chiamato `API_GATEWAY` nelle chiamate API e personalizzato nella console. È possibile utilizzare questo metodo personalizzato per autenticare gli utenti rispetto a un servizio di directory, una coppia nome/password database o altri meccanismi.

Agli utenti viene assegnata una policy con una relazione di fiducia tra loro e un bucket Amazon S3. Potrebbero essere in grado di accedere a tutto o a una parte di un bucket. Affinché un server agisca per conto di un utente, deve ereditare la relazione di fiducia dall'utente. Viene creato un ruolo AWS Identity and Access Management (IAM) che contiene la relazione di trust e a tale ruolo viene assegnata un'`AssumeRole`azione. Il server può quindi eseguire operazioni sui file come se fosse l'utente.

Gli utenti che dispongono di un `home` set di proprietà di directory utilizzeranno tale directory (o cartella) come destinazione e origine delle operazioni sui file. Quando non è impostata una directory `home`, la directory `root` del bucket diventa la directory di destinazione.

I server, gli utenti e i ruoli sono tutti identificati dal rispettivo Amazon Resource Name (ARN). È possibile assegnare tag, che sono coppie chiave-valore, a entità con un ARN. I tag sono metadati che

possono essere utilizzati per raggruppare o cercare queste entità. Un esempio di utilizzo dei tag è per scopi di contabilità.

Nei formati AWS Transfer Family ID vengono rispettate le seguenti convenzioni:

- I valori `ServerId` hanno il formato `s-01234567890abcdef`.
- I valori `SshPublicKeyId` hanno il formato `key-01234567890abcdef`.

I formati Amazon Resource Name (ARN) assumono il seguente formato:

- Per i server, gli ARN assumono il modulo. `arn:aws:transfer:`*`region`*`:`*`account-id`*`:server/`*`server-id`*

  Un esempio di un ARN del server è: `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.
- Per gli utenti, gli ARN hanno il formato `arn:aws:transfer:`*`region`*`:`*`account-id`*`:user/`*`server-id`*`/`*`username`*.

  Un esempio è `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

Le voci DNS (endpoint) in uso sono le seguenti:

- Gli endpoint API hanno il formato `transfer.`*`region`*`.amazonaws.com`.
- Gli endpoint del server hanno il formato `server.transfer.`*`region`*`.amazonaws.com`.

Per un elenco degli endpoint Transfer Family per AWS regione, consulta gli AWS Transfer Family endpoint e le quote in. Riferimenti generali di AWS

Questo riferimento all'interfaccia API per AWS Transfer Family contiene la documentazione per un'interfaccia di programmazione che è possibile utilizzare per gestire. AWS Transfer Family La struttura di riferimento è la seguente:

- Per l'elenco alfabetico delle azioni API, vedere Actions.
- Per l'elenco alfabetico dei tipi di dati, vedere. Data Types
- Per un elenco di parametri di query comuni, consulta la pagina Parametri Comuni.
- Per le descrizioni dei codici di errore, consulta la pagina Errori comuni.

> **Tip**
>
> Invece di eseguire effettivamente un comando, è possibile utilizzare il `--generate-cli-skeleton` parametro con qualsiasi chiamata API per generare e visualizzare un modello di parametro. È quindi possibile utilizzare il modello generato per personalizzarlo e utilizzarlo come input per un comando successivo. Per i dettagli, consultate Generare e utilizzare un file scheletro di parametri.

Azioni

Sono supportate le operazioni seguenti:

- 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

Utilizzato dagli amministratori per scegliere quali gruppi della directory devono avere accesso al caricamento e al download di file tramite AWS Transfer Family i protocolli abilitati. Ad esempio, un Microsoft Active Directory potrebbe contenere 50.000 utenti, ma solo una piccola parte potrebbe aver bisogno della capacità di trasferire file sul server. Un amministratore può utilizzare `CreateAccess` per limitare l'accesso al set corretto di utenti che necessitano di questa funzionalità.

Sintassi della richiesta

```
{
   "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"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ExternalId

Un identificatore univoco necessario per identificare gruppi specifici all'interno della directory. Gli utenti del gruppo che associ hanno accesso alle tue risorse Amazon S3 o Amazon EFS tramite

i protocolli abilitati che utilizzano. AWS Transfer Family Se conosci il nome del gruppo, puoi visualizzare i valori SID eseguendo il seguente comando utilizzando Windows. PowerShell

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

In quel comando, sostituiscilo YourGroupNamecon il nome del tuo gruppo Active Directory.

L'espressione regolare utilizzata per convalidare questo parametro è una stringa di caratteri composta da caratteri alfanumerici maiuscoli e minuscoli senza spazi. È inoltre possibile includere caratteri di sottolineatura o uno dei seguenti caratteri: =, . @: /-

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `S-1-[\d-]+`

Campo obbligatorio: sì

HomeDirectory

La directory di destinazione (cartella) per un utente quando accede al server utilizzando il client.

Un esempio di `HomeDirectory` è `/bucket_name/home/mydirectory`.

> **Note**
>
> Il parametro `HomeDirectory` è utilizzato solo se `HomeDirectoryType` è impostato su `PATH`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

HomeDirectoryMappings

Mappature di directory logiche che specificano quali percorsi e chiavi di Amazon S3 o Amazon EFS devono essere visibili all'utente e in che modo desideri renderli visibili. È necessario

specificare la `Target` coppia `Entry` and, dove `Entry` mostra come il percorso viene reso visibile ed `Target` è il percorso effettivo di Amazon S3 o Amazon EFS. Se si specifica solo un obiettivo, questo viene visualizzato così com'è. È inoltre necessario assicurarsi che il proprio ruolo AWS Identity and Access Management (IAM) fornisca l'accesso ai percorsi in`Target`. Questo valore può essere impostato solo quando `HomeDirectoryType` è impostato su LOGICAL.

Di seguito è riportato un esempio `Target` di coppia `Entry` and.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

Nella maggior parte dei casi, è possibile utilizzare questo valore anziché la politica di sessione per bloccare l'utente nella home directory designata (» `chroot` «). A tale scopo, è possibile `Entry` impostare `/` e `Target` impostare il valore del `HomeDirectory` parametro.

Di seguito è riportato un esempio `Target` di coppia `Entry` and per`chroot`.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Tipo: matrice di oggetti HomeDirectoryMapEntry

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50000 articoli.

Campo obbligatorio: no

HomeDirectoryType

Il tipo di directory (cartella) di destinazione in cui deve trovarsi la directory home degli utenti quando accedono al server. Se lo imposti su`PATH`, l'utente vedrà il bucket Amazon S3 assoluto o il percorso Amazon EFS così com'è nei client del protocollo di trasferimento file. Se lo imposti su`LOGICAL`, devi fornire le mappature relative al modo in cui desideri rendere i percorsi Amazon S3 o Amazon EFS visibili ai tuoi utenti. `HomeDirectoryMappings`

> **Note**
>
> In caso `HomeDirectoryType` `LOGICAL` affermativo, devi fornire le mappature utilizzando il parametro. `HomeDirectoryMappings` Se, invece, `HomeDirectoryType` è`PATH`, si fornisce un percorso assoluto utilizzando il `HomeDirectory` parametro. Non puoi avere entrambi `HomeDirectory` e `HomeDirectoryMappings` nel tuo modello.

-Tipo: stringa

Valori validi: `PATH | LOGICAL`

Campo obbligatorio: no

Policy

Una policy di sessione per il tuo utente in modo da poter utilizzare lo stesso ruolo AWS Identity and Access Management (IAM) su più utenti. Questa policy limita l'accesso di un utente a porzioni del suo bucket Amazon S3. Le variabili che è possibile utilizzare all'interno di questa policy includono `${Transfer:UserName}`, `${Transfer:HomeDirectory}` e `${Transfer:HomeBucket}`.

> **Note**
>
> Questa politica si applica solo quando il dominio `ServerId` è Amazon S3. Amazon EFS non utilizza policy di sessione.
> Per le policy di sessione, AWS Transfer Family memorizza la policy come blob JSON, anziché come Amazon Resource Name (ARN) della policy. È possibile salvare la policy come blob JSON e passarla nell'argomento `Policy`.
> Per un esempio di policy di sessione, consultare Example session policy (Esempio di policy di sessione).
> Per ulteriori informazioni, consulta l'API AssumeRoleReference. AWS Security Token Service

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

PosixProfile

L'identità POSIX completa, incluso ID utente (`Uid`), ID gruppo (`Gid`) e qualsiasi ID gruppo secondario (`SecondaryGids`), che controlla l'accesso degli utenti ai file system Amazon EFS. Le autorizzazioni POSIX impostate su file e directory nel file system determinano il livello di accesso che gli utenti ottengono durante il trasferimento dei file da e verso i file system Amazon EFS.

Tipo: oggetto PosixProfile

Campo obbligatorio: no

Role

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che controlla l'accesso degli utenti al bucket Amazon S3 o al file system Amazon EFS. Le policy associate a questo ruolo determineranno il livello di accesso che desideri offrire agli utenti quando trasferiscono i file da e verso il bucket Amazon S3 o il file system Amazon EFS. Il ruolo IAM deve contenere anche una relazione di trust che consente al server di accedere alle proprie risorse durante la manutenzione delle richieste di trasferimento degli utenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: sì

ServerId

Un identificatore unico assegnato da sistema per un'istanza server. Questo è il server specifico a cui è stato aggiunto l'utente.

- Tipo: stringa

Limiti di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ExternalId

L'identificatore esterno del gruppo i cui utenti hanno accesso alle tue risorse Amazon S3 o Amazon EFS tramite i protocolli abilitati che utilizzano. AWS Transfer Family

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `S-1-[\d-]+`

ServerId

L'identificatore del server a cui è collegato l'utente.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateAgreement

Crea un contratto. Un accordo è un accordo bilaterale di partner commerciale, o partnership, tra un AWS Transfer Family server e un processo AS2. Il contratto definisce la relazione di trasferimento di file e messaggi tra il server e il processo AS2. Per definire un contratto, Transfer Family combina un server, un profilo locale, un profilo del partner, un certificato e altri attributi.

Il partner viene identificato con `PartnerProfileId`, mentre il processo AS2 è identificato con `LocalProfileId`.

Sintassi della richiesta

```
{
   "AccessRole": "string",
   "BaseDirectory": "string",
   "Description": "string",
   "LocalProfileId": "string",
   "PartnerProfileId": "string",
   "ServerId": "string",
   "Status": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessRole

I connettori vengono utilizzati per inviare file utilizzando il protocollo AS2 o SFTP. Per il ruolo di accesso, fornisci l'Amazon Resource Name (ARN) del AWS Identity and Access Management ruolo da utilizzare.

Per connettori AS2

Con AS2, è possibile inviare file chiamando `StartFileTransfer` e specificando i percorsi dei file nel parametro della richiesta, `SendFilePaths`. Utilizziamo la directory principale del file (ad esempio, per `--send-file-paths /bucket/dir/file.txt`, la directory principale è `/bucket/dir/`) per archiviare temporaneamente un file di messaggio AS2 elaborato, archiviare l'MDN quando lo riceviamo dal partner e scrivere un file JSON finale contenente i metadati pertinenti della trasmissione. Pertanto, `AccessRole` deve fornire l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella richiesta `StartFileTransfer`. Inoltre, devi fornire l'accesso in lettura e scrittura alla directory principale dei file che intendi inviare con `StartFileTransfer`.

Se si utilizza l'autenticazione di base per il connettore AS2, il ruolo di accesso richiede l'`secretsmanager:GetSecretValue`autorizzazione per il segreto. Se il segreto viene crittografato utilizzando una chiave gestita dal cliente anziché la chiave AWS gestita in Secrets Manager, il ruolo necessita anche dell'`kms:Decrypt`autorizzazione per quella chiave.

Per connettori SFTP

Assicurati che il ruolo di accesso fornisca l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta. Inoltre, assicurati che il ruolo fornisca l'`secretsmanager:GetSecretValue`autorizzazione a AWS Secrets Manager.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: sì

BaseDirectory

La directory di destinazione (cartella) per i file trasferiti utilizzando il protocollo AS2.

Un esempio di `BaseDirectory` è `/DOC-EXAMPLE-BUCKET/home/mydirectory`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: sì

Description

Un nome o una breve descrizione per identificare l'accordo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 200.

Modello: `[\p{Graph}]+`

Campo obbligatorio: no

LocalProfileId

Un identificativo univoco il profilo locale AS2.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: sì

PartnerProfileId

Un identificativo univoco del profilo del partner utilizzato nel contratto.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: sì

ServerId

Un identificatore unico assegnato da sistema per un'istanza server. Questo è il server specifico utilizzato dall'accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Status

Lo stato dell'accordo. L'accordo può essere uno dei due `ACTIVEINACTIVE`.

- Tipo: stringa

Valori validi: `ACTIVE | INACTIVE`

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i contratti.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "AgreementId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AgreementId

L'identificatore univoco dell'accordo. Utilizza questo ID per eliminare o aggiornare un accordo, nonché in qualsiasi altra chiamata API che richiede di specificare l'ID dell'accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `a-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente crea un accordo e restituisce l'ID dell'accordo.

```
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
```

Risposta di esempio

La chiamata API restituisce l'ID dell'accordo per il nuovo accordo.

```
{
    "AgreementId": "a-11112222333344444"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateConnector

Crea il connettore, che acquisisce i parametri per una connessione per il protocollo AS2 o SFTP. Per AS2, il connettore è necessario per inviare file a un server AS2 ospitato esternamente. Per SFTP, il connettore è necessario quando si inviano file a un server SFTP o si ricevono file da un server SFTP. Per maggiori dettagli sui connettori, consulta Configurare i connettori AS2 e Creare connettori SFTP.

> **Note**
>
> È necessario specificare esattamente un oggetto di configurazione: per AS2 (`As2Config`) o SFTP (). `SftpConfig`

Sintassi della richiesta

```
{
   "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"
```

```
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessRole

I connettori vengono utilizzati per inviare file utilizzando il protocollo AS2 o SFTP. Per il ruolo di accesso, fornisci l'Amazon Resource Name (ARN) del AWS Identity and Access Management ruolo da utilizzare.

Per connettori AS2

Con AS2, è possibile inviare file chiamando `StartFileTransfer` e specificando i percorsi dei file nel parametro della richiesta, `SendFilePaths`. Utilizziamo la directory principale del file (ad esempio, per `--send-file-paths /bucket/dir/file.txt`, la directory principale è `/bucket/dir/`) per archiviare temporaneamente un file di messaggio AS2 elaborato, archiviare l'MDN quando lo riceviamo dal partner e scrivere un file JSON finale contenente i metadati pertinenti della trasmissione. Pertanto, `AccessRole` deve fornire l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella richiesta `StartFileTransfer`. Inoltre, devi fornire l'accesso in lettura e scrittura alla directory principale dei file che intendi inviare con `StartFileTransfer`.

Se si utilizza l'autenticazione di base per il connettore AS2, il ruolo di accesso richiede l'`secretsmanager:GetSecretValue`autorizzazione per il segreto. Se il segreto viene crittografato utilizzando una chiave gestita dal cliente anziché la chiave AWS gestita in Secrets Manager, il ruolo necessita anche dell'`kms:Decrypt`autorizzazione per quella chiave.

Per connettori SFTP

Assicurati che il ruolo di accesso fornisca l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta. Inoltre, assicurati che il ruolo fornisca l'`secretsmanager:GetSecretValue`autorizzazione a AWS Secrets Manager.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: sì

As2Config

Una struttura che contiene i parametri per un oggetto connettore AS2.

Tipo: oggetto As2ConnectorConfig

Campo obbligatorio: no

LoggingRole

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a un connettore di attivare la CloudWatch registrazione per gli eventi Amazon S3. Una volta impostato, puoi visualizzare l'attività del connettore nei tuoi registri. CloudWatch

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

SecurityPolicyName

Speciifica il nome della politica di sicurezza per il connettore.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 100.

Modello: `TransferSFTPConnectorSecurityPolicy-[A-Za-z0-9-]+`

Campo obbligatorio: no

SftpConfig

Una struttura che contiene i parametri per un oggetto connettore SFTP.

Tipo: oggetto SftpConnectorConfig

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i connettori. I tag sono metadati allegati ai connettori per qualsiasi scopo.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Url

L'URL dell'endpoint AS2 o SFTP del partner.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 255.

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ConnectorId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ConnectorId

L'identificatore univoco del connettore, restituito dopo l'esito positivo della chiamata API.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente crea un connettore AS2. Nel comando, sostituite gli elementi come segue:

- `url`: fornisce l'URL per il server AS2 del partner commerciale.
- `your-IAM-role-for-bucket-access`: un ruolo IAM che ha accesso al bucket Amazon S3 che stai utilizzando per archiviare i tuoi file.
- Usa l'ARN per il tuo ruolo di registrazione, che include il tuo ID. Account AWS
- Fornisci un percorso a un file che contiene i parametri di configurazione del connettore AS2. L'oggetto di configurazione del connettore AS2 è descritto in 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
```

Esempio

L'esempio seguente crea un connettore SFTP. Nel comando, sostituite gli elementi come segue:

- `sftp-server-url`: fornite l'URL del server SFTP con cui state scambiando file.
- `your-IAM-role-for-bucket-access`: un ruolo IAM che ha accesso al bucket Amazon S3 che stai utilizzando per archiviare i tuoi file.
- Usa l'ARN per il tuo ruolo di registrazione, che include il tuo ID. Account AWS
- Fornite un percorso a un file che contiene i parametri di configurazione del connettore SFTP. L'oggetto di configurazione del connettore SFTP è descritto in 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
```

Esempio

La chiamata API restituisce l'ID del connettore per il nuovo connettore.

Risposta di esempio

```
{
    "ConnectorId": "a-11112222333344444"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3

- AWS SDK per Python
- AWS SDK per Ruby V3

CreateProfile

Crea il profilo locale o del partner da utilizzare per i trasferimenti AS2.

Sintassi della richiesta

```
{
   "As2Id": "string",
   "CertificateIds": [ "string" ],
   "ProfileType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

As2Id

`As2Id` è il nome AS2, come definito nella RFC 4130. Per i trasferimenti in entrata, questa è l'intestazione `AS2-From` dei messaggi AS2 inviati dal partner. Per i connettori in uscita, questa è l'intestazione `AS2-To` dei messaggi AS2 inviati al partner utilizzando l'operazione API `StartFileTransfer`. Questo ID non può includere spazi.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Modello: `[\p{Print}\s]*`

Campo obbligatorio: sì

CertificateIds

Una serie di identificativi dei certificati importati. Utilizzi questo identificativo per lavorare con i profili e i profili dei partner.

Tipo: matrice di stringhe

Vincoli di lunghezza: lunghezza fissa di 22.

Modello: `cert-([0-9a-f]{17})`

Campo obbligatorio: no

ProfileType

Determina il tipo di profilo da creare:

- `LOCAL`Specificare di creare un profilo locale. Un profilo locale rappresenta l'organizzazione o la parte del server Transfer Family abilitato per AS2.
- `PARTNER`Specificare di creare un profilo partner. Un profilo partner rappresenta un'organizzazione remota, esterna a Transfer Family.

Tipo: stringa

Valori validi: `LOCAL | PARTNER`

Campo obbligatorio: sì

Tags

Coppie chiave-valore che possono essere utilizzate per raggruppare e cercare profili AS2.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "ProfileId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ProfileId

L'identificatore univoco per il profilo AS2, restituito dopo l'esito positivo della chiamata API.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente crea un profilo e ne restituisce l'ID.

Gli ID dei certificati vengono creati durante l'esecuzione`import-certificate`, uno per il certificato di firma e uno per il certificato di crittografia.

```
aws transfer create-profile --as2-id MYCORP --certificate-ids c-abcdefg123456hijk
               c-987654aaaa321bbbb
```

Risposta di esempio

La chiamata API restituisce l'ID del profilo per il nuovo profilo.

```
{
    "ProfileId": "p-11112222333344444"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateServer

Crea l'istanza di un server virtuale a dimensionamento automatico basato sul protocollo FTP selezionato in AWS. Quando si aggiorna il server abilitato al protocollo FTP o quando si usano gli utenti, utilizzare la proprietà `ServerId` generata dal servizio che viene assegnata al server appena creato.

Sintassi della richiesta

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

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Certificate

Il nome della risorsa Amazon (ARN) del certificato AWS Certificate Manager (ACM). Obbligatorio quando `Protocols` è impostato su `FTPS`.

Per richiedere un nuovo certificato pubblico, consulta Richiedere un certificato pubblico nella Guida per l' AWS Certificate Manager utente.

Per importare un certificato esistente in ACM, consulta Importazione di certificati in ACM nella Guida per l' AWS Certificate Manager utente.

Per richiedere un certificato privato per utilizzare FTPS tramite indirizzi IP privati, consulta Richiedere un certificato privato nella Guida per l'utente. AWS Certificate Manager

Sono supportati i certificati con gli algoritmi di crittografia e le dimensioni delle chiavi seguenti:

- RSA a 2048 bit (RSA_2048)
- RSA a 4096 bit (RSA_4096)
- Elliptic Prime Curve a 256 bit (EC_prime256v1)
- Elliptic Prime Curve a 384 bit (EC_secp384r1)
- Elliptic Prime Curve a 521 bit (EC_secp521r1)

> **Note**
>
> Il certificato deve essere un certificato SSL/TLS X.509 versione 3 valido con FQDN o indirizzo IP specificato e le informazioni sull'emittente.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1600 caratteri.

Campo obbligatorio: no

Domain

Il dominio del sistema di storage utilizzato per i trasferimenti di file. Sono disponibili due domini: Amazon Simple Storage Service (Amazon S3) e Amazon Elastic File System (Amazon EFS). Il valore predefinito è S3.

> **Note**
>
> Dopo la creazione del server, il dominio non può essere modificato.

-Tipo: stringa

Valori validi: `S3 | EFS`

Campo obbligatorio: no

EndpointDetails

Le impostazioni dell'endpoint del cloud privato virtuale (VPC) configurate per il server. Quando esegui l'hosting dell'endpoint all'interno del tuo VPC, puoi renderlo accessibile solo alle risorse nel

VPC oppure collegarvi indirizzi IP elastici e renderlo accessibile ai client tramite Internet. I gruppi di sicurezza predefiniti del VPC vengono assegnati automaticamente all'endpoint.

Tipo: oggetto EndpointDetails

Campo obbligatorio: no

EndpointType

Il tipo di endpoint VPC che il server deve utilizzare. È possibile scegliere di rendere l'endpoint del server accessibile pubblicamente (PUBLIC) o ospitarlo all'interno del proprio VPC. Nel caso di un endpoint ospitato in un VPC, è possibile consentire l'accesso solo al server e alle risorse all'interno del VPC o scegliere di renderlo accessibile tramite Internet collegandolo direttamente a indirizzi IP elastici.

> **Note**
>
> Dopo il 19 maggio 2021, non potrai creare un server utilizzando `EndpointType=VPC_ENDPOINT` in your Account AWS se il tuo account non l'ha già fatto prima del 19 maggio 2021. Se hai già creato dei server con `EndpointType=VPC_ENDPOINT` in your Account AWS entro il 19 maggio 2021 o prima, non ne subirai alcuna modifica. Dopo questa data, usa `EndpointType =VPC`.
> Per ulteriori informazioni, consulta Interruzione dell'uso di VPC_ENDPOINT.
> È consigliabile utilizzare `VPC` come `EndpointType`. Con questo tipo di endpoint, è possibile associare direttamente fino a tre indirizzi IPv4 elastici (anche IP BYO) all'endpoint del server e utilizzare i gruppi di sicurezza VPC per limitare il traffico tramite l'indirizzo IP pubblico del client. Questo non è possibile se `EndpointType` è impostato su `VPC_ENDPOINT`.

-Tipo: stringa

Valori validi: `PUBLIC | VPC | VPC_ENDPOINT`

Campo obbligatorio: no

HostKey

La chiave privata RSA, ECDSA o ED25519 da utilizzare per il server compatibile con SFTP. È possibile aggiungere più chiavi host, nel caso in cui si desideri ruotare le chiavi, o disporre di un set di chiavi attive che utilizzano algoritmi diversi.

Utilizzate il seguente comando per generare una chiave RSA a 2048 bit senza passphrase:

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

Utilizzate un valore minimo di 2048 per l'opzione. `-b` È possibile creare una chiave più potente utilizzando 3072 o 4096.

Utilizzate il seguente comando per generare una chiave ECDSA a 256 bit senza passphrase:

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

I valori validi per l'`-b`opzione per ECDSA sono 256, 384 e 521.

Utilizzate il seguente comando per generare una chiave ED25519 senza passphrase:

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

Puoi sostituire tutti questi comandi my-new-server-keycon una stringa a tua scelta.

> **Important**
>
> Se non avete intenzione di migrare gli utenti esistenti da un server esistente che supporta SFTP a un nuovo server, non aggiornate la chiave host. La modifica accidentale della chiave host di un server può creare problemi.

Per ulteriori informazioni, consulta Aggiornare le chiavi host per il server compatibile con SFTP nella Guida per l'utente. AWS Transfer Family

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 4096.

Campo obbligatorio: no

IdentityProviderDetails

Richiesto quando `IdentityProviderType` è impostato su, o`AWS_DIRECTORY_SERVICE`. `AWS_LAMBDA API_GATEWAY` Accetta un array contenente tutte le informazioni necessarie per usare una directory in `AWS_DIRECTORY_SERVICE` o chiamare un'API di autenticazione fornita dal cliente, incluso l'URL dell'API Gateway. Obbligatorio quando `IdentityProviderType` è impostato su `SERVICE_MANAGED`.

Tipo: oggetto IdentityProviderDetails

Campo obbligatorio: no

IdentityProviderType

La modalità di autenticazione di un server. Il valore predefinito è`SERVICE_MANAGED`, che consente di archiviare e accedere alle credenziali utente all'interno del AWS Transfer Family servizio.

`AWS_DIRECTORY_SERVICE`Utilizzalo per fornire l'accesso ai gruppi di Active Directory in AWS Directory Service for Microsoft Active Directory o Microsoft Active Directory nell'ambiente locale o AWS utilizzando AD Connector. Questa opzione prevede inoltre che l'utente fornisca un ID directory utilizzando il parametro `IdentityProviderDetails`.

Utilizza il valore `API_GATEWAY` da integrare con un provider di identità a scelta. L'impostazione `API_GATEWAY` richiede di fornire un URL dell'endpoint del Gateway Amazon API da richiamare per l'autenticazione utilizzando il parametro `IdentityProviderDetails`.

Utilizza il `AWS_LAMBDA` valore per utilizzare direttamente una AWS Lambda funzione come provider di identità. Se scegli questo valore, devi specificare l'ARN per la funzione Lambda nel `Function` parametro per il tipo di dati. `IdentityProviderDetails`

- Tipo: stringa

Valori validi: `SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA`

Campo obbligatorio: no

LoggingRole

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a un server di attivare la CloudWatch registrazione Amazon per Amazon S3 o Amazon EFSEvents. Una volta impostato, puoi visualizzare l'attività degli utenti nei tuoi log. CloudWatch

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Modello: `(|arn:.*role/\S+)`

Campo obbligatorio: no

PostAuthenticationLoginBanner

Specifica una stringa da visualizzare quando gli utenti si connettono a un server. Questa stringa viene visualizzata dopo l'autenticazione dell'utente.

> **Note**
>
> Il protocollo SFTP non supporta banner di visualizzazione post-autenticazione.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 4096.

Modello: `[\x09-\x0D\x20-\x7E]*`

Campo obbligatorio: no

PreAuthenticationLoginBanner

Specifica una stringa da visualizzare quando gli utenti si connettono a un server. Questa stringa viene visualizzata prima dell'autenticazione dell'utente. Il seguente banner, ad esempio, mostra i dettagli sull'utilizzo 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: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 4096.

Modello: `[\x09-\x0D\x20-\x7E]*`

Campo obbligatorio: no

ProtocolDetails

Le impostazioni del protocollo configurate per il server.

- Per indicare la modalità passiva (per i protocolli FTP e FTPS), utilizza il parametro `PassiveIp`. Inserire un singolo indirizzo IPv4 composto da 4 numeri decimali separati da punti, ad esempio l'indirizzo IP esterno di un firewall, un router o un load balancer.

- Per ignorare l'errore generato quando il client tenta di utilizzare il comando `SETSTAT` su un file che stai caricando su un bucket Amazon S3, utilizza il parametro `SetStatOption`. Per fare in modo che il AWS Transfer Family server ignori il `SETSTAT` comando e carichi i file senza dover apportare modifiche al client SFTP, imposta il valore su. `ENABLE_NO_OP` Se imposti il `SetStatOption` parametro su`ENABLE_NO_OP`, Transfer Family genera una voce di registro in Amazon CloudWatch Logs, in modo da poter determinare quando il client sta effettuando una `SETSTAT` chiamata.
- Per determinare se il AWS Transfer Family server riprende le sessioni negoziate recenti tramite un ID di sessione univoco, utilizza il parametro. `TlsSessionResumptionMode`
- `As2Transports` indica il metodo di trasporto per i messaggi AS2. Attualmente è supportato solo HTTP.

Tipo: oggetto ProtocolDetails

Campo obbligatorio: no

Protocols

Specifica il protocollo o i protocolli di trasferimento file su cui il client del protocollo di trasferimento file può connettersi all'endpoint del server. I protocolli disponibili sono:

- `SFTP` (Secure Shell (SSH) File Transfer Protocol): trasferimento di file su SSH
- `FTPS` File Transfer Protocol Secure: trasferimento di file con crittografia TLS
- `FTP` (File Transfer Protocol): trasferimento file non crittografato
- `AS2`(Dichiarazione di applicabilità 2): utilizzata per il trasporto di dati strutturati business-to-business

> **Note**
>
> - Se si selezionaFTPS, è necessario scegliere un certificato archiviato in AWS Certificate Manager (ACM) che viene utilizzato per identificare il server quando i client si connettono ad esso tramite FTPS.
> - Se `Protocol` include `FTP` o `FTPS`, `EndpointType` deve essere `VPC` e `IdentityProviderType` deve essere `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
> - Se `Protocol` include `FTP`, `AddressAllocationIds` non può essere associato.
> - Se `Protocol` è impostato solo su `SFTP`, `EndpointType` può essere impostato su `PUBLIC` e `IdentityProviderType` può essere impostato uno qualunque dei tipi di

identità supportati: `SERVICE_MANAGED`, `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.

- Se `Protocol` include `AS2`, `EndpointType` deve essere `VPC` e il dominio deve essere Amazon S3.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Valori validi: `SFTP | FTP | FTPS | AS2`

Campo obbligatorio: no

S3StorageOptions

Indica se le prestazioni per le tue directory Amazon S3 sono ottimizzate o meno. Questa opzione è disabilitata per impostazione predefinita.

Per impostazione predefinita, le mappature delle home directory hanno un valore di. `TYPE DIRECTORY` Se si abilita questa opzione, è necessario impostarla esplicitamente su `FILE` se si desidera che una mappatura abbia un file di destinazione. `HomeDirectoryMapEntry Type`

Tipo: oggetto S3StorageOptions

Campo obbligatorio: no

SecurityPolicyName

Speciifica il nome della politica di sicurezza per il server.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 100.

Modello: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Campo obbligatorio: no

StructuredLogDestinations

Speciifica i gruppi di log a cui vengono inviati i log del server.

Per specificare un gruppo di log, è necessario fornire l'ARN per un gruppo di log esistente. In questo caso, il formato del gruppo di log è il seguente:

`arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*`

Ad esempio, `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

Se in precedenza è stato specificato un gruppo di log per un server, è possibile cancellarlo e di fatto disattivare la registrazione strutturata fornendo un valore vuoto per questo parametro in una `update-server` chiamata. Per esempio:

```
update-server --server-id s-1234567890abcdef0 --structured-log-
destinations
```

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i server.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

WorkflowDetails

Specifica l'ID del flusso di lavoro da assegnare e il ruolo di esecuzione utilizzato per l'esecuzione del flusso di lavoro.

Oltre a un flusso di lavoro da eseguire quando un file viene caricato completamente, `WorkflowDetails` può contenere anche un ID del flusso di lavoro (e ruolo di esecuzione) per l'esecuzione di un flusso di lavoro in caso di caricamento parziale. Un caricamento parziale si verifica quando la sessione del server si disconnette mentre il file è ancora in fase di caricamento.

Tipo: oggetto WorkflowDetails

Campo obbligatorio: no

Sintassi della risposta

```
{
   "ServerId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ServerId

L'identificatore assegnato dal servizio del server che viene creato.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente crea un nuovo server utilizzando un`VPC_ENDPOINT`.

Richiesta di esempio

```
{
   "EndpointType": "VPC",
   "EndpointDetails":...,
   "HostKey": "Your RSA private key",
   "IdentityProviderDetails": "IdentityProvider",
   "IdentityProviderType": "SERVICE_MANAGED",
```

```
   "LoggingRole": "CloudWatchLoggingRole",
   "Tags": [
      {
         "Key": "Name",
         "Value": "MyServer"
      }
   ]
}
```

Esempio

Questo è un esempio di risposta per questa chiamata API.

Risposta di esempio

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateUser

Crea un utente e lo associa a un server esistente abilitato al protocollo di trasferimento file. È possibile solo creare e associare gli utenti con i server con `IdentityProviderType` impostato su `SERVICE_MANAGED`. Utilizzando i parametri per`CreateUser`, è possibile specificare il nome utente, impostare la home directory, archiviare la chiave pubblica dell'utente e assegnare il ruolo dell'utente AWS Identity and Access Management (IAM). Facoltativamente è anche possibile aggiungere una policy di sessione e assegnare i metadati con tag che possono essere utilizzati per raggruppare e cercare gli utenti.

Sintassi della richiesta

```
{
   "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"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HomeDirectory

La directory di destinazione (cartella) per un utente quando accede al server utilizzando il client.

Un esempio di `HomeDirectory` è `/bucket_name/home/mydirectory`.

> **Note**
>
> Il parametro `HomeDirectory` è utilizzato solo se `HomeDirectoryType` è impostato su `PATH`.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

HomeDirectoryMappings

Mappature di directory logiche che specificano quali percorsi e chiavi di Amazon S3 o Amazon EFS devono essere visibili all'utente e in che modo desideri renderli visibili. È necessario specificare la `Target` coppia `Entry` and, dove `Entry` mostra come il percorso viene reso visibile ed `Target` è il percorso effettivo di Amazon S3 o Amazon EFS. Se si specifica solo un obiettivo, questo viene visualizzato così com'è. È inoltre necessario assicurarsi che il proprio ruolo AWS Identity and Access Management (IAM) fornisca l'accesso ai percorsi in`Target`. Questo valore può essere impostato solo quando `HomeDirectoryType` è impostato su LOGICAL.

Di seguito è riportato un esempio `Target` di coppia `Entry` and.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

Nella maggior parte dei casi, è possibile utilizzare questo valore anziché la politica di sessione per bloccare l'utente nella home directory designata (» `chroot` «). A tale scopo, è possibile impostare

/ e Entry Target impostare il valore che l'utente dovrebbe visualizzare per la propria home directory al momento dell'accesso.

Di seguito è riportato un esempio Target di coppia Entry and perchroot.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Tipo: matrice di oggetti HomeDirectoryMapEntry

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50000 articoli.

Campo obbligatorio: no

HomeDirectoryType

Il tipo di directory (cartella) di destinazione in cui deve trovarsi la directory home degli utenti quando accedono al server. Se lo imposti suPATH, l'utente vedrà il bucket Amazon S3 assoluto o il percorso Amazon EFS così com'è nei client del protocollo di trasferimento file. Se lo imposti suLOGICAL, devi fornire le mappature relative al modo in cui desideri rendere i percorsi Amazon S3 o Amazon EFS visibili ai tuoi utenti. HomeDirectoryMappings

> **Note**
>
> In caso HomeDirectoryType LOGICAL affermativo, devi fornire le mappature utilizzando il parametro. HomeDirectoryMappings Se, invece, HomeDirectoryType èPATH, si fornisce un percorso assoluto utilizzando il HomeDirectory parametro. Non puoi avere entrambi HomeDirectory e HomeDirectoryMappings nel tuo modello.

-Tipo: stringa

Valori validi: PATH | LOGICAL

Campo obbligatorio: no

Policy

Una policy di sessione per il tuo utente in modo da poter utilizzare lo stesso ruolo AWS Identity and Access Management (IAM) su più utenti. Questa policy limita l'accesso di un utente a porzioni del suo bucket Amazon S3. Le variabili che è possibile utilizzare all'interno di questa policy includono ${Transfer:UserName}, ${Transfer:HomeDirectory} e ${Transfer:HomeBucket}.

> **Note**
>
> Questa politica si applica solo quando il dominio `ServerId` è Amazon S3. Amazon EFS non utilizza policy di sessione.
> Per le policy di sessione, AWS Transfer Family memorizza la policy come blob JSON, anziché come Amazon Resource Name (ARN) della policy. È possibile salvare la policy come blob JSON e passarla nell'argomento `Policy`.
> Per un esempio di policy di sessione, consultare Example session policy (Esempio di policy di sessione).
> Per ulteriori informazioni, consulta AssumeRoleil AWS Security Token Service API Reference.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

PosixProfile

Speciifica l'identità POSIX completa, inclusi l'ID utente (`Uid`), l'ID di gruppo (`Gid`) e gli eventuali ID di gruppo secondari (`SecondaryGids`), che controlla l'accesso degli utenti ai file system Amazon EFS. Le autorizzazioni POSIX impostate su file e directory in Amazon EFS determinano il livello di accesso ottenuto dagli utenti durante il trasferimento di file da e verso i file system Amazon EFS.

Tipo: oggetto PosixProfile

Campo obbligatorio: no

Role

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che controlla l'accesso degli utenti al bucket Amazon S3 o al file system Amazon EFS. Le policy associate a questo ruolo determineranno il livello di accesso che desideri offrire agli utenti quando trasferiscono i file da e verso il bucket Amazon S3 o il file system Amazon EFS. Il ruolo IAM deve contenere anche una relazione di trust che consente al server di accedere alle proprie risorse durante la manutenzione delle richieste di trasferimento degli utenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: sì

ServerId

Un identificatore unico assegnato da sistema per un'istanza server. Questo è il server specifico a cui è stato aggiunto l'utente.

- Tipo: stringa

Limiti di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

SshPublicKeyBody

La parte pubblica della chiave Secure Shell (SSH) utilizzata per autenticare l'utente sul server.

I tre elementi standard in formato chiave pubblica SSH sono `<key type><body base64>`, e uno opzionale`<comment>`, con spazi tra ogni elemento.

AWS Transfer Family accetta le chiavi RSA, ECDSA ed ED25519.

- Per le chiavi RSA, il tipo di chiave è. `ssh-rsa`
- Per le chiavi ED25519, il tipo di chiave è. `ssh-ed25519`
- Per le chiavi ECDSA, il tipo di chiave è`ecdsa-sha2-nistp256`, o `ecdsa-sha2-nistp384``ecdsa-sha2-nistp521`, a seconda della dimensione della chiave generata.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare gli utenti. I tag sono metadati associati agli utenti per qualsiasi scopo.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

UserName

Una stringa univoca che identifica un utente ed è associata a un `ServerId`. Questo nome utente deve essere composto da un minimo di 3 a un massimo di 100 caratteri. I seguenti sono caratteri validi: a-z, A-Z, 0-9, carattere di sottolineatura '_', trattino '-', punto '.' e chiocciola '@'. Il nome utente non può iniziare con un trattino, un punto o una chiocciola.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ServerId": "string",
   "UserName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ServerId

L'identificatore del server a cui è collegato l'utente.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

UserName

Una stringa univoca che identifica un utente Transfer Family.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

Per creare un utente, puoi prima salvare i parametri in un file JSON, ad esempio`createUserParameters`, quindi eseguire il comando 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"
}
```

Richiesta di esempio

```
aws transfer create-user --cli-input-json file://createUserParameters
```

Risposta di esempio

```
{
    "ServerId": ""s-1111aaaa2222bbbb3",
    "UserName": "bobusa-API"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

CreateWorkflow

Consente di creare un flusso di lavoro con fasi e dettagli specifici che il flusso di lavoro richiama dopo il completamento del trasferimento dei file. Dopo aver creato un flusso di lavoro, è possibile associarlo a qualsiasi server di trasferimento specificando il campo `workflow-details` nelle operazioni `CreateServer` e `UpdateServer`.

Sintassi della richiesta

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

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Description

Una descrizione testuale del flusso di lavoro.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `[\w- ]*`

Campo obbligatorio: no

OnExceptionSteps

Specifica le fasi (azioni) da eseguire se durante l'esecuzione del flusso di lavoro si verificano eventuali errori.

> **Note**
>
> Per i passaggi personalizzati, la funzione Lambda deve inviare `FAILURE` all'API di callback per avviare i passaggi di eccezione. Inoltre, se la Lambda non invia `SUCCESS` prima del timeout, vengono eseguiti i passaggi di eccezione.

Tipo: matrice di oggetti WorkflowStep

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 8 elementi.

Campo obbligatorio: no

Steps

Specifica i dettagli delle fasi incluse nel flusso di lavoro specificato.

TYPEspecifica quale delle seguenti azioni viene intrapresa per questa fase.

- **`COPY`** - Copiare il file in un'altra posizione.

- **CUSTOM**- Esegue un passaggio personalizzato con un obiettivo di AWS Lambda funzione.
- **DECRYPT** - Decrittografare un file crittografato prima che è stato caricato.
- **DELETE** - Eliminare il file.
- **TAG** - Aggiungere un tag al file.

> **Note**
>
> Attualmente, la copia e l'etichettatura sono supportate solo su S3.

Per la posizione del file, è necessario specificare il bucket e la chiave Amazon S3 oppure l'ID e il percorso del file system Amazon EFS.

Tipo: matrice di oggetti WorkflowStep

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 8 articoli.

Campo obbligatorio: sì

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i flussi di lavoro. I tag sono metadati associati ai flussi di lavoro per qualsiasi scopo.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "WorkflowId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

WorkflowId

Un identificatore univoco per il flusso di lavoro.

- Tipo: stringa

Limiti di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

È possibile salvare le informazioni sulle fasi del flusso di lavoro in un file di testo e quindi utilizzare questo file per creare un flusso di lavoro, come mostrato nell'esempio seguente. Nell'esempio seguente si presuppone che le fasi del flusso di lavoro siano state salvate in *example-file.json* (nella stessa cartella da cui si esegue il comando) e che si desideri creare il flusso di lavoro nella Regione della Virginia settentrionale (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}"
      }
    }
]
```

Esempio

La `CreateWorkflow` chiamata restituisce l'ID del flusso di lavoro per il nuovo flusso di lavoro.

Risposta di esempio

```
{
    "WorkflowId": "w-1234abcd5678efghi"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteAccess

Consente di eliminare l'accesso specificato nei `ExternalID` parametri `ServerID` and.

Sintassi della richiesta

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ExternalId

Un identificatore univoco necessario per identificare gruppi specifici all'interno della directory. Gli utenti del gruppo che associ hanno accesso alle tue risorse Amazon S3 o Amazon EFS tramite i protocolli abilitati che utilizzano. AWS Transfer Family Se conosci il nome del gruppo, puoi visualizzare i valori SID eseguendo il seguente comando utilizzando Windows. PowerShell

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

In quel comando, sostituiscilo YourGroupNamecon il nome del tuo gruppo Active Directory.

L'espressione regolare utilizzata per convalidare questo parametro è una stringa di caratteri composta da caratteri alfanumerici maiuscoli e minuscoli senza spazi. È inoltre possibile includere caratteri di sottolineatura o uno dei seguenti caratteri: =, . @: /-

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `S-1-[\d-]+`

Campo obbligatorio: sì

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui è assegnato questo utente.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteAgreement

Eliminare l'accordo specificato nel campo fornito`AgreementId`.

Sintassi della richiesta

```
{
   "AgreementId": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgreementId

Un identificatore univoco per l'accordo. Questo identificatore viene restituito quando si crea un accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `a-([0-9a-f]{17})`

Campo obbligatorio: sì

ServerId

L'identificatore del server associato all'accordo che si sta eliminando.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteCertificate

Elimina il certificato specificato nel `CertificateId` parametro.

Sintassi della richiesta

```
{
   "CertificateId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

CertificateId

L'identificatore dell'oggetto certificato che si sta eliminando.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 22.

Modello: `cert-([0-9a-f]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteConnector

Elimina il connettore specificato nel modulo fornitoConnectorId.

Sintassi della richiesta

```
{
   "ConnectorId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ConnectorId

L'identificatore univoco del connettore.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: c-([0-9a-f]{17})

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteHostKey

Elimina la chiave host specificata nel `HostKeyId` parametro.

Sintassi della richiesta

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HostKeyId

L'identificatore della chiave host che stai eliminando.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 25.

Modello: `hostkey-[0-9a-f]{17}`

Campo obbligatorio: sì

ServerId

L'identificatore del server che contiene la chiave host che si sta eliminando.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteProfile

Elimina il profilo specificato nel `ProfileId` parametro.

Sintassi della richiesta

```
{
   "ProfileId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ProfileId

L'identificatore del profilo che si sta eliminando.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteServer

Elimina il server abilitato al protocollo di trasferimento file specificato.

Da questa operazione non viene restituita alcuna risposta.

Sintassi della richiesta

```
{
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ServerId

Un identificatore univoco assegnato dal sistema per un'istanza del server.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente elimina un server.

Richiesta di esempio

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Esempio

In caso di successo, non viene restituito nulla.

Risposta di esempio

```
{
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteSshPublicKey

Elimina la chiave pubblica Secure Shell (SSH) di un utente.

Sintassi della richiesta

```
{
   "ServerId": "string",
   "SshPublicKeyId": "string",
   "UserName": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ServerId

Un identificatore univoco assegnato dal sistema per un'istanza del server abilitata al protocollo di trasferimento file a cui è assegnato l'utente.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

SshPublicKeyId

Un identificatore univoco utilizzato per fare riferimento alla chiave SSH specifica dell'utente.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza fissa di 21.

Modello: `key-[0-9a-f]{17}`

Campo obbligatorio: sì

UserName

Una stringa univoca che identifica un utente la cui chiave pubblica viene eliminata.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente elimina la chiave pubblica SSH di un utente.

Richiesta di esempio

```
{
   "ServerId": "s-01234567890abcdef",
   "SshPublicKeyId": "MyPublicKey",
   "UserName": "my_user"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteUser

Elimina l'utente appartenente a un server abilitato al protocollo di trasferimento file specificato.

Non viene restituita alcuna risposta da questa operazione.

> **Note**
>
> Quando si elimina un utente da un server, le informazioni relative all'utente vengono perse.

Sintassi della richiesta

```
{
   "ServerId": "string",
   "UserName": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ServerId

Un identificatore univoco assegnato dal sistema per un'istanza del server a cui è assegnato l'utente.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

UserName

Una stringa univoca che identifica un utente che viene eliminato da un server.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente elimina un utente Transfer Family.

Richiesta di esempio

```
{
   "ServerId": "s-01234567890abcdef",
   "UserNames": "my_user"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteWorkflow

Elimina il flusso di lavoro specificato.

Sintassi della richiesta

```
{
   "WorkflowId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

WorkflowId

Un identificatore univoco per il flusso di lavoro.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeAccess

Descrive l'accesso assegnato allo specifico server abilitato al protocollo di trasferimento file, come identificato dalla sua `ServerId` proprietà e dalla sua. `ExternalId`

La risposta di questa chiamata restituisce le proprietà dell'accesso associato al `ServerId` valore specificato.

Sintassi della richiesta

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ExternalId

Un identificatore univoco necessario per identificare gruppi specifici all'interno della directory. Gli utenti del gruppo che associ hanno accesso alle tue risorse Amazon S3 o Amazon EFS tramite i protocolli abilitati che utilizzano. AWS Transfer Family Se conosci il nome del gruppo, puoi visualizzare i valori SID eseguendo il seguente comando utilizzando Windows. PowerShell

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

In quel comando, sostituiscilo YourGroupNamecon il nome del tuo gruppo Active Directory.

L'espressione regolare utilizzata per convalidare questo parametro è una stringa di caratteri composta da caratteri alfanumerici maiuscoli e minuscoli senza spazi. È inoltre possibile includere caratteri di sottolineatura o uno dei seguenti caratteri: =, . @: /-

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `S-1-[\d-]+`

Campo obbligatorio: sì

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui è assegnato questo accesso.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Access

L'identificatore esterno del server a cui è collegato l'accesso.

Tipo: oggetto DescribedAccess

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui è assegnato questo accesso.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeAgreement

Descrive l'accordo identificato da`AgreementId`.

Sintassi della richiesta

```
{
   "AgreementId": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AgreementId

Un identificatore univoco per l'accordo. Questo identificatore viene restituito quando si crea un accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `a-([0-9a-f]{17})`

Campo obbligatorio: sì

ServerId

L'identificatore del server associato all'accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "Agreement": {
      "AccessRole": "string",
      "AgreementId": "string",
      "Arn": "string",
      "BaseDirectory": "string",
      "Description": "string",
      "LocalProfileId": "string",
      "PartnerProfileId": "string",
      "ServerId": "string",
      "Status": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ]
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Agreement

I dettagli dell'accordo specificato, restituiti come oggetto. `DescribedAgreement`

Tipo: oggetto DescribedAgreement

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeCertificate

Descrive il certificato identificato da`CertificateId`.

Sintassi della richiesta

```
{
   "CertificateId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

CertificateId

Una serie di identificativi dei certificati importati. Utilizzi questo identificativo per lavorare con i profili e i profili dei partner.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 22.

Modello: `cert-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Certificate

I dettagli del certificato specificato, restituito come oggetto.

Tipo: oggetto DescribedCertificate

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeConnector

Descrive il connettore identificato dal `ConnectorId`.

Sintassi della richiesta

```
{
   "ConnectorId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ConnectorId

L'identificatore univoco del connettore.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Connector

La struttura che contiene i dettagli del connettore.

Tipo: oggetto DescribedConnector

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeExecution

È possibile utilizzare `DescribeExecution` per verificare i dettagli dell'esecuzione del flusso di lavoro specificato.

> **Note**
>
> Questa chiamata API restituisce solo i dettagli dei flussi di lavoro in corso.
> Se fornisci un ID per un'esecuzione che non è in corso o se l'esecuzione non corrisponde all'ID del flusso di lavoro specificato, ricevi un'`ResourceNotFound`eccezione.

Sintassi della richiesta

```
{
   "ExecutionId": "string",
   "WorkflowId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ExecutionId

Un identificatore univoco per l'esecuzione di un flusso di lavoro.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 36.

Modello: `[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}`

Campo obbligatorio: sì

WorkflowId

Un identificatore univoco per il flusso di lavoro.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Execution

La struttura che contiene i dettagli dell'esecuzione del flusso di lavoro.

Tipo: oggetto DescribedExecution

WorkflowId

Un identificatore univoco per il flusso di lavoro.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2

- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeHostKey

Restituisce i dettagli della chiave host specificata da `HostKeyId` and`ServerId`.

Sintassi della richiesta

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HostKeyId

L'identificatore della chiave host che vuoi descrivere.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 25.

Modello: `hostkey-[0-9a-f]{17}`

Campo obbligatorio: sì

ServerId

L'identificatore del server che contiene la chiave host che si desidera descrivere.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
```

```
   "HostKey": {
      "Arn": "string",
      "DateImported": number,
      "Description": "string",
      "HostKeyFingerprint": "string",
      "HostKeyId": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Type": "string"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HostKey

Restituisce i dettagli per la chiave host specificata.

Tipo: oggetto DescribedHostKey

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeProfile

Restituisce i dettagli del profilo specificato da`ProfileId`.

Sintassi della richiesta

```
{
   "ProfileId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ProfileId

L'identificatore del profilo che si desidera descrivere.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "Profile": {
      "Arn": "string",
      "As2Id": "string",
      "CertificateIds": [ "string" ],
      "ProfileId": "string",
      "ProfileType": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
```

```
        ]
    }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Profile

I dettagli del profilo specificato, restituiti come oggetto.

Tipo: oggetto DescribedProfile

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeSecurityPolicy

Descrive la politica di sicurezza collegata al server o al connettore SFTP. La risposta contiene una descrizione delle proprietà della politica di sicurezza. Per ulteriori informazioni sulle politiche di sicurezza, vedere Utilizzo delle politiche di sicurezza per i server o Utilizzo delle politiche di sicurezza per i connettori SFTP.

Sintassi della richiesta

```
{
   "SecurityPolicyName": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

SecurityPolicyName

Specificate il nome testuale della politica di sicurezza di cui desiderate i dettagli.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 100.

Modello: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "SecurityPolicy": {
      "Fips": boolean,
      "Protocols": [ "string" ],
      "SecurityPolicyName": "string",
      "SshCiphers": [ "string" ],
      "SshHostKeyAlgorithms": [ "string" ],
      "SshKexs": [ "string" ],
```

```
        "SshMacs": [ "string" ],
        "TlsCiphers": [ "string" ],
        "Type": "string"
    }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

SecurityPolicy

Un array contenente le proprietà della politica di sicurezza.

Tipo: oggetto DescribedSecurityPolicy

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

Il comando di esempio seguente utilizza il nome della politica di sicurezza come argomento e restituisce gli algoritmi per la politica di sicurezza specificata.

Richiesta di esempio

```
aws transfer describe-security-policy --security-policy-name "TransferSecurityPolicy-
FIPS-2023-05"
```

Risposta di esempio

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

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeServer

Descrive un server abilitato al protocollo di trasferimento file specificato passando il `ServerId` parametro.

La risposta contiene una descrizione delle proprietà di un server. Quando si imposta `EndpointType` su VPC, la risposta conterrà il. `EndpointDetails`

Sintassi della richiesta

```
{
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ServerId

Un identificatore univoco assegnato dal sistema per un server.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

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

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Server

Un array contenente le proprietà di un server con le proprietà `ServerID` specificate dall'utente.

Tipo: oggetto DescribedServer

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente restituisce le proprietà assegnate a un server.

Richiesta di esempio

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Esempio

Questo esempio illustra un utilizzo di. DescribeServer

Risposta di esempio

```
{
    "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
    }
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeUser

Descrive l'utente assegnato allo specifico server abilitato al protocollo di trasferimento file, come identificato dalla relativa `ServerId` proprietà.

La risposta di questa chiamata restituisce le proprietà dell'utente associato al `ServerId` valore specificato.

Sintassi della richiesta

```
{
   "ServerId": "string",
   "UserName": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui è assegnato questo utente.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

UserName

Il nome dell'utente assegnato a uno o più server. I nomi utente fanno parte delle credenziali di accesso per utilizzare il AWS Transfer Family servizio ed eseguire attività di trasferimento di file.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui è assegnato questo utente.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

User

Un array contenente le proprietà dell'utente Transfer Family per il `ServerID` valore specificato.

Tipo: oggetto DescribedUser

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente mostra i dettagli di un utente esistente.

Richiesta di esempio

```
aws transfer describe-user --server-id s-1111aaaa2222bbbb3 --user-name bob-test
```

Risposta di esempio

```
{
    "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"
    }
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DescribeWorkflow

Descrive il flusso di lavoro specificato.

Sintassi della richiesta

```
{
   "WorkflowId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

WorkflowId

Un identificatore univoco per il flusso di lavoro.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Workflow

La struttura che contiene i dettagli del flusso di lavoro.

Tipo: oggetto DescribedWorkflow

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ImportCertificate

Importa i certificati di firma e crittografia necessari per creare profili locali (AS2) e profili partner.

Sintassi della richiesta

```
{
   "ActiveDate": number,
   "Certificate": "string",
   "CertificateChain": "string",
   "Description": "string",
   "InactiveDate": number,
   "PrivateKey": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Usage": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ActiveDate

Una data opzionale che specifica quando il certificato diventa attivo.

Tipo: Timestamp

Campo obbligatorio: no

Certificate

- Per la CLI, fornisci un percorso di file per un certificato in formato URI. Ad esempio, `--certificate file://encryption-cert.pem`. In alternativa, puoi fornire il contenuto non elaborato.
- Per l'SDK, specifica il contenuto non elaborato di un file di certificato. Ad esempio, `--certificate "`cat encryption-cert.pem`"`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 16384 caratteri.

Modello: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Campo obbligatorio: sì

CertificateChain

Un elenco opzionale di certificati che compongono la catena del certificato che viene importato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 2097152.

Modello: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Campo obbligatorio: no

Description

Una breve descrizione che aiuta a identificare il certificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 200.

Modello: `[\p{Graph}]+`

Campo obbligatorio: no

InactiveDate

Una data opzionale che specifica quando il certificato cessa di essere attivo.

Tipo: Timestamp

Campo obbligatorio: no

PrivateKey

- Per la CLI, fornite un percorso di file per una chiave privata in formato URI. Ad esempio,. `--private-key file://encryption-key.pem` In alternativa, puoi fornire il contenuto non elaborato del file di chiave privata.

- Per l'SDK, specifica il contenuto non elaborato di un file di chiave privata. Ad esempio, `--private-key "`cat encryption-key.pem`"`

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 16384 caratteri.

Modello: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i certificati.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Usage

Specifica come viene utilizzato questo certificato. Può essere utilizzato nei seguenti modi:

- `SIGNING`: Per firmare messaggi AS2
- `ENCRYPTION`: Per crittografare i messaggi AS2
- `TLS`: Per proteggere le comunicazioni AS2 inviate tramite HTTPS

Tipo: stringa

Valori validi: `SIGNING | ENCRYPTION`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "CertificateId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CertificateId

Una serie di identificativi dei certificati importati. Utilizzi questo identificativo per lavorare con i profili e i profili dei partner.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 22.

Modello: `cert-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente importa un certificato da utilizzare per la crittografia. Nel primo comando, forniamo il contenuto del certificato e dei file della catena di certificati. Utilizzate questo formato per i comandi SDK.

```
aws transfer import-certificate --usage ENCRYPTION --certificate "`cat encryption-
cert.pem`" \
    --private-key "`cat encryption-key.pem`" --certificate-chain "`cat root-ca.pem`"
```

Esempio

L'esempio seguente è identico al comando precedente, tranne per il fatto che forniamo le posizioni dei file della chiave privata, del certificato e della catena di certificati. Questa versione del comando non funziona se utilizzi 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
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ImportHostKey

Aggiunge una chiave host al server specificata dal `ServerId` parametro.

Sintassi della richiesta

```
{
   "Description": "string",
   "HostKeyBody": "string",
   "ServerId": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Description

La descrizione testuale che identifica questa chiave host.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 200.

Modello: `[\p{Print}]*`

Campo obbligatorio: no

HostKeyBody

La parte della chiave privata di una coppia di chiavi SSH.

AWS Transfer Family accetta le chiavi RSA, ECDSA ed ED25519.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 4096.

Campo obbligatorio: sì

ServerId

L'identificatore del server che contiene la chiave host da importare.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Tags

Coppie chiave-valore che possono essere utilizzate per raggruppare e cercare chiavi host.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HostKeyId

Restituisce l'identificatore della chiave host per la chiave importata.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 25.

Modello: `hostkey-[0-9a-f]{17}`

ServerId

Restituisce l'identificatore del server che contiene la chiave importata.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ImportSshPublicKey

Aggiunge una chiave pubblica Secure Shell (SSH) a un utente Transfer Family identificato da un `UserName` valore assegnato allo specifico server abilitato al protocollo di trasferimento file, identificato da. `ServerId`

La risposta restituisce il `UserName` valore, il `ServerId` valore e il nome di. `SshPublicKeyId`

Sintassi della richiesta

```
{
   "ServerId": "string",
   "SshPublicKeyBody": "string",
   "UserName": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ServerId

Un identificatore univoco assegnato dal sistema per un server.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

SshPublicKeyBody

La parte della chiave pubblica di una coppia di chiavi SSH.

AWS Transfer Family accetta le chiavi RSA, ECDSA ed ED25519.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: sì

UserName

Il nome dell'utente Transfer Family assegnato a uno o più server.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ServerId": "string",
   "SshPublicKeyId": "string",
   "UserName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ServerId

Un identificatore univoco assegnato dal sistema per un server.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

SshPublicKeyId

Il nome assegnato a una chiave pubblica dal sistema che è stata importata.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza fissa di 21.

Modello: `key-[0-9a-f]{17}`

UserName

Un nome utente assegnato al `ServerID` valore specificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

Questo comando importa una chiave ECDSA memorizzata nel `id_ecdsa.pub` file.

```
aws transfer import-ssh-public-key --server-id s-021345abcdef6789 --ssh-public-key-body
 file://id_ecdsa.pub --user-name jane-doe
```

Esempio

Se si esegue il comando precedente, il sistema restituisce le seguenti informazioni.

```
{
    "ServerId": "s-021345abcdef6789",
   "SshPublicKeyId": "key-1234567890abcdef0",
   "UserName": "jane-doe"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3

- AWS SDK per Python
- AWS SDK per Ruby V3

ListAccesses

Elenca i dettagli di tutti gli accessi che hai sul tuo server.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Speciifica il numero massimo di SID di accesso da restituire.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Quando è possibile ottenere risultati aggiuntivi dalla `ListAccesses` chiamata, nell'output viene restituito un `NextToken` parametro. È quindi possibile passare un comando successivo al `NextToken` parametro per continuare a elencare gli accessi aggiuntivi.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui sono assegnati utenti.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "Accesses": [
      {
         "ExternalId": "string",
         "HomeDirectory": "string",
         "HomeDirectoryType": "string",
         "Role": "string"
      }
   ],
   "NextToken": "string",
   "ServerId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Accesses

Restituisce gli accessi e le relative proprietà per il `ServerId` valore specificato.

Tipo: matrice di oggetti ListedAccess

NextToken

Quando è possibile ottenere risultati aggiuntivi dalla `ListAccesses` chiamata, viene restituito un `NextToken` parametro nell'output. È quindi possibile passare un comando successivo al `NextToken` parametro per continuare a elencare gli accessi aggiuntivi.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui sono assegnati utenti.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListAgreements

Restituisce un elenco degli accordi per il server identificato da `ServerId` quello fornito. Se desideri limitare i risultati a un determinato numero, fornisci un valore per il `MaxResults` parametro. Se hai eseguito il comando in precedenza e hai ricevuto un valore per`NextToken`, puoi fornire quel valore per continuare a elencare gli accordi da dove li avevi interrotti.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Il numero massimo di accordi da restituire.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Quando è possibile ottenere risultati aggiuntivi dalla `ListAgreements` chiamata, viene restituito un `NextToken` parametro nell'output. È quindi possibile passare un comando successivo al `NextToken` parametro per continuare a elencare gli accordi aggiuntivi.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

ServerId

L'identificatore del server per il quale desideri un elenco di accordi.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "Agreements": [
      {
         "AgreementId": "string",
         "Arn": "string",
         "Description": "string",
         "LocalProfileId": "string",
         "PartnerProfileId": "string",
         "ServerId": "string",
         "Status": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Agreements

Restituisce un array, in cui ogni elemento contiene i dettagli di un accordo.

Tipo: matrice di oggetti ListedAgreement

NextToken

Restituisce un token che è possibile utilizzare per chiamare `ListAgreements` nuovamente e ricevere risultati aggiuntivi, se presenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListCertificates

Restituisce un elenco dei certificati correnti in cui sono stati importati AWS Transfer Family. Se desideri limitare i risultati a un determinato numero, fornisci un valore per il `MaxResults` parametro. Se hai eseguito il comando in precedenza e hai ricevuto un valore per il `NextToken` parametro, puoi fornire quel valore per continuare a elencare i certificati da dove avevi interrotto.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Il numero massimo di certificati da restituire.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Quando è possibile ottenere risultati aggiuntivi dalla `ListCertificates` chiamata, viene restituito un `NextToken` parametro nell'output. È quindi possibile passare un comando successivo al `NextToken` parametro per continuare a elencare certificati aggiuntivi.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "Certificates": [
      {
         "ActiveDate": number,
         "Arn": "string",
         "CertificateId": "string",
         "Description": "string",
         "InactiveDate": number,
         "Status": "string",
         "Type": "string",
         "Usage": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Certificates

Restituisce una matrice dei certificati specificati nella `ListCertificates` chiamata.

Tipo: matrice di oggetti ListedCertificate

NextToken

Restituisce il token successivo, che è possibile utilizzare per elencare il certificato successivo.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListConnectors

Elenca i connettori per la regione specificata.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Il numero massimo di connettori da restituire.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Quando è possibile ottenere risultati aggiuntivi dalla `ListConnectors` chiamata, viene restituito un `NextToken` parametro nell'output. È quindi possibile passare un comando successivo al `NextToken` parametro per continuare a elencare connettori aggiuntivi.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

Sintassi della risposta

```
{
```

```
   "Connectors": [
      {
         "Arn": "string",
         "ConnectorId": "string",
         "Url": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Connectors

Restituisce un array, in cui ogni elemento contiene i dettagli di un connettore.

Tipo: matrice di oggetti ListedConnector

NextToken

Restituisce un token che puoi usare per chiamare `ListConnectors` nuovamente e ricevere risultati aggiuntivi, se ce ne sono.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListExecutions

Elenca tutte le esecuzioni in corso per il flusso di lavoro specificato.

> **Note**
>
> Se l'ID del flusso di lavoro specificato non può essere trovato, `ListExecutions` restituisce un'`ResourceNotFound`eccezione.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string",
   "WorkflowId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Speciifica il numero massimo di esecuzioni da restituire.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

`ListExecutions`restituisce il `NextToken` parametro nell'output. È quindi possibile passare il `NextToken` parametro in un comando successivo per continuare a elencare le esecuzioni aggiuntive.

Ciò è utile, ad esempio, per l'impaginazione. Se hai 100 esecuzioni per un flusso di lavoro, potresti voler elencare solo le prime 10. In tal caso, chiama l'API specificando: `max-results`

```
aws transfer list-executions --max-results 10
```

Ciò restituisce i dettagli per le prime 10 esecuzioni, nonché il puntatore (`NextToken`) all'undicesima esecuzione. Ora puoi richiamare nuovamente l'API, fornendo il valore che hai ricevuto: `NextToken`

```
aws transfer list-executions --max-results 10 --next-token
$somePointerReturnedFromPreviousListResult
```

Questa chiamata restituisce le successive 10 esecuzioni, dall'undicesima alla ventesima. È quindi possibile ripetere la chiamata fino a quando non saranno stati restituiti i dettagli di tutte le 100 esecuzioni.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

WorkflowId

Un identificatore univoco per il flusso di lavoro.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "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"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Executions

Restituisce i dettagli per ogni esecuzione, in un `ListedExecution` array.

Tipo: matrice di oggetti ListedExecution

NextToken

`ListExecutions`restituisce il `NextToken` parametro nell'output. È quindi possibile passare il `NextToken` parametro in un comando successivo per continuare a elencare le esecuzioni aggiuntive.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

WorkflowId

Un identificatore univoco per il flusso di lavoro.

- Tipo: stringa

  Vincoli di lunghezza: lunghezza fissa di 19.

  Modello: `w-([a-z0-9]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListHostKeys

Restituisce un elenco di chiavi host per il server specificato dal `ServerId` parametro.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Il numero massimo di chiavi host da restituire.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Se ci sono risultati aggiuntivi che non sono stati restituiti, viene restituito un `NextToken` parametro. È possibile utilizzare quel valore per una chiamata successiva per continuare `ListHostKeys` a elencare i risultati.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

ServerId

L'identificatore del server che contiene le chiavi host che si desidera visualizzare.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "HostKeys": [
      {
         "Arn": "string",
         "DateImported": number,
         "Description": "string",
         "Fingerprint": "string",
         "HostKeyId": "string",
         "Type": "string"
      }
   ],
   "NextToken": "string",
   "ServerId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HostKeys

Restituisce un array, in cui ogni elemento contiene i dettagli di una chiave host.

Tipo: matrice di oggetti ListedHostKey

NextToken

Restituisce un token che è possibile utilizzare per chiamare `ListHostKeys` nuovamente e ricevere risultati aggiuntivi, se presenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

ServerId

Restituisce l'identificatore del server che contiene le chiavi host elencate.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListProfiles

Restituisce un elenco dei profili per il sistema. Se volete limitare i risultati a un certo numero, fornite un valore per il `MaxResults` parametro. Se hai eseguito il comando in precedenza e hai ricevuto un valore per`NextToken`, puoi fornire quel valore per continuare a elencare i profili da dove avevi interrotto.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ProfileType": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Il numero massimo di profili da restituire.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Se ci sono risultati aggiuntivi che non sono stati restituiti, viene restituito un `NextToken` parametro. È possibile utilizzare quel valore per una chiamata successiva per continuare `ListProfiles` a elencare i risultati.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

ProfileType

Indica se elencare solo i profili di tipo LOCAL o solo i profili di tipo PARTNER. Se non fornito nella richiesta, il comando elenca tutti i tipi di profili.

- Tipo: stringa

Valori validi: LOCAL | PARTNER

Campo obbligatorio: no

Sintassi della risposta

```
{
   "NextToken": "string",
   "Profiles": [
      {
         "Arn": "string",
         "As2Id": "string",
         "ProfileId": "string",
         "ProfileType": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

Restituisce un token che puoi usare per chiamare di ListProfiles nuovo e ricevere risultati aggiuntivi, se ce ne sono.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Profiles

Restituisce un array, in cui ogni elemento contiene i dettagli di un profilo.

Tipo: matrice di oggetti ListedProfile

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListSecurityPolicies

Elenca le politiche di sicurezza collegate ai server e ai connettori SFTP. Per ulteriori informazioni sulle politiche di sicurezza, vedere Utilizzo delle politiche di sicurezza per i server o Utilizzo delle politiche di sicurezza per i connettori SFTP.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Speciifica il numero di politiche di sicurezza da restituire come risposta alla `ListSecurityPolicies` query.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Quando si ottengono risultati aggiuntivi dal `ListSecurityPolicies` comando, viene restituito un `NextToken` parametro nell'output. È quindi possibile passare il `NextToken` parametro in un comando successivo per continuare a elencare le politiche di sicurezza aggiuntive.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "NextToken": "string",
   "SecurityPolicyNames": [ "string" ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

Quando è possibile ottenere risultati aggiuntivi dall'`ListSecurityPolicies`operazione, viene restituito un `NextToken` parametro nell'output. In un comando seguente, è possibile passare il `NextToken` parametro per continuare a elencare le politiche di sicurezza.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

SecurityPolicyNames

Una serie di politiche di sicurezza elencate.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 100.

Modello: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente elenca i nomi di tutte le politiche di sicurezza disponibili.

Richiesta di esempio

```
aws transfer list-security-policies
```

Risposta di esempio

```
{
    "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"
    ]
```

```
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListServers

Elenca i server abilitati al protocollo di trasferimento file associati all'account AWS .

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Speciifica il numero di server da restituire come risposta alla query. `ListServers`

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Quando si ottengono risultati aggiuntivi dal `ListServers` comando, viene restituito un `NextToken` parametro nell'output. È quindi possibile passare il `NextToken` parametro in un comando successivo per continuare a elencare server aggiuntivi.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "NextToken": "string",
```

```
   "Servers": [
      {
         "Arn": "string",
         "Domain": "string",
         "EndpointType": "string",
         "IdentityProviderType": "string",
         "LoggingRole": "string",
         "ServerId": "string",
         "State": "string",
         "UserCount": number
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

Quando è possibile ottenere risultati aggiuntivi dall'`ListServers`operazione, viene restituito un `NextToken` parametro nell'output. In un comando seguente, è possibile passare il `NextToken` parametro per continuare a elencare server aggiuntivi.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Servers

Una serie di server elencati.

Tipo: matrice di oggetti ListedServer

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente elenca i server presenti nel tuo Account AWS.

Nota che i `NextToken` valori di esempio non sono reali: servono a indicare come usare il parametro.

Richiesta di esempio

```
{
   "MaxResults": 1,
   "NextToken": "token-from-previous-API-call"
}
```

Risposta di esempio

```
{
   "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
        }
    ]
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListTagsForResource

Elenca tutti i tag associati all'Amazon Resource Name (ARN) specificato. La risorsa può essere un utente, un server o un ruolo.

Sintassi della richiesta

```
{
   "Arn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Arn

Richiede i tag associati a un particolare Amazon Resource Name (ARN). Un ARN è un identificatore per una AWS risorsa specifica, ad esempio un server, un utente o un ruolo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

MaxResults

Speciifica il numero di tag da restituire come risposta alla richiesta. `ListTagsForResource`

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Quando si richiedono risultati aggiuntivi dall'`ListTagsForResource`operazione, viene restituito un `NextToken` parametro nell'input. È quindi possibile passare un comando successivo al `NextToken` parametro per continuare a elencare tag aggiuntivi.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "Arn": "string",
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Arn

L'ARN di cui hai specificato l'elenco dei tag.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

NextToken

Quando è possibile ottenere risultati aggiuntivi dalla `ListTagsForResource` chiamata, viene restituito un `NextToken` parametro nell'output. È quindi possibile passare un comando successivo al `NextToken` parametro per continuare a elencare tag aggiuntivi.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Tags

Coppie chiave-valore assegnate a una risorsa, in genere allo scopo di raggruppare e cercare elementi. I tag sono metadati definiti dall'utente.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente elenca i tag per la risorsa con l'ARN specificato.

Richiesta di esempio

```
{
   "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef"
}
```

Esempio

Questo esempio illustra un utilizzo di. ListTagsForResource

Risposta di esempio

```
{
   "Tags": [
      {
         "Key": "Name",
         "Value": "MyServer"
      }
   ]
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2

- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListUsers

Elenca gli utenti di un server abilitato al protocollo di trasferimento file che specificate passando il `ServerId` parametro.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Speciifica il numero di utenti da restituire come risposta alla richiesta. `ListUsers`

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

Se ci sono risultati aggiuntivi dalla `ListUsers` chiamata, viene restituito un `NextToken` parametro nell'output. È quindi possibile `NextToken` passarlo a un `ListUsers` comando successivo per continuare a elencare altri utenti.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui sono assegnati utenti.

- Tipo: stringa

  Vincoli di lunghezza: lunghezza fissa di 19.

  Modello: `s-([0-9a-f]{17})`

  Campo obbligatorio: sì

Sintassi della risposta

```
{
   "NextToken": "string",
   "ServerId": "string",
   "Users": [
      {
         "Arn": "string",
         "HomeDirectory": "string",
         "HomeDirectoryType": "string",
         "Role": "string",
         "SshPublicKeyCount": number,
         "UserName": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

Quando è possibile ottenere risultati aggiuntivi dalla `ListUsers` chiamata, viene restituito un `NextToken` parametro nell'output. È quindi possibile passare un comando successivo al `NextToken` parametro per continuare a elencare altri utenti.

- Tipo: stringa

  Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui sono assegnati gli utenti.

- Tipo: stringa

  Vincoli di lunghezza: lunghezza fissa di 19.

  Modello: `s-([0-9a-f]{17})`

Users

Restituisce gli utenti di Transfer Family e le relative proprietà per il `ServerId` valore specificato.

Tipo: matrice di oggetti ListedUser

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

La chiamata `ListUsers` API restituisce un elenco di utenti associati a un server specificato dall'utente.

Richiesta di esempio

```
        {
         "MaxResults": 100,
         "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b1X0cnVuU2F0ZV9hbW91bnQiOiAyfQ==",
         "ServerId": "s-01234567890abcdef"
         }
```

Esempio

Questo è un esempio di risposta per questa chiamata API.

Risposta di esempio

```
{
   "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"
```

```
        }
    ]
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListWorkflows

Elenca tutti i flussi di lavoro associati Account AWS alla tua regione corrente.

Sintassi della richiesta

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

MaxResults

Speciifica il numero massimo di flussi di lavoro da restituire.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 1000.

Campo obbligatorio: no

NextToken

`ListWorkflows`restituisce il `NextToken` parametro nell'output. È quindi possibile passare il `NextToken` parametro in un comando successivo per continuare a elencare flussi di lavoro aggiuntivi.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "NextToken": "string",
```

```
   "Workflows": [
      {
         "Arn": "string",
         "Description": "string",
         "WorkflowId": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

`ListWorkflows`restituisce il `NextToken` parametro nell'output. È quindi possibile passare il `NextToken` parametro in un comando successivo per continuare a elencare flussi di lavoro aggiuntivi.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 6144.

Workflows

Restituisce il `Arn``WorkflowId`, e `Description` per ogni flusso di lavoro.

Tipo: matrice di oggetti ListedWorkflow

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidNextTokenException

Il `NextToken` parametro passato non è valido.

Codice di stato HTTP: 400

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

SendWorkflowStepState

Invia un callback per passaggi personalizzati asincroni.

I `ExecutionIdWorkflowId`, e `Token` vengono passati alla risorsa di destinazione durante l'esecuzione di una fase personalizzata di un flusso di lavoro. È necessario includere quelli con il relativo callback oltre a fornire uno stato.

Sintassi della richiesta

```
{
   "ExecutionId": "string",
   "Status": "string",
   "Token": "string",
   "WorkflowId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ExecutionId

Un identificatore univoco per l'esecuzione di un flusso di lavoro.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 36.

Modello: `[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}`

Campo obbligatorio: sì

Status

Indica se il passaggio specificato è riuscito o meno.

- Tipo: stringa

Valori validi: `SUCCESS | FAILURE`

Campo obbligatorio: sì

Token

Utilizzato per distinguere tra più callback per più fasi Lambda all'interno della stessa esecuzione.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 64 caratteri.

Modello: `\w+`

Campo obbligatorio: sì

WorkflowId

Un identificatore univoco per il flusso di lavoro.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartDirectoryListing

Recupera un elenco del contenuto di una directory da un server SFTP remoto. È possibile specificare l'ID del connettore, il percorso di output e il percorso della directory remota. È inoltre possibile specificare il `MaxItems` valore opzionale per controllare il numero massimo di elementi elencati dalla directory remota. Questa API restituisce un elenco di tutti i file e le directory nella directory remota (fino al valore massimo), ma non restituisce file o cartelle nelle sottodirectory. Cioè, restituisce solo un elenco di file e directory completo di un livello.

Dopo aver ricevuto il file di elenco, puoi fornire i file che desideri trasferire al `RetrieveFilePaths` parametro della chiamata `StartFileTransfer` API.

La convenzione di denominazione per il file di output è *`connector-ID-listing-ID`*`.json`. Il file di output contiene le seguenti informazioni:

- `filePath`: il percorso completo di un file remoto, relativo alla directory della richiesta di quotazione per il connettore SFTP sul server remoto.
- `modifiedTimestamp`: l'ultima volta che il file è stato modificato, nel formato dell'ora UTC. Questo campo è facoltativo. Se gli attributi del file remoto non contengono un timestamp, questo viene omesso dall'elenco dei file.
- `size`: la dimensione del file, in byte. Questo campo è facoltativo. Se gli attributi del file remoto non contengono una dimensione del file, questo viene omesso dall'elenco dei file.
- `path`: il percorso completo di una directory remota, relativo alla directory della richiesta di elenco per il connettore SFTP sul server remoto.
- `truncated`: un flag che indica se l'output della lista contiene o meno tutti gli elementi contenuti nella directory remota. Se il valore di `Truncated` output è vero, puoi aumentare il valore fornito nell'attributo `max-items` input opzionale per poter elencare più elementi (fino alla dimensione massima consentita dell'elenco di 10.000 elementi).

Sintassi della richiesta

```
{
   "ConnectorId": "string",
   "MaxItems": number,
   "OutputDirectoryPath": "string",
   "RemoteDirectoryPath": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ConnectorId

L'identificatore univoco del connettore.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Campo obbligatorio: sì

MaxItems

Un parametro opzionale in cui è possibile specificare il numero massimo di nomi di file/directory da recuperare. Il valore predefinito è 1,000.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 10000.

Campo obbligatorio: no

OutputDirectoryPath

Speciifica il percorso (bucket e prefisso) nello storage Amazon S3 per archiviare i risultati dell'elenco delle directory.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri.

Modello: `(.)+`

Campo obbligatorio: sì

RemoteDirectoryPath

Specificate la directory sul server SFTP remoto di cui desiderate elencarne il contenuto.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri.

Modello: `(.)+`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ListingId": "string",
   "OutputFileName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ListingId

Restituisce un identificatore univoco per la chiamata all'elenco delle directory.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 512 caratteri.

Modello: `[0-9a-zA-Z./-]+`

OutputFileName

Restituisce il nome del file in cui sono memorizzati i risultati. Questa è una combinazione dell'ID del connettore e dell'ID dell'elenco:`<connector-id>-<listing-id>.json`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 26. Lunghezza massima di 537.

Modello: `c-([0-9a-f]{17})-[0-9a-zA-Z./-]+.json`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente elenca il contenuto della home cartella sul server SFTP remoto, identificato dal connettore specificato. I risultati vengono inseriti nella posizione `/DOC-EXAMPLE-BUCKET/connector-files` Amazon S3 e in un file denominato. `c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json`

Richiesta di esempio

```
{
    "ConnectorId": "c-AAAA1111BBBB2222C",
    "MaxItems": "10",
    "OutputDirectoryPath": "/DOC-EXAMPLE-BUCKET/connector-files",
    "RemoteDirectoryPath": "/home"
}
```

Risposta di esempio

```
{
    "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
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartFileTransfer

Inizia un trasferimento di file tra l' AWS archiviazione locale e un server AS2 o SFTP remoto.

- Per un connettore AS2, è necessario specificare `ConnectorId` e uno o più `SendFilePaths` per identificare i file che si desidera trasferire.
- Per un connettore SFTP, il trasferimento dei file può essere in uscita o in entrata. In entrambi i casi, si specifica il. `ConnectorId` A seconda della direzione del trasferimento, si specificano anche i seguenti elementi:
  - Se trasferisci un file dal server SFTP di un partner allo storage Amazon Web Services, ne specifichi uno o più `RetrieveFilePaths` per identificare i file che desideri trasferire e `LocalDirectoryPath` a per specificare la cartella di destinazione.
  - Se trasferisci un file dal server SFTP di un partner dallo AWS storage, ne specifichi uno o più `SendFilePaths` per identificare i file che desideri trasferire e un `RemoteDirectoryPath` per specificare la cartella di destinazione.

Sintassi della richiesta

```
{
   "ConnectorId": "string",
   "LocalDirectoryPath": "string",
   "RemoteDirectoryPath": "string",
   "RetrieveFilePaths": [ "string" ],
   "SendFilePaths": [ "string" ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ConnectorId

L'identificatore univoco del connettore.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Campo obbligatorio: sì

LocalDirectoryPath

Per un trasferimento in entrata, `LocaDirectoryPath` specifica la destinazione per uno o più file trasferiti dal server SFTP del partner.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri.

Modello: `(.)+`

Campo obbligatorio: no

RemoteDirectoryPath

Per un trasferimento in uscita, `RemoteDirectoryPath` specifica la destinazione di uno o più file trasferiti al server SFTP del partner. Se non si specifica a`RemoteDirectoryPath`, la destinazione dei file trasferiti è la home directory dell'utente SFTP.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri.

Modello: `(.)+`

Campo obbligatorio: no

RetrieveFilePaths

Uno o più percorsi di origine per il server SFTP del partner. Ogni stringa rappresenta un percorso del file di origine per un trasferimento di file in entrata.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 10 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri.

Modello: `(.)+`

Campo obbligatorio: no

SendFilePaths

Uno o più percorsi di origine per lo storage Amazon S3. Ogni stringa rappresenta un percorso di file di origine per un trasferimento di file in uscita. Ad esempio, *DOC-EXAMPLE-BUCKET/myfile.txt* .

> **Note**
>
> *DOC-EXAMPLE-BUCKET* Sostituiscilo con uno dei tuoi bucket effettivi.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 10 elementi.

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri.

Modello: `(.)+`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "TransferId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

TransferId

Restituisce l'identificatore univoco per il trasferimento del file.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 512 caratteri.

Modello: `[0-9a-zA-Z./-]+`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente avvia un trasferimento di file AS2 da un server Transfer Family all'endpoint di un partner commerciale remoto. *DOC-EXAMPLE-BUCKET* Sostituiscilo con uno dei tuoi bucket attuali.

Richiesta di esempio

```
{
```

```
    "ConnectorId": "c-AAAA1111BBBB2222C",
    "SendFilePaths": [
        "/DOC-EXAMPLE-BUCKET/myfile-1.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-2.txt",
        "/DOC-EXAMPLE-BUCKET/myfile-3.txt"
    ]
}
```

Risposta di esempio

```
{
   "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Esempio

L'esempio seguente avvia un trasferimento di file dalla AWS memoria locale a un server SFTP remoto.

Richiesta di esempio

```
{
    "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"
}
```

Risposta di esempio

```
{
   "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
}
```

Esempio

L'esempio seguente avvia un trasferimento di file da un server SFTP remoto all'archiviazione locale AWS .

Richiesta di esempio

```
{
    "ConnectorId": "c-111122223333AAAAA",
    "RetrieveFilePaths": [
        "/MySFTPFolder/toTranferFamily/myfile-1.txt",
        "/MySFTPFolder/toTranferFamily/myfile-2.txt",
        "/MySFTPFolder/toTranferFamily/myfile-3.txt"
    ],
    "LocalDirectoryPath": "/DOC-EXAMPLE-BUCKET/mySourceFiles"
}
```

Risposta di esempio

```
{
   "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartServer

Modifica lo stato di un server abilitato al protocollo di trasferimento file da a`OFFLINE`. `ONLINE` Non ha alcun impatto su un server che lo è già. `ONLINE` Un `ONLINE` server può accettare ed elaborare lavori di trasferimento di file.

Lo stato di `STARTING` indica che il server si trova in uno stato intermedio, ovvero non è completamente in grado di rispondere o non è completamente online. I valori di `START_FAILED` can indicano una condizione di errore.

Non viene restituita alcuna risposta da questa chiamata.

Sintassi della richiesta

```
{
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ServerId

Un identificatore univoco assegnato dal sistema per un server avviato dall'utente.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente avvia un server.

Richiesta di esempio

```
{
   "ServerId": "s-01234567890abcdef"
```

```
}
```

Esempio

Questo è un esempio di risposta per questa chiamata API.

Risposta di esempio

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StopServer

Modifica lo stato di un server abilitato al protocollo di trasferimento file da a`ONLINE`. `OFFLINE` Un `OFFLINE` server non può accettare ed elaborare lavori di trasferimento di file. Le informazioni legate al server, come le proprietà del server e dell'utente, non vengono influenzate dall'arresto del server.

> **Note**
>
> L'arresto del server non riduce né influisce sulla fatturazione degli endpoint del protocollo di trasferimento file; è necessario eliminare il server per interrompere la fatturazione.

Lo stato di `STOPPING` indica che il server si trova in uno stato intermedio, ovvero non è completamente in grado di rispondere o non è completamente offline. I valori di `STOP_FAILED` can indicano una condizione di errore.

Non viene restituita alcuna risposta da questa chiamata.

Sintassi della richiesta

```
{
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ServerId

Un identificatore univoco assegnato dal sistema per un server che hai fermato.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente arresta un server.

Richiesta di esempio

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Esempio

Questo è un esempio di risposta per questa chiamata API.

Risposta di esempio

```
{
   "ServerId": "s-01234567890abcdef"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

TagResource

Associa una coppia chiave-valore a una risorsa, identificata dal relativo Amazon Resource Name (ARN). Le risorse sono utenti, server, ruoli e altre entità.

Non viene restituita alcuna risposta da questa chiamata.

Sintassi della richiesta

```
{
   "Arn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Arn

Un Amazon Resource Name (ARN) per una AWS risorsa specifica, come un server, un utente o un ruolo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

Tags

Coppie chiave-valore assegnate agli ARN che puoi utilizzare per raggruppare e cercare risorse per tipo. È possibile allegare questi metadati alle risorse (server, utenti, flussi di lavoro e così via) per qualsiasi scopo.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente aggiunge un tag a un server abilitato al protocollo di trasferimento file.

Richiesta di esempio

```
{
   "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
   "Tags": [
      {
         "Key": "Group",
         "Value": "Europe"
      }
   ]
}
```

Esempio

Questo esempio illustra un utilizzo di. TagResource

Risposta di esempio

```
         HTTP 200 response with an empty HTTP body.
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

TestConnection

Verifica se il connettore SFTP è configurato correttamente. Ti consigliamo vivamente di chiamare questa operazione per testare la tua capacità di trasferire file tra l' AWS archiviazione locale e il server SFTP di un partner commerciale.

Sintassi della richiesta

```
{
   "ConnectorId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ConnectorId

L'identificatore univoco del connettore.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ConnectorId": "string",
   "Status": "string",
   "StatusMessage": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ConnectorId

Restituisce l'identificatore dell'oggetto connettore che state testando.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Status

Restituisce se `OK` il test ha avuto esito positivo o `ERROR` se il test ha esito negativo.

- Tipo: stringa

StatusMessage

Restituisce `Connection succeeded` se il test ha esito positivo. In alternativa, restituisce un messaggio di errore descrittivo se il test ha esito negativo. L'elenco seguente fornisce dettagli sulla risoluzione dei problemi, a seconda del messaggio di errore ricevuto.

- Verifica che il tuo nome segreto sia allineato a quello nelle autorizzazioni Transfer Role.
- Verifica l'URL del server nella configurazione del connettore e verifica che le credenziali di accesso funzionino correttamente all'esterno del connettore.
- Verifica che il segreto esista e sia formattato correttamente.
- Verifica che la chiave host affidabile nella configurazione del connettore corrisponda all'`ssh-keyscan`output.

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente verifica la connessione a un server remoto.

```
aws transfer test-connection --connector-id c-abcd1234567890fff
```

Risposta di esempio

In caso di successo, la chiamata API restituisce i seguenti dettagli.

```
{

    "Status": "OK",

    "StatusMessage": "Connection succeeded"

}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

TestIdentityProvider

Se il server `IdentityProviderType` di un server abilitato al protocollo di trasferimento file è `AWS_DIRECTORY_SERVICE` o`API_Gateway`, verifica se il provider di identità è configurato correttamente. Ti consigliamo vivamente di richiamare questa operazione per testare il tuo metodo di autenticazione non appena crei il server. In questo modo, puoi risolvere i problemi relativi all'integrazione del provider di identità per garantire che gli utenti possano utilizzare correttamente il servizio.

I parametri `ServerId` e `UserName` sono obbligatori. I `ServerProtocol`, `SourceIp`, e `UserPassword` sono tutti opzionali.

Tieni presente quanto segue:

- Non puoi usare `TestIdentityProvider` se il `IdentityProviderType` tuo server lo è`SERVICE_MANAGED`.
- `TestIdentityProvider`non funziona con le chiavi: accetta solo password.
- `TestIdentityProvider`può testare il funzionamento delle password per un Identity Provider personalizzato che gestisce chiavi e password.
- Se si forniscono valori errati per qualsiasi parametro, il `Response` campo è vuoto.
- Se si fornisce un ID server per un server che utilizza utenti gestiti dal servizio, viene visualizzato un errore:

  ```
  An error occurred (InvalidRequestException) when calling the
  TestIdentityProvider operation: s-server-ID not configured for external
  auth
  ```

- Se si immette un ID server per il `--server-id` parametro che non identifica un server di trasferimento effettivo, viene visualizzato il seguente errore:

  ```
  An error occurred (ResourceNotFoundException) when calling the
  TestIdentityProvider operation: Unknown server.
  ```

  È possibile che il server si trovi in una regione diversa. È possibile specificare una regione aggiungendo quanto segue:`--region region-code`, ad esempio `--region us-east-2` per specificare un server negli Stati Uniti orientali (Ohio).

Sintassi della richiesta

```
{
   "ServerId": "string",
   "ServerProtocol": "string",
   "SourceIp": "string",
   "UserName": "string",
   "UserPassword": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ServerId

Un identificatore assegnato dal sistema per un server specifico. Il metodo di autenticazione utente di quel server viene testato con un nome utente e una password.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

ServerProtocol

Il tipo di protocollo di trasferimento file da testare.

I protocolli disponibili sono:

- Protocollo di trasferimento file (SFTP) Secure Shell (SSH)
- Protocollo di trasferimento file sicuro (FTPS)
- Protocollo di trasferimento file (FTP)
- Dichiarazione di applicabilità 2 (AS2)

- Tipo: stringa

Valori validi: `SFTP | FTP | FTPS | AS2`

Campo obbligatorio: no

SourceIp

L'indirizzo IP di origine dell'account da testare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 32 caratteri.

Modello: `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`

Campo obbligatorio: no

UserName

Il nome dell'account da testare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: sì

UserPassword

La password dell'account da testare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "Message": "string",
   "Response": "string",
   "StatusCode": number,
   "Url": "string"
```

```
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Message

Un messaggio che indica se il test ha avuto esito positivo o meno.

> **Note**
>
> Se viene restituita una stringa vuota, la causa più probabile è che l'autenticazione non sia riuscita a causa di un nome utente o di una password errati.

- Tipo: stringa

Response

La risposta restituita dall'API Gateway o dalla funzione Lambda.

- Tipo: stringa

StatusCode

Il codice di stato HTTP che è la risposta del tuo API Gateway o della tua funzione Lambda.

Tipo: integer

Url

L'endpoint del servizio utilizzato per autenticare un utente.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 255.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

La seguente richiesta restituisce un messaggio da un provider di identità indicante che una combinazione di nome utente e password è un'identità valida con cui utilizzare AWS Transfer Family.

Richiesta di esempio

```
{
   "ServerID": "s-01234567890abcdef",
   "UserName": "my_user",
   "UserPassword": "MyPassword-1"
}
```

Esempio

La risposta seguente mostra un esempio di risposta per un test riuscito.

Risposta di esempio

```
      "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": ""
```

Esempio

La risposta seguente indica che l'utente specificato appartiene a più di un gruppo con accesso.

```
        "Response":"",
        "StatusCode":200,
        "Message":"More than one associated access found for user's groups."
```

Esempio

Se hai creato e configurato un provider di identità personalizzato utilizzando un API Gateway, puoi inserire il seguente comando per testare il tuo utente:

`aws transfer test-identity-provider --server-id` *`s-0123456789abcdefg`* `--user-name` *`myuser`*

dove s-0123456789abcdefg è il server di trasferimento e myuser è il nome utente per l'utente personalizzato.

Se il comando ha esito positivo, la risposta è simile alla seguente, dove:

- Account AWS L'ID è 012345678901
- Il ruolo utente è user-role-api-gateway
- La home directory è myuser-bucket
- La chiave pubblica è chiave pubblica

- L'URL di chiamata è 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"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua AWS , consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UntagResource

Distacca una coppia chiave-valore da una risorsa, identificata dal relativo Amazon Resource Name (ARN). Le risorse sono utenti, server, ruoli e altre entità.

Non viene restituita alcuna risposta da questa chiamata.

Sintassi della richiesta

```
{
   "Arn": "string",
   "TagKeys": [ "string" ]
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Arn

Il valore della risorsa a cui verrà rimosso il tag. Un Amazon Resource Name (ARN) è un identificatore per una AWS risorsa specifica, come un server, un utente o un ruolo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

TagKeys

TagKeys sono coppie chiave-valore assegnate agli ARN che possono essere utilizzate per raggruppare e cercare risorse per tipo. Questi metadati possono essere allegati alle risorse per qualsiasi scopo.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 128 caratteri.

Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

Esempi

Esempio

L'esempio seguente rimuove un tag di un server abilitato al protocollo di trasferimento file.

Richiesta di esempio

```
{
   "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
   "TagKeys": "Europe" ]
}
```

Esempio

Questo esempio illustra un utilizzo di. UntagResource

Risposta di esempio

```
        HTTP 200 response with an empty HTTP body.
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateAccess

Consente di aggiornare i parametri per l'accesso specificato nei `ExternalID` parametri `ServerID` and.

Sintassi della richiesta

```
{
   "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"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ExternalId

Un identificatore univoco necessario per identificare gruppi specifici all'interno della directory. Gli utenti del gruppo che associ hanno accesso alle tue risorse Amazon S3 o Amazon EFS tramite i protocolli abilitati che utilizzano. AWS Transfer Family Se conosci il nome del gruppo, puoi visualizzare i valori SID eseguendo il seguente comando utilizzando Windows. PowerShell

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

In quel comando, sostituiscilo YourGroupNamecon il nome del tuo gruppo Active Directory.

L'espressione regolare utilizzata per convalidare questo parametro è una stringa di caratteri composta da caratteri alfanumerici maiuscoli e minuscoli senza spazi. È inoltre possibile includere caratteri di sottolineatura o uno dei seguenti caratteri: =, . @: /-

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `S-1-[\d-]+`

Campo obbligatorio: sì

HomeDirectory

La directory di destinazione (cartella) per un utente quando accede al server utilizzando il client.

Un esempio di `HomeDirectory` è `/bucket_name/home/mydirectory`.

> **Note**
>
> Il parametro `HomeDirectory` è utilizzato solo se `HomeDirectoryType` è impostato su `PATH`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

HomeDirectoryMappings

Mappature di directory logiche che specificano quali percorsi e chiavi di Amazon S3 o Amazon EFS devono essere visibili all'utente e in che modo desideri renderli visibili. È necessario specificare la `Target` coppia `Entry` and, dove `Entry` mostra come il percorso viene reso visibile

ed `Target` è il percorso effettivo di Amazon S3 o Amazon EFS. Se si specifica solo un obiettivo, questo viene visualizzato così com'è. È inoltre necessario assicurarsi che il proprio ruolo AWS Identity and Access Management (IAM) fornisca l'accesso ai percorsi in`Target`. Questo valore può essere impostato solo quando `HomeDirectoryType` è impostato su LOGICAL.

Di seguito è riportato un esempio `Target` di coppia `Entry` and.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

Nella maggior parte dei casi, è possibile utilizzare questo valore anziché la politica di sessione per bloccare l'utente nella home directory designata (» `chroot` «). A tale scopo, è possibile `Entry` impostare `/` e `Target` impostare il valore del `HomeDirectory` parametro.

Di seguito è riportato un esempio `Target` di coppia `Entry` and per`chroot`.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Tipo: matrice di oggetti HomeDirectoryMapEntry

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50000 articoli.

Campo obbligatorio: no

HomeDirectoryType

Il tipo di directory (cartella) di destinazione in cui deve trovarsi la directory home degli utenti quando accedono al server. Se lo imposti su`PATH`, l'utente vedrà il bucket Amazon S3 assoluto o il percorso Amazon EFS così com'è nei client del protocollo di trasferimento file. Se lo imposti su`LOGICAL`, devi fornire le mappature relative al modo in cui desideri rendere i percorsi Amazon S3 o Amazon EFS visibili ai tuoi utenti. `HomeDirectoryMappings`

> **Note**
>
> In caso `HomeDirectoryType` `LOGICAL` affermativo, devi fornire le mappature utilizzando il parametro. `HomeDirectoryMappings` Se, invece, `HomeDirectoryType` è`PATH`, si fornisce un percorso assoluto utilizzando il `HomeDirectory` parametro. Non puoi avere entrambi `HomeDirectory` e `HomeDirectoryMappings` nel tuo modello.

-Tipo: stringa

Valori validi: `PATH | LOGICAL`

Campo obbligatorio: no

Policy

Una policy di sessione per il tuo utente in modo da poter utilizzare lo stesso ruolo AWS Identity and Access Management (IAM) su più utenti. Questa policy limita l'accesso di un utente a porzioni del suo bucket Amazon S3. Le variabili che è possibile utilizzare all'interno di questa policy includono `${Transfer:UserName}`, `${Transfer:HomeDirectory}` e `${Transfer:HomeBucket}`.

> **Note**
>
> Questa politica si applica solo quando il dominio `ServerId` è Amazon S3. Amazon EFS non utilizza policy di sessione.
> Per le policy di sessione, AWS Transfer Family memorizza la policy come blob JSON, anziché come Amazon Resource Name (ARN) della policy. È possibile salvare la policy come blob JSON e passarla nell'argomento `Policy`.
> Per un esempio di policy di sessione, consultare Example session policy (Esempio di policy di sessione).
> Per ulteriori informazioni, consulta AssumeRoleil AWS Security Token Service API Reference.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

PosixProfile

L'identità POSIX completa, incluso ID utente (`Uid`), ID gruppo (`Gid`) e qualsiasi ID gruppo secondario (`SecondaryGids`), che controlla l'accesso degli utenti ai file system Amazon EFS. Le autorizzazioni POSIX impostate su file e directory nel file system determinano il livello di accesso che gli utenti ottengono durante il trasferimento dei file da e verso i file system Amazon EFS.

Tipo: oggetto PosixProfile

Campo obbligatorio: no

Role

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che controlla l'accesso degli utenti al bucket Amazon S3 o al file system Amazon EFS. Le policy associate a questo ruolo determineranno il livello di accesso che desideri offrire agli utenti quando trasferiscono i file da e verso il bucket Amazon S3 o il file system Amazon EFS. Il ruolo IAM deve contenere anche una relazione di trust che consente al server di accedere alle proprie risorse durante la manutenzione delle richieste di trasferimento degli utenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

ServerId

Un identificatore unico assegnato da sistema per un'istanza server. Questo è il server specifico a cui è stato aggiunto l'utente.

- Tipo: stringa

Limiti di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ExternalId": "string",
   "ServerId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ExternalId

L'identificatore esterno del gruppo i cui utenti hanno accesso alle tue risorse Amazon S3 o Amazon EFS tramite i protocolli abilitati utilizzando Transfer AWS Family.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `S-1-[\d-]+`

ServerId

L'identificatore del server a cui è collegato l'utente.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateAgreement

Aggiorna alcuni parametri per un accordo esistente. Fornisci l'`AgreementId` e `ServerId` per l'accordo che desideri aggiornare, insieme ai nuovi valori per i parametri da aggiornare.

Sintassi della richiesta

```
{
   "AccessRole": "string",
   "AgreementId": "string",
   "BaseDirectory": "string",
   "Description": "string",
   "LocalProfileId": "string",
   "PartnerProfileId": "string",
   "ServerId": "string",
   "Status": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessRole

I connettori vengono utilizzati per inviare file utilizzando il protocollo AS2 o SFTP. Per il ruolo di accesso, fornisci l'Amazon Resource Name (ARN) del AWS Identity and Access Management ruolo da utilizzare.

Per connettori AS2

Con AS2, è possibile inviare file chiamando `StartFileTransfer` e specificando i percorsi dei file nel parametro della richiesta, `SendFilePaths`. Utilizziamo la directory principale del file (ad esempio, per `--send-file-paths /bucket/dir/file.txt`, la directory principale è `/bucket/dir/`) per archiviare temporaneamente un file di messaggio AS2 elaborato, archiviare l'MDN quando lo riceviamo dal partner e scrivere un file JSON finale contenente i metadati pertinenti della trasmissione. Pertanto, `AccessRole` deve fornire l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella richiesta `StartFileTransfer`. Inoltre, devi fornire l'accesso in lettura e scrittura alla directory principale dei file che intendi inviare con `StartFileTransfer`.

Se si utilizza l'autenticazione di base per il connettore AS2, il ruolo di accesso richiede l'`secretsmanager:GetSecretValue`autorizzazione per il segreto. Se il segreto viene crittografato utilizzando una chiave gestita dal cliente anziché la chiave AWS gestita in Secrets Manager, il ruolo necessita anche dell'`kms:Decrypt`autorizzazione per quella chiave.

Per connettori SFTP

Assicurati che il ruolo di accesso fornisca l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta. Inoltre, assicurati che il ruolo fornisca l'`secretsmanager:GetSecretValue`autorizzazione a AWS Secrets Manager.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

AgreementId

Un identificatore univoco per l'accordo. Questo identificatore viene restituito quando si crea un accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `a-([0-9a-f]{17})`

Campo obbligatorio: sì

BaseDirectory

Per modificare la directory di destinazione (cartella) per i file che vengono trasferiti, fornisci la cartella bucket che desideri utilizzare, ad esempio. */DOC-EXAMPLE-BUCKET/home/mydirectory*

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

Description

Per sostituire la descrizione esistente, fornisci una breve descrizione dell'accordo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 200.

Modello: `[\p{Graph}]+`

Campo obbligatorio: no

LocalProfileId

Un identificativo univoco il profilo locale AS2.

Per modificare l'identificatore del profilo locale, inserisci qui un nuovo valore.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

PartnerProfileId

Un identificatore univoco per il profilo del partner. Per modificare l'identificatore del profilo partner, inserisci qui un nuovo valore.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

ServerId

Un identificatore unico assegnato da sistema per un'istanza server. Questo è il server specifico utilizzato dall'accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Status

È possibile aggiornare lo stato dell'accordo attivando un accordo inattivo o viceversa.

Tipo: stringa

Valori validi: `ACTIVE | INACTIVE`

Campo obbligatorio: no

Sintassi della risposta

```
{
   "AgreementId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AgreementId

Un identificatore univoco per l'accordo. Questo identificatore viene restituito quando si crea un accordo.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `a-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++

- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateCertificate

Aggiorna le date attive e inattive di un certificato.

Sintassi della richiesta

```
{
   "ActiveDate": number,
   "CertificateId": "string",
   "Description": "string",
   "InactiveDate": number
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

ActiveDate

Una data opzionale che specifica quando il certificato diventa attivo.

Tipo: Timestamp

Campo obbligatorio: no

CertificateId

L'identificatore dell'oggetto certificato che stai aggiornando.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 22.

Modello: `cert-([0-9a-f]{17})`

Campo obbligatorio: sì

Description

Una breve descrizione per aiutare a identificare il certificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 200.

Modello: `[\p{Graph}]+`

Campo obbligatorio: no

InactiveDate

Una data opzionale che specifica quando il certificato cessa di essere attivo.

Tipo: Timestamp

Campo obbligatorio: no

Sintassi della risposta

```
{
   "CertificateId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

CertificateId

Restituisce l'identificatore dell'oggetto certificato che si sta aggiornando.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa pari a 22.

Modello: `cert-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente aggiorna la data attiva di un certificato, impostando la data attiva al 16 gennaio 2022 alle 16:12:07 UTC -5 ore.

Richiesta di esempio

```
aws transfer update-certificate --certificate-id c-abcdefg123456hijk --active-date
 2022-01-16T16:12:07-05:00
```

Esempio

Di seguito è riportato un esempio di risposta per questa chiamata API.

Risposta di esempio

```
"CertificateId": "c-abcdefg123456hijk"
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateConnector

Aggiorna alcuni parametri per un connettore esistente. Fornisci `ConnectorId` il connettore che desideri aggiornare, insieme ai nuovi valori per i parametri da aggiornare.

Sintassi della richiesta

```
{
   "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"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

AccessRole

I connettori vengono utilizzati per inviare file utilizzando il protocollo AS2 o SFTP. Per il ruolo di accesso, fornisci l'Amazon Resource Name (ARN) del AWS Identity and Access Management ruolo da utilizzare.

Per connettori AS2

Con AS2, è possibile inviare file chiamando `StartFileTransfer` e specificando i percorsi dei file nel parametro della richiesta, `SendFilePaths`. Utilizziamo la directory principale del file (ad esempio, per `--send-file-paths /bucket/dir/file.txt`, la directory principale è `/bucket/dir/`) per archiviare temporaneamente un file di messaggio AS2 elaborato, archiviare l'MDN quando lo riceviamo dal partner e scrivere un file JSON finale contenente i metadati pertinenti della trasmissione. Pertanto, `AccessRole` deve fornire l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella richiesta `StartFileTransfer`. Inoltre, devi fornire l'accesso in lettura e scrittura alla directory principale dei file che intendi inviare con `StartFileTransfer`.

Se si utilizza l'autenticazione di base per il connettore AS2, il ruolo di accesso richiede l'`secretsmanager:GetSecretValue`autorizzazione per il segreto. Se il segreto viene crittografato utilizzando una chiave gestita dal cliente anziché la chiave AWS gestita in Secrets Manager, il ruolo necessita anche dell'`kms:Decrypt`autorizzazione per quella chiave.

Per connettori SFTP

Assicurati che il ruolo di accesso fornisca l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta. Inoltre, assicurati che il ruolo fornisca l'`secretsmanager:GetSecretValue`autorizzazione a AWS Secrets Manager.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

As2Config

Una struttura che contiene i parametri per un oggetto connettore AS2.

Tipo: oggetto As2ConnectorConfig

Campo obbligatorio: no

ConnectorId

L'identificatore univoco del connettore.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Campo obbligatorio: sì

LoggingRole

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a un connettore di attivare la CloudWatch registrazione per gli eventi Amazon S3. Una volta impostato, puoi visualizzare l'attività del connettore nei tuoi registri. CloudWatch

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

SecurityPolicyName

Speciifica il nome della politica di sicurezza per il connettore.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 100.

Modello: `TransferSFTPConnectorSecurityPolicy-[A-Za-z0-9-]+`

Campo obbligatorio: no

SftpConfig

Una struttura che contiene i parametri per un oggetto connettore SFTP.

Tipo: oggetto SftpConnectorConfig

Campo obbligatorio: no

Url

L'URL dell'endpoint AS2 o SFTP del partner.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 255.

Campo obbligatorio: no

Sintassi della risposta

```
{
   "ConnectorId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ConnectorId

Restituisce l'identificatore dell'oggetto connettore che state aggiornando.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateHostKey

Aggiorna la descrizione della chiave host specificata dai `HostKeyId` parametri `ServerId` and.

Sintassi della richiesta

```
{
   "Description": "string",
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Description

Una descrizione aggiornata per la chiave host.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 200.

Modello: `[\p{Print}]*`

Campo obbligatorio: sì

HostKeyId

L'identificatore della chiave host che stai aggiornando.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 25.

Modello: `hostkey-[0-9a-f]{17}`

Campo obbligatorio: sì

ServerId

L'identificatore del server che contiene la chiave host che si sta aggiornando.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "HostKeyId": "string",
   "ServerId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

HostKeyId

Restituisce l'identificatore della chiave host per la chiave host aggiornata.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 25.

Modello: `hostkey-[0-9a-f]{17}`

ServerId

Restituisce l'identificatore del server che contiene la chiave host aggiornata.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET

- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateProfile

Aggiorna alcuni parametri per un profilo esistente. Fornisci `ProfileId` il profilo che desideri aggiornare, insieme ai nuovi valori per i parametri da aggiornare.

Sintassi della richiesta

```
{
   "CertificateIds": [ "string" ],
   "ProfileId": "string"
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

CertificateIds

Una serie di identificativi dei certificati importati. Utilizzi questo identificativo per lavorare con i profili e i profili dei partner.

Tipo: matrice di stringhe

Vincoli di lunghezza: lunghezza fissa di 22.

Modello: `cert-([0-9a-f]{17})`

Campo obbligatorio: no

ProfileId

L'identificatore dell'oggetto del profilo che state aggiornando.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ProfileId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ProfileId

Restituisce l'identificatore del profilo che viene aggiornato.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateServer

Aggiorna le proprietà del server abilitato al protocollo di trasferimento file dopo la creazione del server.

La `UpdateServer` chiamata restituisce il `ServerId` nome del server aggiornato.

Sintassi della richiesta

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

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

Certificate

L'Amazon Resource Name (ARN) del AWS certificato Certificate Manager (ACM). Obbligatorio quando `Protocols` è impostato su `FTPS`.

Per richiedere un nuovo certificato pubblico, consulta Richiedere un certificato pubblico nella Guida per l'utente di AWS Certificate Manager.

Per importare un certificato esistente in ACM, consulta Importazione di certificati in ACM nella Guida per l'utente di AWS Certificate Manager.

Per richiedere un certificato privato per utilizzare FTPS tramite indirizzi IP privati, consulta Richiedere un certificato privato nella Guida per l'utente di AWS Certificate Manager.

Sono supportati i certificati con gli algoritmi di crittografia e le dimensioni delle chiavi seguenti:

- RSA a 2048 bit (RSA_2048)
- RSA a 4096 bit (RSA_4096)
- Elliptic Prime Curve a 256 bit (EC_prime256v1)
- Elliptic Prime Curve a 384 bit (EC_secp384r1)

- Elliptic Prime Curve a 521 bit (EC_secp521r1)

> **Note**
>
> Il certificato deve essere un certificato SSL/TLS X.509 versione 3 valido con FQDN o indirizzo IP specificato e le informazioni sull'emittente.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1600 caratteri.

Campo obbligatorio: no

EndpointDetails

Le impostazioni dell'endpoint del cloud privato virtuale (VPC) configurate per il server. Quando esegui l'hosting dell'endpoint all'interno del tuo VPC, puoi renderlo accessibile solo alle risorse nel VPC oppure collegarvi indirizzi IP elastici e renderlo accessibile ai client tramite Internet. I gruppi di sicurezza predefiniti del VPC vengono assegnati automaticamente all'endpoint.

Tipo: oggetto EndpointDetails

Campo obbligatorio: no

EndpointType

Il tipo di endpoint VPC che il server deve utilizzare. È possibile scegliere di rendere l'endpoint del server accessibile pubblicamente (PUBLIC) o ospitarlo all'interno del proprio VPC. Nel caso di un endpoint ospitato in un VPC, è possibile consentire l'accesso solo al server e alle risorse all'interno del VPC o scegliere di renderlo accessibile tramite Internet collegandolo direttamente a indirizzi IP elastici.

> **Note**
>
> Dopo il 19 maggio 2021, non potrai creare un server utilizzando `EndpointType=VPC_ENDPOINT` il tuo AWS account se il tuo account non l'ha già fatto prima del 19 maggio 2021. Se hai già creato dei server `EndpointType=VPC_ENDPOINT` nel tuo AWS account entro il 19 maggio 2021 o prima, non ne subirai alcuna modifica. Dopo questa data, usa `EndpointType =VPC`.
> Per ulteriori informazioni, consulta Interruzione dell'uso di VPC_ENDPOINT.

È consigliabile utilizzare `VPC` come `EndpointType`. Con questo tipo di endpoint, è possibile associare direttamente fino a tre indirizzi IPv4 elastici (anche IP BYO) all'endpoint del server e utilizzare i gruppi di sicurezza VPC per limitare il traffico tramite l'indirizzo IP pubblico del client. Questo non è possibile se `EndpointType` è impostato su `VPC_ENDPOINT`.

-Tipo: stringa

Valori validi: `PUBLIC | VPC | VPC_ENDPOINT`

Campo obbligatorio: no

HostKey

La chiave privata RSA, ECDSA o ED25519 da utilizzare per il server compatibile con SFTP. È possibile aggiungere più chiavi host, nel caso in cui si desideri ruotare le chiavi, o disporre di un set di chiavi attive che utilizzano algoritmi diversi.

Utilizzate il seguente comando per generare una chiave RSA a 2048 bit senza passphrase:

`ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key`.

Utilizzate un valore minimo di 2048 per l'opzione. `-b` È possibile creare una chiave più potente utilizzando 3072 o 4096.

Utilizzate il seguente comando per generare una chiave ECDSA a 256 bit senza passphrase:

`ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key`.

I valori validi per l'`-b`opzione per ECDSA sono 256, 384 e 521.

Utilizzate il seguente comando per generare una chiave ED25519 senza passphrase:

`ssh-keygen -t ed25519 -N "" -f my-new-server-key`.

Puoi sostituire tutti questi comandi my-new-server-keycon una stringa a tua scelta.

Important

Se non avete intenzione di migrare gli utenti esistenti da un server esistente che supporta SFTP a un nuovo server, non aggiornate la chiave host. La modifica accidentale della chiave host di un server può creare problemi.

Per ulteriori informazioni, consulta Aggiornare le chiavi host per il server compatibile con SFTP nella Guida per l'utente. AWS Transfer Family

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 4096.

Campo obbligatorio: no

IdentityProviderDetails

Un array contenente tutte le informazioni necessarie per richiamare il metodo API di autenticazione di un cliente.

Tipo: oggetto IdentityProviderDetails

Campo obbligatorio: no

LoggingRole

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a un server di attivare la CloudWatch registrazione Amazon per Amazon S3 o Amazon EFSEvents. Una volta impostato, puoi visualizzare l'attività degli utenti nei tuoi log. CloudWatch

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Modello: `(|arn:.*role/\S+)`

Campo obbligatorio: no

PostAuthenticationLoginBanner

Specifica una stringa da visualizzare quando gli utenti si connettono a un server. Questa stringa viene visualizzata dopo l'autenticazione dell'utente.

> **Note**
>
> Il protocollo SFTP non supporta banner di visualizzazione post-autenticazione.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 4096.

Modello: `[\x09-\x0D\x20-\x7E]*`

Campo obbligatorio: no

PreAuthenticationLoginBanner

Specifica una stringa da visualizzare quando gli utenti si connettono a un server. Questa stringa viene visualizzata prima dell'autenticazione dell'utente. Il seguente banner, ad esempio, mostra i dettagli sull'utilizzo 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: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 4096.

Modello: `[\x09-\x0D\x20-\x7E]*`

Campo obbligatorio: no

ProtocolDetails

Le impostazioni del protocollo configurate per il server.

- Per indicare la modalità passiva (per i protocolli FTP e FTPS), utilizza il parametro `PassiveIp`. Inserire un singolo indirizzo IPv4 composto da 4 numeri decimali separati da punti, ad esempio l'indirizzo IP esterno di un firewall, un router o un load balancer.
- Per ignorare l'errore generato quando il client tenta di utilizzare il comando `SETSTAT` su un file che stai caricando su un bucket Amazon S3, utilizza il parametro `SetStatOption`. Per fare in modo che il AWS Transfer Family server ignori il `SETSTAT` comando e carichi i file senza dover apportare modifiche al client SFTP, imposta il valore su. `ENABLE_NO_OP` Se imposti il `SetStatOption` parametro su`ENABLE_NO_OP`, Transfer Family genera una voce di registro in Amazon CloudWatch Logs, in modo da poter determinare quando il client sta effettuando una `SETSTAT` chiamata.
- Per determinare se il AWS Transfer Family server riprende le sessioni negoziate recenti tramite un ID di sessione univoco, utilizza il parametro. `TlsSessionResumptionMode`
- `As2Transports` indica il metodo di trasporto per i messaggi AS2. Attualmente è supportato solo HTTP.

Tipo: oggetto ProtocolDetails

Campo obbligatorio: no

Protocols

Specifica il protocollo o i protocolli di trasferimento file su cui il client del protocollo di trasferimento file può connettersi all'endpoint del server. I protocolli disponibili sono:

- `SFTP` (Secure Shell (SSH) File Transfer Protocol): trasferimento di file su SSH
- `FTPS` File Transfer Protocol Secure: trasferimento di file con crittografia TLS
- `FTP` (File Transfer Protocol): trasferimento file non crittografato
- `AS2`(Dichiarazione di applicabilità 2): utilizzata per il trasporto di dati strutturati business-to-business

> **Note**
>
> - Se si selezionaFTPS, è necessario scegliere un certificato archiviato in AWS Certificate Manager (ACM) che viene utilizzato per identificare il server quando i client si connettono ad esso tramite FTPS.
> - Se `Protocol` include `FTP` o `FTPS`, `EndpointType` deve essere `VPC` e `IdentityProviderType` deve essere `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
> - Se `Protocol` include `FTP`, `AddressAllocationIds` non può essere associato.
> - Se `Protocol` è impostato solo su `SFTP`, `EndpointType` può essere impostato su `PUBLIC` e `IdentityProviderType` può essere impostato uno qualunque dei tipi di identità supportati: `SERVICE_MANAGED`, `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
> - Se `Protocol` include `AS2`, `EndpointType` deve essere `VPC` e il dominio deve essere Amazon S3.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Valori validi: `SFTP | FTP | FTPS | AS2`

Campo obbligatorio: no

S3StorageOptions

Indica se le prestazioni per le tue directory Amazon S3 sono ottimizzate o meno. Questa opzione è disabilitata per impostazione predefinita.

Per impostazione predefinita, le mappature delle home directory hanno un valore di. `TYPE` `DIRECTORY` Se si abilita questa opzione, è necessario impostarla esplicitamente su `FILE` se si desidera che una mappatura abbia un file di destinazione. `HomeDirectoryMapEntry` `Type`

Tipo: oggetto S3StorageOptions

Campo obbligatorio: no

SecurityPolicyName

Speciifica il nome della politica di sicurezza per il server.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 100.

Modello: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Campo obbligatorio: no

ServerId

Un identificatore univoco assegnato dal sistema per un'istanza del server a cui è assegnato l'utente Transfer Family.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

StructuredLogDestinations

Speciifica i gruppi di log a cui vengono inviati i log del server.

Per specificare un gruppo di log, è necessario fornire l'ARN per un gruppo di log esistente. In questo caso, il formato del gruppo di log è il seguente:

`arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*`

Ad esempio, `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

Se in precedenza è stato specificato un gruppo di log per un server, è possibile cancellarlo e di fatto disattivare la registrazione strutturata fornendo un valore vuoto per questo parametro in una `update-server` chiamata. Per esempio:

```
update-server --server-id s-1234567890abcdef0 --structured-log-destinations
```

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: no

WorkflowDetails

Specifica l'ID del flusso di lavoro da assegnare e il ruolo di esecuzione utilizzato per l'esecuzione del flusso di lavoro.

Oltre a un flusso di lavoro da eseguire quando un file viene caricato completamente, `WorkflowDetails` può contenere anche un ID del flusso di lavoro (e ruolo di esecuzione) per l'esecuzione di un flusso di lavoro in caso di caricamento parziale. Un caricamento parziale si verifica quando la sessione del server si disconnette mentre il file è ancora in fase di caricamento.

Per rimuovere un flusso di lavoro associato da un server, è possibile fornire un oggetto `OnUpload` vuoto, come nel seguente esempio.

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details '{"OnUpload":[]}'
```

Tipo: oggetto WorkflowDetails

Campo obbligatorio: no

Sintassi della risposta

```
{
```

```
   "ServerId": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ServerId

Un identificatore univoco assegnato dal sistema per un server a cui è assegnato l'utente Transfer Family.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

ConflictException

Questa eccezione viene generata quando `UpdateServer` viene chiamato per un server abilitato al protocollo di trasferimento file che ha VPC come tipo di endpoint e quello del server non `VpcEndpointID` è nello stato disponibile.

Codice di stato HTTP: 400

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel servizio. AWS Transfer Family

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceExistsException

La risorsa richiesta non esiste o esiste in una regione diversa da quella specificata per il comando.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente aggiorna il ruolo di un server.

Richiesta di esempio

```
{
   "EndpointDetails": {
   "VpcEndpointId": "vpce-01234f056f3g13",
   "LoggingRole": "CloudWatchS3Events",
   "ServerId": "s-01234567890abcdef"
```

```
    }
}
```

Esempio

L'esempio seguente rimuove tutti i flussi di lavoro associati dal server.

Richiesta di esempio

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
 '{"OnUpload":[]}'
```

Esempio

Questo è un esempio di risposta per questa chiamata API.

Risposta di esempio

```
{
    "ServerId": "s-01234567890abcdef"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

UpdateUser

Assegna nuove proprietà a un utente. I parametri passati modificano alcuni o tutti i seguenti elementi: la home directory, il ruolo e la politica per il `UserName` e specificati dall'`ServerId`utente.

La risposta restituisce `ServerId` and the `UserName` per l'utente aggiornato.

Nella console, puoi selezionare Restricted quando crei o aggiorni un utente. Ciò garantisce che l'utente non possa accedere a nulla al di fuori della propria home directory. Il modo programmatico per configurare questo comportamento consiste nell'aggiornare l'utente. `HomeDirectoryType`Impostateli su `LOGICAL` e `HomeDirectoryMappings` specificateli con `Entry` as root (`/`) e `Target` come directory home.

Ad esempio, se la home directory dell'utente è`/test/admin-user`, il comando seguente aggiorna l'utente in modo che la sua configurazione nella console mostri il flag Restricted come selezionato.

```
aws transfer update-user --server-id <server-id> --user-name admin-user --
home-directory-type LOGICAL --home-directory-mappings "[{\"Entry\":\"/\",
\"Target\":\"/test/admin-user\"}]"
```

Sintassi della richiesta

```
{
   "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"
```

```
}
```

Parametri della richiesta

Per informazioni sui parametri comuni per tutte le azioni, consulta Parametri comuni.

La richiesta accetta i seguenti dati in formato JSON.

HomeDirectory

La directory di destinazione (cartella) per un utente quando accede al server utilizzando il client.

Un esempio di `HomeDirectory` è `/bucket_name/home/mydirectory`.

> **Note**
>
> Il parametro `HomeDirectory` è utilizzato solo se `HomeDirectoryType` è impostato su `PATH`.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

HomeDirectoryMappings

Mappature di directory logiche che specificano quali percorsi e chiavi di Amazon S3 o Amazon EFS devono essere visibili all'utente e in che modo desideri renderli visibili. È necessario specificare la `Target` coppia `Entry` and, dove `Entry` mostra come il percorso viene reso visibile ed `Target` è il percorso effettivo di Amazon S3 o Amazon EFS. Se si specifica solo un obiettivo, questo viene visualizzato così com'è. È inoltre necessario assicurarsi che il proprio ruolo AWS Identity and Access Management (IAM) fornisca l'accesso ai percorsi in`Target`. Questo valore può essere impostato solo quando `HomeDirectoryType` è impostato su LOGICAL.

Di seguito è riportato un esempio `Target` di coppia `Entry` and.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/
mydirectory" } ]
```

Nella maggior parte dei casi, è possibile utilizzare questo valore anziché la politica di sessione per bloccare l'utente nella home directory designata (» `chroot` «). A tale scopo, è possibile `Entry` impostare '/' e `Target` impostare il valore del HomeDirectory parametro.

Di seguito è riportato un esempio `Target` di coppia `Entry` and per`chroot`.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Tipo: matrice di oggetti HomeDirectoryMapEntry

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50000 articoli.

Campo obbligatorio: no

HomeDirectoryType

Il tipo di directory (cartella) di destinazione in cui deve trovarsi la directory home degli utenti quando accedono al server. Se lo imposti su`PATH`, l'utente vedrà il bucket Amazon S3 assoluto o il percorso Amazon EFS così com'è nei client del protocollo di trasferimento file. Se lo imposti su`LOGICAL`, devi fornire le mappature relative al modo in cui desideri rendere i percorsi Amazon S3 o Amazon EFS visibili ai tuoi utenti. `HomeDirectoryMappings`

> **Note**
>
> In caso `HomeDirectoryType` `LOGICAL` affermativo, devi fornire le mappature utilizzando il parametro. `HomeDirectoryMappings` Se, invece, `HomeDirectoryType` è`PATH`, si fornisce un percorso assoluto utilizzando il `HomeDirectory` parametro. Non puoi avere entrambi `HomeDirectory` e `HomeDirectoryMappings` nel tuo modello.

-Tipo: stringa

Valori validi: `PATH | LOGICAL`

Campo obbligatorio: no

Policy

Una policy di sessione per il tuo utente in modo da poter utilizzare lo stesso ruolo AWS Identity and Access Management (IAM) su più utenti. Questa policy limita l'accesso di un utente a porzioni del suo bucket Amazon S3. Le variabili che è possibile utilizzare all'interno

di questa policy includono `${Transfer:UserName}`, `${Transfer:HomeDirectory}` e `${Transfer:HomeBucket}`.

> **Note**
>
> Questa politica si applica solo quando il dominio `ServerId` è Amazon S3. Amazon EFS non utilizza policy di sessione.
> Per le policy di sessione, AWS Transfer Family memorizza la policy come blob JSON, anziché come Amazon Resource Name (ARN) della policy. È possibile salvare la policy come blob JSON e passarla nell'argomento `Policy`.
> Per un esempio di policy di sessione, consultare Example session policy (Esempio di policy di sessione).
> Per ulteriori informazioni, consulta AssumeRoleil AWS Security Token Service API Reference.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

PosixProfile

Speciifica l'identità POSIX completa, inclusi l'ID utente (`Uid`), l'ID di gruppo (`Gid`) e gli eventuali ID di gruppo secondari (`SecondaryGids`), che controlla l'accesso degli utenti ai tuoi Amazon Elastic File System (Amazon EFS). Le autorizzazioni POSIX impostate su file e directory nel tuo file system determinano il livello di accesso che gli utenti ottengono quando trasferiscono file da e verso i tuoi file system Amazon EFS.

Tipo: oggetto PosixProfile

Campo obbligatorio: no

Role

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che controlla l'accesso degli utenti al bucket Amazon S3 o al file system Amazon EFS. Le policy associate a questo ruolo determineranno il livello di accesso che desideri offrire agli utenti quando trasferiscono i file da e verso il bucket Amazon S3 o il file system Amazon EFS. Il ruolo IAM deve

contenere anche una relazione di trust che consente al server di accedere alle proprie risorse durante la manutenzione delle richieste di trasferimento degli utenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

ServerId

Un identificatore univoco assegnato dal sistema per un'istanza del server Transfer Family a cui è assegnato l'utente.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

UserName

Una stringa univoca che identifica un utente ed è associata a un server come specificato da `ServerId`. Questo nome utente deve essere composto da un minimo di 3 a un massimo di 100 caratteri. I seguenti sono caratteri validi: a-z, A-Z, 0-9, carattere di sottolineatura '_', trattino '-', punto '.' e chiocciola '@'. Il nome utente non può iniziare con un trattino, un punto o una chiocciola.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: sì

Sintassi della risposta

```
{
   "ServerId": "string",
```

```
   "UserName": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ServerId

Un identificatore univoco assegnato dal sistema per un'istanza del server Transfer Family a cui è assegnato l'account.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

UserName

L'identificatore univoco di un utente assegnato a un'istanza del server specificata nella richiesta.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

InternalServiceError

Questa eccezione viene generata quando si verifica un errore nel AWS Transfer Family servizio.

Codice di stato HTTP: 500

InvalidRequestException

Questa eccezione viene generata quando il client invia una richiesta non valida.

Codice di stato HTTP: 400

ResourceNotFoundException

Questa eccezione viene generata quando una risorsa non viene trovata dal servizio AWS Transfer Family.

Codice di stato HTTP: 400

ServiceUnavailableException

La richiesta non è riuscita perché il servizio AWS Transfer Family non è disponibile.

Codice di stato HTTP: 500

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

Esempi

Esempio

L'esempio seguente aggiorna un utente Transfer Family.

Richiesta di esempio

```
{
   "HomeDirectory": "/bucket2/documentation",
   "HomeDirectoryMappings": [
      {
         "Entry": "/directory1",
         "Target": "/bucket_name/home/mydirectory"
      }
   ],
   "HomeDirectoryType:" "PATH",
   "Role": "AssumeRole",
   "ServerId": "s-01234567890abcdef",
   "UserName": "my_user"
}
```

Esempio

Questo è un esempio di risposta per questa chiamata API.

Risposta di esempio

```
{
   "ServerId": "s-01234567890abcdef",
   "UserName": "my_user"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

Tipi di dati

Sono supportati i tipi di dati seguenti:

- 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 i dettagli per un oggetto connettore AS2. L'oggetto connettore viene utilizzato per i processi AS2 in uscita, per connettere il AWS Transfer Family cliente con il partner commerciale.

Indice

BasicAuthSecretId

Fornisce supporto di autenticazione di base all'API AS2 Connectors. Per utilizzare l'autenticazione di base, devi fornire il nome o Amazon Resource Name (ARN) di un secret in. AWS Secrets Manager

Il valore predefinito per questo parametro è`null`, che indica che l'autenticazione di base non è abilitata per il connettore.

Se il connettore deve utilizzare l'autenticazione di base, il segreto deve avere il seguente formato:

```
{ "Username": "user-name", "Password": "user-password" }
```

Sostituisci `user-name` e `user-password` con le credenziali dell'utente effettivo che viene autenticato.

Tieni presente quanto segue:

- Stai archiviando queste credenziali in Secrets Manager, non passandole direttamente a questa API.
- Se utilizzi l'API, gli SDK o CloudFormation per configurare il connettore, devi creare il segreto prima di poter abilitare l'autenticazione di base. Tuttavia, se utilizzi la console di AWS gestione, puoi fare in modo che il sistema crei il segreto per te.

Se in precedenza hai abilitato l'autenticazione di base per un connettore, puoi disabilitarla utilizzando la chiamata `UpdateConnector` API. Ad esempio, se si utilizza la CLI, è possibile eseguire il comando seguente per rimuovere l'autenticazione di base:

```
update-connector --connector-id my-connector-id --as2-config
'BasicAuthSecretId=""'
```

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

Compression

Speciifica se il file AS2 è compresso.

- Tipo: stringa

Valori validi: `ZLIB | DISABLED`

Campo obbligatorio: no

EncryptionAlgorithm

L'algoritmo utilizzato per crittografare il file.

Tieni presente quanto segue:

- Non utilizzare l'`DES_EDE3_CBC`algoritmo a meno che non sia necessario supportare un client legacy che lo richiede, poiché si tratta di un algoritmo di crittografia debole.
- È possibile specificare solo `NONE` se l'URL del connettore utilizza HTTPS. L'utilizzo di HTTPS garantisce che nessun traffico venga inviato in formato non crittografato.

- Tipo: stringa

Valori validi: `AES128_CBC | AES192_CBC | AES256_CBC | DES_EDE3_CBC | NONE`

Campo obbligatorio: no

LocalProfileId

Un identificativo univoco il profilo locale AS2.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

MdnResponse

Utilizzato per le richieste in uscita (da un AWS Transfer Family server a un server AS2 partner) per determinare se la risposta del partner per i trasferimenti è sincrona o asincrona. Specificare uno dei seguenti valori:

- SYNC: Il sistema prevede una risposta MDN sincrona, che confermi che il file è stato trasferito correttamente (o meno).
- NONE: specifica che non è richiesta alcuna risposta MDN.

-Tipo: stringa

Valori validi: SYNC | NONE

Campo obbligatorio: no

MdnSigningAlgorithm

L'algoritmo di firma per la risposta MDN.

> **Note**
>
> Se impostato su DEFAULT (o non impostato affatto), SigningAlgorithm viene utilizzato il valore di.

-Tipo: stringa

Valori validi: SHA256 | SHA384 | SHA512 | SHA1 | NONE | DEFAULT

Campo obbligatorio: no

MessageSubject

Utilizzato come attributo di intestazione Subject HTTP nei messaggi AS2 inviati con il connettore.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri.

Modello: [\p{Print}\p{Blank}]+

Campo obbligatorio: no

PartnerProfileId

Un identificatore univoco per il profilo partner del connettore.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

SigningAlgorithm

L'algoritmo utilizzato per firmare i messaggi AS2 inviati con il connettore.

-Tipo: stringa

Valori validi: `SHA256 | SHA384 | SHA512 | SHA1 | NONE`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

CopyStepDetails

Ogni tipo di passo ha una propria `StepDetails` struttura.

Indice

DestinationFileLocation

Specificate la posizione del file da copiare. Usa `${Transfer:UserName}` o `${Transfer:UploadDate}` in questo campo per parametrizzare il prefisso di destinazione in base al nome utente o alla data di caricamento.

- Imposta il valore di `DestinationFileLocation` `${Transfer:UserName}` to per copiare i file caricati in un bucket Amazon S3 con il prefisso del nome dell'utente Transfer Family che ha caricato il file.
- Imposta il valore di `DestinationFileLocation` `${Transfer:UploadDate}` to per copiare i file caricati in un bucket Amazon S3 con il prefisso della data di caricamento.

> **Note**
>
> Il sistema utilizza un formato di data AAAA-MM-GG, in base *`UploadDate`* alla data di caricamento del file in formato UTC.

Tipo: oggetto InputFileLocation

Campo obbligatorio: no

Name

Il nome della fase, utilizzato come identificatore.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 30.

Modello: `[\w-]*`

Campo obbligatorio: no

OverwriteExisting

Un contrassegno che indica se sovrascrivere o meno un file esistente con lo stesso nome. Il valore predefinito è `FALSE`.

Se il flusso di lavoro sta elaborando un file con lo stesso nome di un file esistente, il comportamento è il seguente:

- In caso `OverwriteExisting` `TRUE` affermativo, il file esistente viene sostituito con il file in fase di elaborazione.
- In caso `OverwriteExisting` `FALSE` affermativo, non accade nulla e l'elaborazione del flusso di lavoro si interrompe.

-Tipo: stringa

Valori validi: `TRUE | FALSE`

Campo obbligatorio: no

SourceFileLocation

Speciifica il file da utilizzare come input per la fase del flusso di lavoro: l'output del passaggio precedente o il file originariamente caricato per il flusso di lavoro.

- Per utilizzare il file precedente come input, immettere`${previous.file}`. In questo caso, questa fase del flusso di lavoro utilizza come input il file di output della fase precedente del flusso di lavoro. Si tratta del valore di default.
- Per utilizzare la posizione del file originariamente caricato come input per questo passaggio, inserisci`${original.file}`.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `\$\{(\w+.)+\w+\}`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

CustomStepDetails

Ogni tipo di passo ha una propria `StepDetails` struttura.

Indice

Name

Il nome della fase, utilizzato come identificatore.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 30.

Modello: `[\w-]*`

Campo obbligatorio: no

SourceFileLocation

Speciifica il file da utilizzare come input per la fase del flusso di lavoro: l'output del passaggio precedente o il file originariamente caricato per il flusso di lavoro.

- Per utilizzare il file precedente come input, immettere`${previous.file}`. In questo caso, questa fase del flusso di lavoro utilizza come input il file di output della fase precedente del flusso di lavoro. Si tratta del valore di default.
- Per utilizzare la posizione del file originariamente caricato come input per questo passaggio, inserisci`${original.file}`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `\$\{(\w+.)+\w+\}`

Campo obbligatorio: no

Target

L'ARN per la funzione Lambda che viene chiamata.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 170.

Modello: `arn:[a-z-]+:lambda:.*`

Campo obbligatorio: no

TimeoutSeconds

Timeout, in secondi, per il passaggio.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo di 1800.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DecryptStepDetails

Ogni tipo di passo ha una propria `StepDetails` struttura.

Indice

DestinationFileLocation

Speciifica la posizione del file da decifrare. Usa `${Transfer:UserName}` o `${Transfer:UploadDate}` in questo campo per parametrizzare il prefisso di destinazione in base al nome utente o alla data di caricamento.

- Imposta il valore di `DestinationFileLocation` to per `${Transfer:UserName}` decrittografare i file caricati in un bucket Amazon S3 con il prefisso del nome dell'utente Transfer Family che ha caricato il file.
- Imposta il valore di `DestinationFileLocation` `${Transfer:UploadDate}` to per decrittografare i file caricati in un bucket Amazon S3 con il prefisso della data di caricamento.

> **Note**
>
> Il sistema utilizza un formato di data AAAA-MM-GG, in base *`UploadDate`* alla data di caricamento del file in formato UTC.

Tipo: oggetto InputFileLocation

Campo obbligatorio: sì

Type

Il tipo di crittografia utilizzato. Attualmente, questo valore deve esserePGP.

-Tipo: stringa

Valori validi: `PGP`

Campo obbligatorio: sì

Name

Il nome della fase, utilizzato come identificatore.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 30.

Modello: `[\w-]*`

Campo obbligatorio: no

OverwriteExisting

Un contrassegno che indica se sovrascrivere o meno un file esistente con lo stesso nome. Il valore predefinito è `FALSE`.

Se il flusso di lavoro sta elaborando un file con lo stesso nome di un file esistente, il comportamento è il seguente:

- In caso `OverwriteExisting` `TRUE` affermativo, il file esistente viene sostituito con il file in fase di elaborazione.
- In caso `OverwriteExisting` `FALSE` affermativo, non accade nulla e l'elaborazione del flusso di lavoro si interrompe.

Tipo: stringa

Valori validi: `TRUE | FALSE`

Campo obbligatorio: no

SourceFileLocation

Speciifica il file da utilizzare come input per la fase del flusso di lavoro: l'output del passaggio precedente o il file originariamente caricato per il flusso di lavoro.

- Per utilizzare il file precedente come input, immettere`${previous.file}`. In questo caso, questa fase del flusso di lavoro utilizza come input il file di output della fase precedente del flusso di lavoro. Si tratta del valore di default.
- Per utilizzare la posizione del file originariamente caricato come input per questo passaggio, inserisci`${original.file}`.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `\$\{(\w+.)+\w+\}`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DeleteStepDetails

Il nome del passaggio, utilizzato per identificare il passaggio di eliminazione.

Indice

Name

Il nome del passaggio, utilizzato come identificatore.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 30.

Modello: `[\w-]*`

Campo obbligatorio: no

SourceFileLocation

Speciifica il file da utilizzare come input per la fase del flusso di lavoro: l'output del passaggio precedente o il file originariamente caricato per il flusso di lavoro.

- Per utilizzare il file precedente come input, immettere`${previous.file}`. In questo caso, questa fase del flusso di lavoro utilizza come input il file di output della fase precedente del flusso di lavoro. Si tratta del valore di default.
- Per utilizzare la posizione del file originariamente caricato come input per questo passaggio, inserisci`${original.file}`.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `\$\{(\w+.)+\w+\}`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++

- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedAccess

Descrive le proprietà dell'accesso specificato.

Indice

ExternalId

Un identificatore univoco necessario per identificare gruppi specifici all'interno della directory. Gli utenti del gruppo che associ hanno accesso alle tue risorse Amazon S3 o Amazon EFS tramite i protocolli abilitati che utilizzano. AWS Transfer Family Se conosci il nome del gruppo, puoi visualizzare i valori SID eseguendo il seguente comando utilizzando Windows. PowerShell

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

In quel comando, sostituiscilo YourGroupNamecon il nome del tuo gruppo Active Directory.

L'espressione regolare utilizzata per convalidare questo parametro è una stringa di caratteri composta da caratteri alfanumerici maiuscoli e minuscoli senza spazi. È inoltre possibile includere caratteri di sottolineatura o uno dei seguenti caratteri: =, . @: /-

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `S-1-[\d-]+`

Campo obbligatorio: no

HomeDirectory

La directory di destinazione (cartella) per un utente quando accede al server utilizzando il client.

Un esempio di `HomeDirectory` è `/bucket_name/home/mydirectory`.

> **Note**
>
> Il parametro `HomeDirectory` è utilizzato solo se `HomeDirectoryType` è impostato su `PATH`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

HomeDirectoryMappings

Mappature di directory logiche che specificano quali percorsi e chiavi di Amazon S3 o Amazon EFS devono essere visibili all'utente e in che modo desideri renderli visibili. È necessario specificare la `Target` coppia `Entry` and, dove `Entry` mostra come il percorso viene reso visibile ed `Target` è il percorso effettivo di Amazon S3 o Amazon EFS. Se si specifica solo un obiettivo, questo viene visualizzato così com'è. È inoltre necessario assicurarsi che il proprio ruolo AWS Identity and Access Management (IAM) fornisca l'accesso ai percorsi in`Target`. Questo valore può essere impostato solo quando `HomeDirectoryType` è impostato su LOGICAL.

Nella maggior parte dei casi, è possibile utilizzare questo valore anziché la politica di sessione per bloccare l'accesso associato alla home directory designata (» `chroot` «). A tale scopo, è possibile `Entry` impostare '/' e `Target` impostare il valore del `HomeDirectory` parametro.

Tipo: matrice di oggetti HomeDirectoryMapEntry

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50000 articoli.

Campo obbligatorio: no

HomeDirectoryType

Il tipo di directory (cartella) di destinazione in cui deve trovarsi la directory home degli utenti quando accedono al server. Se lo imposti su`PATH`, l'utente vedrà il bucket Amazon S3 assoluto o il percorso Amazon EFS così com'è nei client del protocollo di trasferimento file. Se lo imposti su`LOGICAL`, devi fornire le mappature relative al modo in cui desideri rendere i percorsi Amazon S3 o Amazon EFS visibili ai tuoi utenti. `HomeDirectoryMappings`

> **Note**
>
> In caso `HomeDirectoryType` `LOGICAL` affermativo, devi fornire le mappature utilizzando il parametro. `HomeDirectoryMappings` Se, invece, `HomeDirectoryType` è`PATH`, si fornisce un percorso assoluto utilizzando il `HomeDirectory` parametro. Non puoi avere entrambi `HomeDirectory` e `HomeDirectoryMappings` nel tuo modello.

- Tipo: stringa

Valori validi: `PATH | LOGICAL`

Campo obbligatorio: no

Policy

Una policy di sessione per il tuo utente in modo da poter utilizzare lo stesso ruolo AWS Identity and Access Management (IAM) su più utenti. Questa policy limita l'accesso di un utente a porzioni del suo bucket Amazon S3. Le variabili che è possibile utilizzare all'interno di questa policy includono `${Transfer:UserName}`, `${Transfer:HomeDirectory}` e `${Transfer:HomeBucket}`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

PosixProfile

L'identità POSIX completa, incluso ID utente (`Uid`), ID gruppo (`Gid`) e qualsiasi ID gruppo secondario (`SecondaryGids`), che controlla l'accesso degli utenti ai file system Amazon EFS. Le autorizzazioni POSIX impostate su file e directory nel file system determinano il livello di accesso che gli utenti ottengono durante il trasferimento dei file da e verso i file system Amazon EFS.

Tipo: oggetto PosixProfile

Campo obbligatorio: no

Role

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che controlla l'accesso degli utenti al bucket Amazon S3 o al file system Amazon EFS. Le policy associate a questo ruolo determineranno il livello di accesso che desideri offrire agli utenti quando trasferiscono i file da e verso il bucket Amazon S3 o il file system Amazon EFS. Il ruolo IAM deve contenere anche una relazione di trust che consente al server di accedere alle proprie risorse durante la manutenzione delle richieste di trasferimento degli utenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta AWS quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedAgreement

Descrive le proprietà di un accordo.

Indice

Arn

L'Amazon Resource Name (ARN) univoco per l'accordo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

AccessRole

I connettori vengono utilizzati per inviare file utilizzando il protocollo AS2 o SFTP. Per il ruolo di accesso, fornisci l'Amazon Resource Name (ARN) del AWS Identity and Access Management ruolo da utilizzare.

Per connettori AS2

Con AS2, è possibile inviare file chiamando `StartFileTransfer` e specificando i percorsi dei file nel parametro della richiesta, `SendFilePaths`. Utilizziamo la directory principale del file (ad esempio, per `--send-file-paths /bucket/dir/file.txt`, la directory principale è `/bucket/dir/`) per archiviare temporaneamente un file di messaggio AS2 elaborato, archiviare l'MDN quando lo riceviamo dal partner e scrivere un file JSON finale contenente i metadati pertinenti della trasmissione. Pertanto, `AccessRole` deve fornire l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella richiesta `StartFileTransfer`. Inoltre, devi fornire l'accesso in lettura e scrittura alla directory principale dei file che intendi inviare con `StartFileTransfer`.

Se si utilizza l'autenticazione di base per il connettore AS2, il ruolo di accesso richiede l'`secretsmanager:GetSecretValue`autorizzazione per il segreto. Se il segreto viene crittografato utilizzando una chiave gestita dal cliente anziché la chiave AWS gestita in Secrets Manager, il ruolo necessita anche dell'`kms:Decrypt`autorizzazione per quella chiave.

Per connettori SFTP

Assicurati che il ruolo di accesso fornisca l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta. Inoltre, assicurati che il ruolo fornisca l'`secretsmanager:GetSecretValue`autorizzazione a AWS Secrets Manager.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

AgreementId

Un identificatore univoco per l'accordo. Questo identificatore viene restituito quando si crea un accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `a-([0-9a-f]{17})`

Campo obbligatorio: no

BaseDirectory

La directory (cartella) di destinazione per i file trasferiti utilizzando il protocollo AS2.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

Description

Il nome o la descrizione breve utilizzata per identificare il contratto.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 200.

Modello: `[\p{Graph}]+`

Campo obbligatorio: no

LocalProfileId

Un identificativo univoco il profilo locale AS2.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

PartnerProfileId

Un identificativo univoco del profilo del partner utilizzato nel contratto.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

ServerId

Un identificatore unico assegnato da sistema per un'istanza server. Questo identificativo indica il server specifico utilizzato dal contratto.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: no

Status

Lo stato attuale del contratto, `ACTIVE` o `INACTIVE`.

- Tipo: stringa

Valori validi: `ACTIVE | INACTIVE`

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i contratti.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedCertificate

Descrive le proprietà di un certificato.

Indice

Arn

Il nome della risorsa Amazon (ARN) del certificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

ActiveDate

Una data opzionale che specifica quando il certificato diventa attivo.

Tipo: Timestamp

Campo obbligatorio: no

Certificate

Il nome del file del certificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 16384 caratteri.

Modello: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Campo obbligatorio: no

CertificateChain

L'elenco dei certificati che costituiscono la catena del certificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 2097152.

Modello: `[\u0009\u000A\u000D\u0020-\u00FF]*`

Campo obbligatorio: no

CertificateId

Una serie di identificativi dei certificati importati. Utilizzi questo identificativo per lavorare con i profili e i profili dei partner.

- Tipo: stringa

Limiti di lunghezza: lunghezza fissa di 22.

Modello: `cert-([0-9a-f]{17})`

Campo obbligatorio: no

Description

Il nome o la descrizione utilizzati per identificare il certificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 200.

Modello: `[\p{Graph}]+`

Campo obbligatorio: no

InactiveDate

Una data opzionale che specifica quando il certificato cessa di essere attivo.

Tipo: Timestamp

Campo obbligatorio: no

NotAfterDate

La data finale di validità del certificato.

Tipo: Timestamp

Campo obbligatorio: no

NotBeforeDate

La prima data di validità del certificato.

Tipo: Timestamp

Campo obbligatorio: no

Serial

Il numero di serie del certificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 48.

Modello: `[\p{XDigit}{2}:?]*`

Campo obbligatorio: no

Status

Il certificato può essere `ACTIVE`, `PENDING_ROTATION` o `INACTIVE`. `PENDING_ROTATION` significa che questo certificato sostituirà il certificato corrente alla scadenza.

- Tipo: stringa

Valori validi: `ACTIVE | PENDING_ROTATION | INACTIVE`

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i certificati.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Type

Se per il certificato è stata specificata una chiave privata, il tipo è `CERTIFICATE_WITH_PRIVATE_KEY`. Se non esiste una chiave privata, il tipo è `CERTIFICATE`.

- Tipo: stringa

Valori validi: `CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY`

Campo obbligatorio: no

Usage

Specifica come viene utilizzato questo certificato. Può essere utilizzato nei seguenti modi:

- `SIGNING`: Per firmare messaggi AS2
- `ENCRYPTION`: Per crittografare i messaggi AS2
- `TLS`: Per proteggere le comunicazioni AS2 inviate tramite HTTPS

-Tipo: stringa

Valori validi: `SIGNING | ENCRYPTION`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedConnector

Descrive i parametri per il connettore, come identificato da`ConnectorId`.

Indice

Arn

L'Amazon Resource Name (ARN) univoco per il connettore.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

AccessRole

I connettori vengono utilizzati per inviare file utilizzando il protocollo AS2 o SFTP. Per il ruolo di accesso, fornisci l'Amazon Resource Name (ARN) del AWS Identity and Access Management ruolo da utilizzare.

Per connettori AS2

Con AS2, è possibile inviare file chiamando `StartFileTransfer` e specificando i percorsi dei file nel parametro della richiesta, `SendFilePaths`. Utilizziamo la directory principale del file (ad esempio, per `--send-file-paths /bucket/dir/file.txt`, la directory principale è `/bucket/dir/`) per archiviare temporaneamente un file di messaggio AS2 elaborato, archiviare l'MDN quando lo riceviamo dal partner e scrivere un file JSON finale contenente i metadati pertinenti della trasmissione. Pertanto, `AccessRole` deve fornire l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella richiesta `StartFileTransfer`. Inoltre, devi fornire l'accesso in lettura e scrittura alla directory principale dei file che intendi inviare con `StartFileTransfer`.

Se si utilizza l'autenticazione di base per il connettore AS2, il ruolo di accesso richiede l'`secretsmanager:GetSecretValue`autorizzazione per il segreto. Se il segreto viene crittografato utilizzando una chiave gestita dal cliente anziché la chiave AWS gestita in Secrets Manager, il ruolo necessita anche dell'`kms:Decrypt`autorizzazione per quella chiave.

Per connettori SFTP

Assicurati che il ruolo di accesso fornisca l'accesso in lettura e scrittura alla directory principale della posizione del file utilizzata nella `StartFileTransfer` richiesta. Inoltre, assicurati che il ruolo fornisca l'`secretsmanager:GetSecretValue`autorizzazione a AWS Secrets Manager.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

As2Config

Una struttura che contiene i parametri per un oggetto connettore AS2.

Tipo: oggetto As2ConnectorConfig

Campo obbligatorio: no

ConnectorId

L'identificatore univoco del connettore.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Campo obbligatorio: no

LoggingRole

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a un connettore di attivare la CloudWatch registrazione per gli eventi Amazon S3. Una volta impostato, puoi visualizzare l'attività del connettore nei tuoi registri. CloudWatch

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

SecurityPolicyName

Il nome testuale della politica di sicurezza per il connettore specificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 100.

Modello: `TransferSFTPConnectorSecurityPolicy-[A-Za-z0-9-]+`

Campo obbligatorio: no

ServiceManagedEgressIpAddresses

L'elenco degli indirizzi IP in uscita di questo connettore. Questi indirizzi IP vengono assegnati automaticamente quando si crea il connettore.

Tipo: matrice di stringhe

Modello: `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`

Campo obbligatorio: no

SftpConfig

Una struttura che contiene i parametri per un oggetto connettore SFTP.

Tipo: oggetto SftpConnectorConfig

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i connettori.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Url

L'URL dell'endpoint AS2 o SFTP del partner.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 255.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedExecution

I dettagli per un oggetto di esecuzione.

Indice

ExecutionId

Un identificatore univoco per l'esecuzione di un flusso di lavoro.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 36.

Modello: `[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}`

Campo obbligatorio: no

ExecutionRole

Il ruolo IAM associato all'esecuzione.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

InitialFileLocation

Una struttura che descrive la posizione dei file Amazon S3 o EFS. Questa è la posizione del file all'inizio dell'esecuzione: se il file viene copiato, questa è la posizione del file iniziale (non quella di destinazione).

Tipo: oggetto FileLocation

Campo obbligatorio: no

LoggingConfiguration

Il ruolo di registrazione IAM associato all'esecuzione.

Tipo: oggetto LoggingConfiguration

Campo obbligatorio: no

PosixProfile

L'identità POSIX completa, incluso ID utente (`Uid`), ID gruppo (`Gid`) e qualsiasi ID gruppo secondario (`SecondaryGids`), che controlla l'accesso degli utenti ai file system Amazon EFS. Le autorizzazioni POSIX impostate su file e directory nel file system determinano il livello di accesso che gli utenti ottengono durante il trasferimento dei file da e verso i file system Amazon EFS.

Tipo: oggetto PosixProfile

Campo obbligatorio: no

Results

Una struttura che descrive i risultati dell'esecuzione. Ciò include un elenco dei passaggi con i dettagli di ogni passaggio, il tipo e il messaggio di errore (se presenti) e la `OnExceptionSteps` struttura.

Tipo: oggetto ExecutionResults

Campo obbligatorio: no

ServiceMetadata

Un oggetto contenitore per i dettagli della sessione associati a un flusso di lavoro.

Tipo: oggetto ServiceMetadata

Campo obbligatorio: no

Status

Lo stato è quello dell'esecuzione. Può essere in corso, completata, è stata rilevata un'eccezione o sta gestendo l'eccezione.

- Tipo: stringa

Valori validi: `IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedHostKey

I dettagli per una chiave host del server.

Indice

Arn

L'unico Amazon Resource Name (ARN) per la chiave host.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

DateImported

La data in cui la chiave host è stata aggiunta al server.

Tipo: Timestamp

Campo obbligatorio: no

Description

La descrizione testuale di questa chiave host.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 200.

Modello: `[\p{Print}]*`

Campo obbligatorio: no

HostKeyFingerprint

L'impronta digitale della chiave pubblica, che è una breve sequenza di byte utilizzata per identificare la chiave pubblica più lunga.

- Tipo: stringa

Campo obbligatorio: no

HostKeyId

Un identificatore univoco per la chiave host.

Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 25.

Modello: `hostkey-[0-9a-f]{17}`

Campo obbligatorio: no

Tags

Coppie chiave-valore che possono essere utilizzate per raggruppare e cercare chiavi host.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Type

L'algoritmo di crittografia utilizzato per la chiave host. Il `Type` parametro viene specificato utilizzando uno dei seguenti valori:

- `ssh-rsa`
- `ssh-ed25519`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedProfile

I dettagli per un profilo AS2 locale o partner.

Indice

Arn

L'Amazon Resource Name (ARN) univoco per il profilo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

As2Id

`As2Id` è il nome AS2, come definito nella RFC 4130. Per i trasferimenti in entrata, questa è l'intestazione `AS2-From` dei messaggi AS2 inviati dal partner. Per i connettori in uscita, questa è l'intestazione `AS2-To` dei messaggi AS2 inviati al partner utilizzando l'operazione API `StartFileTransfer`. Questo ID non può includere spazi.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Modello: `[\p{Print}\s]*`

Campo obbligatorio: no

CertificateIds

Una serie di identificativi dei certificati importati. Utilizzi questo identificativo per lavorare con i profili e i profili dei partner.

Tipo: matrice di stringhe

Vincoli di lunghezza: lunghezza fissa di 22.

Modello: `cert-([0-9a-f]{17})`

Campo obbligatorio: no

ProfileId

Un identificatore univoco per il profilo AS2 locale o del partner.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

ProfileType

Indica se elencare solo i profili di tipo `LOCAL` o solo i profili di tipo `PARTNER`. Se non fornito nella richiesta, il comando elenca tutti i tipi di profili.

- Tipo: stringa

Valori validi: `LOCAL | PARTNER`

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i profili.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedSecurityPolicy

Descrive le proprietà di una politica di sicurezza specificata dall'utente. Per ulteriori informazioni sulle politiche di sicurezza, vedere Utilizzo delle politiche di sicurezza per i server o Utilizzo delle politiche di sicurezza per i connettori SFTP.

Indice

SecurityPolicyName

Il nome testuale della politica di sicurezza specificata.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 100.

Modello: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Campo obbligatorio: sì

Fips

Speciifica se questa politica abilita gli standard federali di elaborazione delle informazioni (FIPS). Questo parametro si applica alle politiche di sicurezza dei server e dei connettori.

Tipo: Booleano

Campo obbligatorio: no

Protocols

Elenca i protocolli di trasferimento dei file a cui si applica la politica di sicurezza.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi.

Valori validi: `SFTP | FTPS`

Campo obbligatorio: no

SshCiphers

Elenca gli algoritmi di crittografia Secure Shell (SSH) abilitati nella politica di sicurezza collegata al server o al connettore. Questo parametro si applica alle politiche di sicurezza del server e dei connettori.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

SshHostKeyAlgorithms

Elenca gli algoritmi chiave dell'host per la politica di sicurezza.

> **Note**
>
> Questo parametro si applica solo alle politiche di sicurezza per i connettori.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

SshKexs

Elenca gli algoritmi di crittografia SSH (KEX) abilitati nella politica di sicurezza collegata al server o al connettore. Questo parametro si applica alle politiche di sicurezza del server e dei connettori.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

SshMacs

Elenca gli algoritmi di crittografia del codice di autenticazione dei messaggi SSH (MAC) abilitati nella politica di sicurezza collegata al server o al connettore. Questo parametro si applica alle politiche di sicurezza del server e dei connettori.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

TlsCiphers

Elenca gli algoritmi di crittografia Transport Layer Security (TLS) abilitati nella politica di sicurezza collegata al server.

> **Note**
>
> Questo parametro si applica solo alle politiche di sicurezza per i server.

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

Type

Il tipo di risorsa a cui si applica la politica di sicurezza, server o connettore.

-Tipo: stringa

Valori validi: `SERVER | CONNECTOR`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedServer

Descrive le proprietà di un server abilitato al protocollo di trasferimento file specificato.

Indice

Arn

Speciifica l'Amazon Resource Name (ARN) univoco del server.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

As2ServiceManagedEgressIpAddresses

L'elenco degli indirizzi IP di uscita di questo server. Questi indirizzi IP sono rilevanti solo per i server che utilizzano il protocollo AS2. Vengono utilizzati per l'invio di mDNS asincroni.

Questi indirizzi IP vengono assegnati automaticamente quando si crea un server AS2. Inoltre, se si aggiorna un server esistente e si aggiunge il protocollo AS2, vengono assegnati anche indirizzi IP statici.

Tipo: matrice di stringhe

Modello: `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`

Campo obbligatorio: no

Certificate

Speciifica l'ARN del certificato Certificate AWS Manager (ACM). Obbligatorio quando `Protocols` è impostato su `FTPS`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1600 caratteri.

Campo obbligatorio: no

Domain

Specifica il dominio del sistema di storage utilizzato per i trasferimenti di file. Sono disponibili due domini: Amazon Simple Storage Service (Amazon S3) e Amazon Elastic File System (Amazon EFS). Il valore predefinito è S3.

- Tipo: stringa

Valori validi: `S3 | EFS`

Campo obbligatorio: no

EndpointDetails

Le impostazioni dell'endpoint del cloud privato virtuale (VPC) configurate per il server. Quando esegui l'hosting dell'endpoint all'interno del tuo VPC, puoi renderlo accessibile solo alle risorse nel VPC oppure collegarvi indirizzi IP elastici e renderlo accessibile ai client tramite Internet. I gruppi di sicurezza predefiniti del VPC vengono assegnati automaticamente all'endpoint.

Tipo: oggetto EndpointDetails

Campo obbligatorio: no

EndpointType

Definisce il tipo di endpoint a cui è connesso il server. Se il server è connesso a un endpoint VPC, il server non è accessibile tramite la rete Internet pubblica.

- Tipo: stringa

Valori validi: `PUBLIC | VPC | VPC_ENDPOINT`

Campo obbligatorio: no

HostKeyFingerprint

Specifica l'impronta digitale SHA256 con codifica Base64 della chiave host del server. Questo valore è equivalente all'output del comando. `ssh-keygen -l -f my-new-server-key`

- Tipo: stringa

Campo obbligatorio: no

IdentityProviderDetails

Specificate le informazioni per chiamare un'API di autenticazione fornita dal cliente. Questo campo non viene compilato quando il valore `IdentityProviderType` di un server è o. `AWS_DIRECTORY_SERVICE` `SERVICE_MANAGED`

Tipo: oggetto IdentityProviderDetails

Campo obbligatorio: no

IdentityProviderType

La modalità di autenticazione di un server. Il valore predefinito è`SERVICE_MANAGED`, che consente di archiviare e accedere alle credenziali utente all'interno del AWS Transfer Family servizio.

`AWS_DIRECTORY_SERVICE`Utilizzalo per fornire l'accesso ai gruppi di Active Directory in AWS Directory Service for Microsoft Active Directory o Microsoft Active Directory nell'ambiente locale o AWS utilizzando AD Connector. Questa opzione prevede inoltre che l'utente fornisca un ID directory utilizzando il parametro `IdentityProviderDetails`.

Utilizza il valore `API_GATEWAY` da integrare con un provider di identità a scelta. L'impostazione `API_GATEWAY` richiede di fornire un URL dell'endpoint del Gateway Amazon API da richiamare per l'autenticazione utilizzando il parametro `IdentityProviderDetails`.

Utilizza il `AWS_LAMBDA` valore per utilizzare direttamente una AWS Lambda funzione come provider di identità. Se scegli questo valore, devi specificare l'ARN per la funzione Lambda nel `Function` parametro per il tipo di dati. `IdentityProviderDetails`

- Tipo: stringa

Valori validi: `SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA`

Campo obbligatorio: no

LoggingRole

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a un server di attivare la CloudWatch registrazione Amazon per Amazon S3 o Amazon EFSEvents. Una volta impostato, puoi visualizzare l'attività degli utenti nei tuoi log. CloudWatch

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Modello: `(|arn:.*role/\S+)`

Campo obbligatorio: no

PostAuthenticationLoginBanner

Specifica una stringa da visualizzare quando gli utenti si connettono a un server. Questa stringa viene visualizzata dopo l'autenticazione dell'utente.

> **Note**
>
> Il protocollo SFTP non supporta banner di visualizzazione post-autenticazione.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 4096.

Modello: `[\x09-\x0D\x20-\x7E]*`

Campo obbligatorio: no

PreAuthenticationLoginBanner

Specifica una stringa da visualizzare quando gli utenti si connettono a un server. Questa stringa viene visualizzata prima dell'autenticazione dell'utente. Il seguente banner, ad esempio, mostra i dettagli sull'utilizzo 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: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 4096.

Modello: `[\x09-\x0D\x20-\x7E]*`

Campo obbligatorio: no

ProtocolDetails

Le impostazioni del protocollo configurate per il server.

- Per indicare la modalità passiva (per i protocolli FTP e FTPS), utilizza il parametro `PassiveIp`. Inserire un singolo indirizzo IPv4 composto da 4 numeri decimali separati da punti, ad esempio l'indirizzo IP esterno di un firewall, un router o un load balancer.
- Per ignorare l'errore generato quando il client tenta di utilizzare il comando `SETSTAT` su un file che stai caricando su un bucket Amazon S3, utilizza il parametro `SetStatOption`. Per fare in modo che il AWS Transfer Family server ignori il `SETSTAT` comando e carichi i file senza dover apportare modifiche al client SFTP, imposta il valore su. `ENABLE_NO_OP` Se imposti il `SetStatOption` parametro su`ENABLE_NO_OP`, Transfer Family genera una voce di registro in Amazon CloudWatch Logs, in modo da poter determinare quando il client sta effettuando una `SETSTAT` chiamata.
- Per determinare se il AWS Transfer Family server riprende le sessioni negoziate recenti tramite un ID di sessione univoco, utilizza il parametro. `TlsSessionResumptionMode`
- `As2Transports` indica il metodo di trasporto per i messaggi AS2. Attualmente è supportato solo HTTP.

Tipo: oggetto ProtocolDetails

Campo obbligatorio: no

Protocols

Specifica il protocollo o i protocolli di trasferimento file su cui il client del protocollo di trasferimento file può connettersi all'endpoint del server. I protocolli disponibili sono:

- `SFTP` (Secure Shell (SSH) File Transfer Protocol): trasferimento di file su SSH
- `FTPS` File Transfer Protocol Secure: trasferimento di file con crittografia TLS
- `FTP` (File Transfer Protocol): trasferimento file non crittografato
- `AS2`(Dichiarazione di applicabilità 2): utilizzata per il trasporto di dati strutturati business-to-business

> **Note**
>
> - Se si selezionaFTPS, è necessario scegliere un certificato archiviato in AWS Certificate Manager (ACM) che viene utilizzato per identificare il server quando i client si connettono ad esso tramite FTPS.

- Se `Protocol` include `FTP` o `FTPS`, `EndpointType` deve essere `VPC` e `IdentityProviderType` deve essere `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
- Se `Protocol` include `FTP`, `AddressAllocationIds` non può essere associato.
- Se `Protocol` è impostato solo su `SFTP`, `EndpointType` può essere impostato su `PUBLIC` e `IdentityProviderType` può essere impostato uno qualunque dei tipi di identità supportati: `SERVICE_MANAGED`, `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` o `API_GATEWAY`.
- Se `Protocol` include `AS2`, `EndpointType` deve essere `VPC` e il dominio deve essere Amazon S3.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 4 articoli.

Valori validi: `SFTP | FTP | FTPS | AS2`

Campo obbligatorio: no

S3StorageOptions

Indica se le prestazioni per le tue directory Amazon S3 sono ottimizzate o meno. Questa opzione è disabilitata per impostazione predefinita.

Per impostazione predefinita, le mappature delle home directory hanno un valore di. `TYPE` `DIRECTORY` Se abiliti questa opzione, dovrai quindi impostarla in modo esplicito `FILE` se desideri che una mappatura abbia un file di destinazione. `HomeDirectoryMapEntry` `Type`

Tipo: oggetto S3StorageOptions

Campo obbligatorio: no

SecurityPolicyName

Speciifica il nome della politica di sicurezza per il server.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 100.

Modello: `Transfer[A-Za-z0-9]*SecurityPolicy-[A-Za-z0-9-]+`

Campo obbligatorio: no

ServerId

Speciifica l'identificatore univoco assegnato dal sistema per un server creato dall'utente.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: no

State

La condizione del server descritta. Il valore di `ONLINE` indica che il server può accettare lavori e trasferire file. Un `State` valore di `OFFLINE` indica che il server non è in grado di eseguire operazioni di trasferimento di file.

Gli stati di `STARTING` e `STOPPING` indicano che il server si trova in uno stato intermedio, ovvero non è completamente in grado di rispondere o non è completamente offline. I valori di `START_FAILED` o `STOP_FAILED` possono indicare una condizione di errore.

- Tipo: stringa

Valori validi: `OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED`

Campo obbligatorio: no

StructuredLogDestinations

Speciifica i gruppi di log a cui vengono inviati i log del server.

Per specificare un gruppo di log, è necessario fornire l'ARN per un gruppo di log esistente. In questo caso, il formato del gruppo di log è il seguente:

`arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*`

Ad esempio, `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

Se in precedenza è stato specificato un gruppo di log per un server, è possibile cancellarlo e di fatto disattivare la registrazione strutturata fornendo un valore vuoto per questo parametro in una `update-server` chiamata. Per esempio:

`update-server --server-id s-1234567890abcdef0 --structured-log-destinations`

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: no

Tags

Speciifica le coppie chiave-valore che è possibile utilizzare per cercare e raggruppare i server assegnati al server descritto.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

UserCount

Speciifica il numero di utenti assegnati a un server specificato con. `ServerId`

Tipo: integer

Campo obbligatorio: no

WorkflowDetails

Specifica l'ID del flusso di lavoro da assegnare e il ruolo di esecuzione utilizzato per l'esecuzione del flusso di lavoro.

Oltre a un flusso di lavoro da eseguire quando un file viene caricato completamente, `WorkflowDetails` può contenere anche un ID del flusso di lavoro (e ruolo di esecuzione) per l'esecuzione di un flusso di lavoro in caso di caricamento parziale. Un caricamento parziale si verifica quando la sessione del server si disconnette mentre il file è ancora in fase di caricamento.

Tipo: oggetto WorkflowDetails

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedUser

Descrive le proprietà di un utente specificato.

Indice

Arn

Speciifica l'Amazon Resource Name (ARN) univoco per l'utente di cui è stata richiesta la descrizione.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

HomeDirectory

La directory di destinazione (cartella) per un utente quando accede al server utilizzando il client.

Un esempio di `HomeDirectory` è `/bucket_name/home/mydirectory`.

> **Note**
>
> Il parametro `HomeDirectory` è utilizzato solo se `HomeDirectoryType` è impostato su `PATH`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

HomeDirectoryMappings

Mappature di directory logiche che specificano quali percorsi e chiavi di Amazon S3 o Amazon EFS devono essere visibili all'utente e in che modo desideri renderli visibili. È necessario

specificare la `Target` coppia `Entry` and, dove `Entry` mostra come il percorso viene reso visibile ed `Target` è il percorso effettivo di Amazon S3 o Amazon EFS. Se si specifica solo un obiettivo, questo viene visualizzato così com'è. È inoltre necessario assicurarsi che il proprio ruolo AWS Identity and Access Management (IAM) fornisca l'accesso ai percorsi in`Target`. Questo valore può essere impostato solo quando `HomeDirectoryType` è impostato su LOGICAL.

Nella maggior parte dei casi, è possibile utilizzare questo valore al posto della politica di sessione per bloccare l'utente nella home directory designata (» `chroot` «). A tale scopo, è possibile `Entry` impostare '/' e `Target` impostare il valore del HomeDirectory parametro.

Tipo: matrice di oggetti HomeDirectoryMapEntry

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50000 articoli.

Campo obbligatorio: no

HomeDirectoryType

Il tipo di directory (cartella) di destinazione in cui deve trovarsi la directory home degli utenti quando accedono al server. Se lo imposti su`PATH`, l'utente vedrà il bucket Amazon S3 assoluto o il percorso Amazon EFS così com'è nei client del protocollo di trasferimento file. Se lo imposti su`LOGICAL`, devi fornire le mappature relative al modo in cui desideri rendere i percorsi Amazon S3 o Amazon EFS visibili ai tuoi utenti. `HomeDirectoryMappings`

> **Note**
>
> In caso `HomeDirectoryType` `LOGICAL` affermativo, devi fornire le mappature utilizzando il parametro. `HomeDirectoryMappings` Se, invece, `HomeDirectoryType` è`PATH`, si fornisce un percorso assoluto utilizzando il `HomeDirectory` parametro. Non puoi avere entrambi `HomeDirectory` e `HomeDirectoryMappings` nel tuo modello.

-Tipo: stringa

Valori validi: `PATH | LOGICAL`

Campo obbligatorio: no

Policy

Una policy di sessione per il tuo utente in modo da poter utilizzare lo stesso ruolo AWS Identity and Access Management (IAM) su più utenti. Questa policy limita l'accesso di un

utente a porzioni del suo bucket Amazon S3. Le variabili che è possibile utilizzare all'interno di questa policy includono `${Transfer:UserName}`, `${Transfer:HomeDirectory}` e `${Transfer:HomeBucket}`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

PosixProfile

Specifica l'identità POSIX completa, inclusi ID utente (`Uid`), ID gruppo (`Gid`) e qualsiasi ID gruppo secondario (`SecondaryGids`), che controlla l'accesso degli utenti ai file system Amazon Elastic File System (Amazon EFS). Le autorizzazioni POSIX impostate su file e directory nel file system determinano il livello di accesso che gli utenti ottengono durante il trasferimento dei file da e verso i file system Amazon EFS.

Tipo: oggetto PosixProfile

Campo obbligatorio: no

Role

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che controlla l'accesso degli utenti al bucket Amazon S3 o al file system Amazon EFS. Le policy associate a questo ruolo determineranno il livello di accesso che desideri offrire agli utenti quando trasferiscono i file da e verso il bucket Amazon S3 o il file system Amazon EFS. Il ruolo IAM deve contenere anche una relazione di trust che consente al server di accedere alle proprie risorse durante la manutenzione delle richieste di trasferimento degli utenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

SshPublicKeys

Contiene la porzione di chiave pubblica delle chiavi SSH (Secure Shell) archiviate per l'utente descritto.

Tipo: matrice di oggetti SshPublicKey

Membri dell'array: numero minimo di 0 elementi. Numero massimo 5 elementi.

Campo obbligatorio: no

Tags

Speciifica le coppie chiave-valore per l'utente richiesto. Il tag può essere utilizzato per cercare e raggruppare utenti per diversi scopi.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

UserName

Speciifica il nome dell'utente per il quale è stato richiesto di essere descritto. I nomi utente vengono utilizzati per scopi di autenticazione. Questa è la stringa che verrà utilizzata dall'utente quando accede al server.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

DescribedWorkflow

Descrive le proprietà del flusso di lavoro specificato

Indice

Arn

Speciifica l'Amazon Resource Name (ARN) univoco per il flusso di lavoro.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

Description

Specifica la descrizione testuale per il flusso di lavoro.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `[\w- ]*`

Campo obbligatorio: no

OnExceptionSteps

Specifica le fasi (azioni) da eseguire se durante l'esecuzione del flusso di lavoro si verificano eventuali errori.

Tipo: matrice di oggetti WorkflowStep

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 8 articoli.

Campo obbligatorio: no

Steps

Specifica i dettagli delle fasi incluse nel flusso di lavoro specificato.

Tipo: matrice di oggetti WorkflowStep

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 8 articoli.

Campo obbligatorio: no

Tags

Le coppie chiave-valore che è possibile utilizzare per raggruppare e cercare i flussi di lavoro. I tag sono metadati associati ai flussi di lavoro per qualsiasi scopo.

Tipo: matrice di oggetti Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

WorkflowId

Un identificatore univoco per il flusso di lavoro.

-Tipo: stringa

Limiti di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

EfsFileLocation

Specificate i dettagli per la posizione del file che viene utilizzato nel flusso di lavoro. Applicabile solo se utilizzi Amazon Elastic File Systems (Amazon EFS) per lo storage.

Indice

FileSystemId

L'identificatore del file system, assegnato da Amazon EFS.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 128 caratteri.

Modello: `(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})`

Campo obbligatorio: no

Path

Il nome del percorso della cartella utilizzata da un flusso di lavoro.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 65536.

Modello: `[^\x00]+`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

EndpointDetails

Le impostazioni degli endpoint del cloud privato virtuale (VPC) configurate per il server abilitato al protocollo di trasferimento file. Con un endpoint VPC, puoi limitare l'accesso al server e alle risorse solo all'interno del VPC. Per controllare il traffico Internet in entrata, richiama l'`UpdateServer`API e collega un indirizzo IP elastico all'endpoint del server.

> **Note**
>
> Dopo il 19 maggio 2021, non potrai creare un server utilizzando `EndpointType=VPC_ENDPOINT` il tuo AWS account se quest'ultimo non l'ha già fatto prima del 19 maggio 2021. Se hai già creato dei server `EndpointType=VPC_ENDPOINT` nel tuo AWS account entro il 19 maggio 2021 o prima, non ne subirai alcuna modifica. Dopo questa data, usa `EndpointType =VPC`.
> Per ulteriori informazioni, consulta Interruzione dell'uso di VPC_ENDPOINT.

Indice

AddressAllocationIds

Un elenco di ID di allocazione indirizzi necessari per collegare un indirizzo IP elastico all'endpoint del server.

Un ID di allocazione degli indirizzi corrisponde all'ID di allocazione di un indirizzo IP elastico. Questo valore può essere recuperato dal `allocationId` campo dal tipo di dati Amazon EC2 Address. Un modo per recuperare questo valore consiste nel chiamare l'API EC2. DescribeAddresses

Questo parametro è facoltativo. Imposta questo parametro se desideri rendere il tuo endpoint VPC rivolto al pubblico. Per i dettagli, consulta Creare un endpoint con accesso a Internet per il tuo server.

> **Note**
>
> Questa proprietà può essere impostata solo come segue:
>
> - `EndpointType`deve essere impostata su `VPC`
> - Il server Transfer Family deve essere offline.

- Non è possibile impostare questo parametro per i server Transfer Family che utilizzano il protocollo FTP.
- Il server deve essere già `SubnetIds` popolato (`SubnetIds`e `AddressAllocationIds` non può essere aggiornato contemporaneamente).
- `AddressAllocationIds`non può contenere duplicati e deve avere una lunghezza uguale a. `SubnetIds` Ad esempio, se si dispone di tre ID di sottorete, è necessario specificare anche tre ID di allocazione degli indirizzi.
- Chiama l'`UpdateServer`API per impostare o modificare questo parametro.

Tipo: matrice di stringhe

Campo obbligatorio: no

SecurityGroupIds

Elenco degli ID dei gruppi di sicurezza disponibili per il collegamento all'endpoint del server.

> **Note**
>
> Questa proprietà può essere utilizzata solo quando `EndpointType` è impostato su `VPC`. Puoi modificare la `SecurityGroupIds` proprietà nell'UpdateServerAPI solo se stai cambiando `EndpointType` da `PUBLIC` o `VPC_ENDPOINT` a`VPC`. Per modificare i gruppi di sicurezza associati all'endpoint VPC del tuo server dopo la creazione, usa l'API Amazon EC2. ModifyVpcEndpoint

Tipo: matrice di stringhe

Limitazioni di lunghezza: lunghezza minima pari a 11. Lunghezza massima di 20.

Modello: `sg-[0-9a-f]{8,17}`

Campo obbligatorio: no

SubnetIds

Elenco di ID di sottorete necessari per ospitare l'endpoint del server nel VPC.

> **Note**
>
> Questa proprietà può essere utilizzata solo quando `EndpointType` è impostato su `VPC`.

Tipo: matrice di stringhe

Campo obbligatorio: no

VpcEndpointId

L'identificatore dell'endpoint VPC.

> **Note**
>
> Questa proprietà può essere utilizzata solo quando `EndpointType` è impostato su `VPC_ENDPOINT`.
> Per ulteriori informazioni, consulta Interruzione dell'uso di VPC_ENDPOINT.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 22.

Modello: `vpce-[0-9a-f]{17}`

Campo obbligatorio: no

VpcId

L'identificatore VPC del VPC in cui verrà ospitato l'endpoint di un server.

> **Note**
>
> Questa proprietà può essere utilizzata solo quando `EndpointType` è impostato su `VPC`.

-Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta AWS quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ExecutionError

Specificate il messaggio e il tipo di errore per un errore che si verifica durante l'esecuzione del flusso di lavoro.

Indice

Message

Speciifica il messaggio descrittivo che corrisponde a. `ErrorType`

Tipo: stringa

Campo obbligatorio: sì

Type

Speciifica il tipo di errore.

- `ALREADY_EXISTS`: si verifica per una fase di copia, se l'opzione di sovrascrittura non è selezionata e nella posizione di destinazione esiste già un file con lo stesso nome.
- `BAD_REQUEST`: una richiesta generica errata: ad esempio, viene restituito un passaggio che tenta di etichettare un file EFS`BAD_REQUEST`, poiché è possibile taggare solo i file S3.
- `CUSTOM_STEP_FAILED`: si verifica quando il passaggio personalizzato ha fornito un callback che indica un errore.
- `INTERNAL_SERVER_ERROR`: un errore generico che può verificarsi per diversi motivi.
- `NOT_FOUND`: si verifica quando un'entità richiesta, ad esempio un file sorgente per una fase di copia, non esiste.
- `PERMISSION_DENIED`: si verifica se la policy non contiene le autorizzazioni corrette per completare uno o più passaggi del flusso di lavoro.
- `TIMEOUT`: si verifica quando scade il timeout dell'esecuzione.

  > **Note**
  >
  > È possibile impostare un passaggio personalizzato, da 1 secondo a 1800 secondi (30 minuti). `TimeoutSeconds`

- `THROTTLED`: si verifica se si supera la nuova frequenza di ricarica di esecuzione di un flusso di lavoro al secondo.

- Tipo: stringa

Valori validi: `PERMISSION_DENIED | CUSTOM_STEP_FAILED | THROTTLED | ALREADY_EXISTS | NOT_FOUND | BAD_REQUEST | TIMEOUT | INTERNAL_SERVER_ERROR`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ExecutionResults

Specificate i passaggi del flusso di lavoro, nonché i passaggi da eseguire in caso di errori durante l'esecuzione del flusso di lavoro.

Indice

OnExceptionSteps

Specifica le fasi (azioni) da eseguire se durante l'esecuzione del flusso di lavoro si verificano eventuali errori.

Tipo: matrice di oggetti ExecutionStepResult

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Steps

Specifica i dettagli delle fasi incluse nel flusso di lavoro specificato.

Tipo: matrice di oggetti ExecutionStepResult

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 50 item.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ExecutionStepResult

Specificate i seguenti dettagli per il passo: errore (se presente), output (se presente) e tipo di passo.

Indice

Error

Specificate i dettagli di un errore, se si è verificato durante l'esecuzione della fase del flusso di lavoro specificata.

Tipo: oggetto ExecutionError

Campo obbligatorio: no

Outputs

I valori per la coppia chiave/valore applicata come tag al file. Applicabile solo se il tipo di passo è. `TAG`

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 65536.

Campo obbligatorio: no

StepType

Uno dei tipi di passaggi disponibili.

- **`COPY`** - Copiare il file in un'altra posizione.
- **`CUSTOM`**- Esegui un passaggio personalizzato con un obiettivo di AWS Lambda funzione.
- **`DECRYPT`** - Decrittografare un file crittografato prima che è stato caricato.
- **`DELETE`** - Eliminare il file.
- **`TAG`** - Aggiungere un tag al file.

-Tipo: stringa

Valori validi: `COPY | CUSTOM | TAG | DELETE | DECRYPT`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

FileLocation

Specifica i dettagli del file Amazon S3 o EFS da utilizzare nella fase.

Indice

EfsFileLocation

Speciifica l'identificatore Amazon EFS e il percorso del file utilizzato.

Tipo: oggetto EfsFileLocation

Campo obbligatorio: no

S3FileLocation

Speciifica i dettagli S3 per il file utilizzato, come bucket, ETag e così via.

Tipo: oggetto S3FileLocation

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta AWS quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

HomeDirectoryMapEntry

Rappresenta un oggetto che contiene voci e destinazioni per `HomeDirectoryMappings`.

Di seguito è riportato un esempio `Target` di coppia `Entry` and per`chroot`.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Indice

Entry

Rappresenta una voce per `HomeDirectoryMappings`.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `/.*`

Campo obbligatorio: sì

Target

Rappresenta la destinazione di mappatura utilizzata in una voce `HomeDirectoryMapEntry`.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `/.*`

Campo obbligatorio: sì

Type

Specificate il tipo di mappatura. Imposta il tipo su `FILE` se vuoi che la mappatura punti a un file o che `DIRECTORY` la directory punti a una directory.

> **Note**
>
> Per impostazione predefinita, i mapping della home directory hanno un valore `Type` di `DIRECTORY` quando si crea un server Transfer Family. È necessario impostare

esplicitamente su `Type` `FILE` se si desidera che una mappatura abbia un file di destinazione.

-Tipo: stringa

Valori validi: `FILE | DIRECTORY`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

IdentityProviderDetails

Restituisce informazioni relative al tipo di autenticazione utente in uso per gli utenti di un server abilitato al protocollo di trasferimento file. Un server può avere un solo metodo di autenticazione.

Indice

DirectoryId

L'identificatore della AWS Directory Service directory che desideri utilizzare come provider di identità.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 12.

Modello: `d-[0-9a-f]{10}`

Campo obbligatorio: no

Function

L'ARN per una funzione Lambda da utilizzare per il provider di identità.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 170.

Modello: `arn:[a-z-]+:lambda:.*`

Campo obbligatorio: no

InvocationRole

Questo parametro è applicabile solo se lo è il tuo`IdentityProviderType`. `API_GATEWAY` Fornisce il tipo di `InvocationRole` usato per autenticare l'account dell'utente.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

SftpAuthenticationMethods

Per i server compatibili con SFTP e solo per i provider di identità personalizzati, è possibile specificare se autenticarsi utilizzando una password, una coppia di chiavi SSH o entrambi.

- `PASSWORD`- gli utenti devono fornire la propria password per connettersi.
- `PUBLIC_KEY`- gli utenti devono fornire la propria chiave privata per connettersi.
- `PUBLIC_KEY_OR_PASSWORD`- gli utenti possono autenticarsi con la propria password o la propria chiave. Si tratta del valore di default.
- `PUBLIC_KEY_AND_PASSWORD`- gli utenti devono fornire sia la chiave privata che la password per connettersi. Il server controlla prima la chiave e poi, se la chiave è valida, il sistema richiede una password. Se la chiave privata fornita non corrisponde alla chiave pubblica archiviata, l'autenticazione fallisce.

➖Tipo: stringa

Valori validi: `PASSWORD | PUBLIC_KEY | PUBLIC_KEY_OR_PASSWORD | PUBLIC_KEY_AND_PASSWORD`

Campo obbligatorio: no

Url

Contiene il percorso dell'endpoint del servizio utilizzato per autenticare gli utenti.

➖Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 255.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

InputFileLocation

Specificate la posizione del file in fase di elaborazione.

Indice

EfsFileLocation

Speciifica i dettagli per il file Amazon Elastic File System (Amazon EFS) che viene decrittografato.

Tipo: oggetto EfsFileLocation

Campo obbligatorio: no

S3FileLocation

Speciifica i dettagli per il file Amazon S3 che viene copiato o decrittografato.

Tipo: oggetto S3InputFileLocation

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua AWS , consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedAccess

Elenca le proprietà per uno o più accessi associati specificati.

Indice

ExternalId

Un identificatore univoco necessario per identificare gruppi specifici all'interno della directory. Gli utenti del gruppo che associ hanno accesso alle tue risorse Amazon S3 o Amazon EFS tramite i protocolli abilitati che utilizzano. AWS Transfer Family Se conosci il nome del gruppo, puoi visualizzare i valori SID eseguendo il seguente comando utilizzando Windows. PowerShell

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

In quel comando, sostituiscilo YourGroupNamecon il nome del tuo gruppo Active Directory.

L'espressione regolare utilizzata per convalidare questo parametro è una stringa di caratteri composta da caratteri alfanumerici maiuscoli e minuscoli senza spazi. È inoltre possibile includere caratteri di sottolineatura o uno dei seguenti caratteri: =, . @: /-

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Modello: `S-1-[\d-]+`

Campo obbligatorio: no

HomeDirectory

La directory di destinazione (cartella) per un utente quando accede al server utilizzando il client.

Un esempio di `HomeDirectory` è `/bucket_name/home/mydirectory`.

> **Note**
>
> Il parametro `HomeDirectory` è utilizzato solo se `HomeDirectoryType` è impostato su `PATH`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

HomeDirectoryType

Il tipo di directory (cartella) di destinazione in cui deve trovarsi la directory home degli utenti quando accedono al server. Se lo imposti su`PATH`, l'utente vedrà il bucket Amazon S3 assoluto o il percorso Amazon EFS così com'è nei client del protocollo di trasferimento file. Se lo imposti su`LOGICAL`, devi fornire le mappature relative al modo in cui desideri rendere i percorsi Amazon S3 o Amazon EFS visibili ai tuoi utenti. `HomeDirectoryMappings`

> **Note**
>
> In caso `HomeDirectoryType` `LOGICAL` affermativo, devi fornire le mappature utilizzando il parametro. `HomeDirectoryMappings` Se, invece, `HomeDirectoryType` è`PATH`, si fornisce un percorso assoluto utilizzando il `HomeDirectory` parametro. Non puoi avere entrambi `HomeDirectory` e `HomeDirectoryMappings` nel tuo modello.

-Tipo: stringa

Valori validi: `PATH | LOGICAL`

Campo obbligatorio: no

Role

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che controlla l'accesso degli utenti al bucket Amazon S3 o al file system Amazon EFS. Le policy associate a questo ruolo determineranno il livello di accesso che desideri offrire agli utenti quando trasferiscono i file da e verso il bucket Amazon S3 o il file system Amazon EFS. Il ruolo IAM deve contenere anche una relazione di trust che consente al server di accedere alle proprie risorse durante la manutenzione delle richieste di trasferimento degli utenti.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta AWS quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedAgreement

Descrive le proprietà di un accordo.

Indice

AgreementId

Un identificatore univoco per l'accordo. Questo identificatore viene restituito quando si crea un accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `a-([0-9a-f]{17})`

Campo obbligatorio: no

Arn

L'Amazon Resource Name (ARN) del contratto specificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: no

Description

La descrizione attuale del contratto. È possibile modificarla richiamando l'`UpdateAgreement`operazione e fornendo una nuova descrizione.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 200.

Modello: `[\p{Graph}]+`

Campo obbligatorio: no

LocalProfileId

Un identificativo univoco il profilo locale AS2.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

PartnerProfileId

Un identificatore univoco per il profilo del partner.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

ServerId

L'identificatore univoco dell'accordo.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: no

Status

L'accordo può essere uno dei due. `ACTIVE` `INACTIVE`

- Tipo: stringa

Valori validi: `ACTIVE | INACTIVE`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedCertificate

Descrive le proprietà di un certificato.

Indice

ActiveDate

Una data opzionale che specifica quando il certificato diventa attivo.

Tipo: Timestamp

Campo obbligatorio: no

Arn

L'Amazon Resource Name (ARN) del certificato specificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: no

CertificateId

Una serie di identificativi dei certificati importati. Utilizzi questo identificativo per lavorare con i profili e i profili dei partner.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 22.

Modello: `cert-([0-9a-f]{17})`

Campo obbligatorio: no

Description

Il nome o la breve descrizione utilizzata per identificare il certificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 200.

Modello: `[\p{Graph}]+`

Campo obbligatorio: no

InactiveDate

Una data opzionale che specifica quando il certificato cessa di essere attivo.

Tipo: Timestamp

Campo obbligatorio: no

Status

Il certificato può essere `ACTIVE`, `PENDING_ROTATION` o `INACTIVE`. `PENDING_ROTATION` significa che questo certificato sostituirà il certificato corrente alla scadenza.

- Tipo: stringa

Valori validi: `ACTIVE | PENDING_ROTATION | INACTIVE`

Campo obbligatorio: no

Type

Il tipo di certificato. Se per il certificato è stata specificata una chiave privata, il tipo è `CERTIFICATE_WITH_PRIVATE_KEY`. Se non esiste una chiave privata, il tipo è `CERTIFICATE`.

- Tipo: stringa

Valori validi: `CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY`

Campo obbligatorio: no

Usage

Specifica come viene utilizzato questo certificato. Può essere utilizzato nei seguenti modi:

- `SIGNING`: Per firmare messaggi AS2
- `ENCRYPTION`: Per crittografare i messaggi AS2
- `TLS`: Per proteggere le comunicazioni AS2 inviate tramite HTTPS

- Tipo: stringa

Valori validi: `SIGNING | ENCRYPTION`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedConnector

Restituisce i dettagli del connettore specificato.

Indice

Arn

L'Amazon Resource Name (ARN) del connettore specificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: no

ConnectorId

L'identificatore univoco del connettore.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `c-([0-9a-f]{17})`

Campo obbligatorio: no

Url

L'URL dell'endpoint AS2 o SFTP del partner.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 255.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedExecution

Restituisce le proprietà dell'esecuzione specificata.

Indice

ExecutionId

Un identificatore univoco per l'esecuzione di un flusso di lavoro.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 36.

Modello: `[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}`

Campo obbligatorio: no

InitialFileLocation

Una struttura che descrive la posizione dei file Amazon S3 o EFS. Questa è la posizione del file all'inizio dell'esecuzione: se il file viene copiato, questa è la posizione del file iniziale (non quella di destinazione).

Tipo: oggetto FileLocation

Campo obbligatorio: no

ServiceMetadata

Un oggetto contenitore per i dettagli della sessione associati a un flusso di lavoro.

Tipo: oggetto ServiceMetadata

Campo obbligatorio: no

Status

Lo stato è quello dell'esecuzione. Può essere in corso, completata, è stata rilevata un'eccezione o sta gestendo l'eccezione.

- Tipo: stringa

Valori validi: `IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedHostKey

Restituisce le proprietà della chiave host specificata.

Indice

Arn

L'unico Amazon Resource Name (ARN) della chiave host.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

DateImported

La data in cui la chiave host è stata aggiunta al server.

Tipo: Timestamp

Campo obbligatorio: no

Description

La descrizione corrente della chiave host. È possibile modificarla richiamando l'`UpdateHostKey`operazione e fornendo una nuova descrizione.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 200.

Modello: `[\p{Print}]*`

Campo obbligatorio: no

Fingerprint

L'impronta digitale della chiave pubblica, che è una breve sequenza di byte utilizzata per identificare la chiave pubblica più lunga.

- Tipo: stringa

Campo obbligatorio: no

HostKeyId

Un identificatore univoco per la chiave host.

-Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 25.

Modello: `hostkey-[0-9a-f]{17}`

Campo obbligatorio: no

Type

L'algoritmo di crittografia utilizzato per la chiave host. Il `Type` parametro viene specificato utilizzando uno dei seguenti valori:

- `ssh-rsa`
- `ssh-ed25519`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

-Tipo: stringa

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedProfile

Restituisce le proprietà del profilo specificato.

Indice

Arn

L'Amazon Resource Name (ARN) del profilo specificato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: no

As2Id

`As2Id` è il nome AS2, come definito nella RFC 4130. Per i trasferimenti in entrata, questa è l'intestazione `AS2-From` dei messaggi AS2 inviati dal partner. Per i connettori in uscita, questa è l'intestazione `AS2-To` dei messaggi AS2 inviati al partner utilizzando l'operazione API `StartFileTransfer`. Questo ID non può includere spazi.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Modello: `[\p{Print}\s]*`

Campo obbligatorio: no

ProfileId

Un identificatore univoco per il profilo AS2 locale o del partner.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `p-([0-9a-f]{17})`

Campo obbligatorio: no

ProfileType

Indica se elencare solo i profili di tipo LOCAL o solo i profili di tipo PARTNER. Se non fornito nella richiesta, il comando elenca tutti i tipi di profili.

- Tipo: stringa

Valori validi: LOCAL | PARTNER

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedServer

Restituisce le proprietà di un server abilitato al protocollo di trasferimento file specificato.

Indice

Arn

Speciifica l'Amazon Resource Name (ARN) univoco per un server da elencare.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

Domain

Specifica il dominio del sistema di storage utilizzato per i trasferimenti di file. Sono disponibili due domini: Amazon Simple Storage Service (Amazon S3) e Amazon Elastic File System (Amazon EFS). Il valore predefinito è S3.

- Tipo: stringa

Valori validi: `S3 | EFS`

Campo obbligatorio: no

EndpointType

Speciifica il tipo di endpoint VPC a cui è connesso il server. Se il server è connesso a un endpoint VPC, il server non è accessibile tramite la rete Internet pubblica.

- Tipo: stringa

Valori validi: `PUBLIC | VPC | VPC_ENDPOINT`

Campo obbligatorio: no

IdentityProviderType

La modalità di autenticazione di un server. Il valore predefinito è`SERVICE_MANAGED`, che consente di archiviare e accedere alle credenziali utente all'interno del servizio. AWS Transfer Family

`AWS_DIRECTORY_SERVICE`Utilizzalo per fornire l'accesso ai gruppi di Active Directory in AWS Directory Service for Microsoft Active Directory o Microsoft Active Directory nell'ambiente locale o AWS utilizzando AD Connector. Questa opzione prevede inoltre che l'utente fornisca un ID directory utilizzando il parametro `IdentityProviderDetails`.

Utilizza il valore `API_GATEWAY` da integrare con un provider di identità a scelta. L'impostazione `API_GATEWAY` richiede di fornire un URL dell'endpoint del Gateway Amazon API da richiamare per l'autenticazione utilizzando il parametro `IdentityProviderDetails`.

Utilizza il `AWS_LAMBDA` valore per utilizzare direttamente una AWS Lambda funzione come provider di identità. Se scegli questo valore, devi specificare l'ARN per la funzione Lambda nel `Function` parametro per il tipo di dati. `IdentityProviderDetails`

- Tipo: stringa

Valori validi: `SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA`

Campo obbligatorio: no

LoggingRole

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a un server di attivare la CloudWatch registrazione Amazon per Amazon S3 o Amazon EFSEvents. Una volta impostato, puoi visualizzare l'attività degli utenti nei tuoi log. CloudWatch

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

ServerId

Speciifica l'identificatore univoco assegnato dal sistema per i server elencati.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: no

State

La condizione del server descritta. Il valore di `ONLINE` indica che il server può accettare lavori e trasferire file. Un `State` valore di `OFFLINE` indica che il server non è in grado di eseguire operazioni di trasferimento di file.

Gli stati di `STARTING` e `STOPPING` indicano che il server si trova in uno stato intermedio, ovvero non è completamente in grado di rispondere o non è completamente offline. I valori di `START_FAILED` o `STOP_FAILED` possono indicare una condizione di errore.

- Tipo: stringa

Valori validi: `OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED`

Campo obbligatorio: no

UserCount

Speciifica il numero di utenti assegnati a un server specificato con. `ServerId`

Tipo: integer

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedUser

Restituisce le proprietà dell'utente specificato.

Indice

Arn

Fornisce l'Amazon Resource Name (ARN) univoco per l'utente che desideri conoscere.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: sì

HomeDirectory

La directory di destinazione (cartella) per un utente quando accede al server utilizzando il client.

Un esempio di `HomeDirectory` è `/bucket_name/home/mydirectory`.

> **Note**
>
> Il parametro `HomeDirectory` è utilizzato solo se `HomeDirectoryType` è impostato su `PATH`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `(|/.*)`

Campo obbligatorio: no

HomeDirectoryType

Il tipo di directory (cartella) di destinazione in cui deve trovarsi la directory home degli utenti quando accedono al server. Se lo imposti su`PATH`, l'utente vedrà il bucket Amazon S3 assoluto

o il percorso Amazon EFS così com'è nei client del protocollo di trasferimento file. Se lo imposti su`LOGICAL`, devi fornire le mappature relative al modo in cui desideri rendere i percorsi Amazon S3 o Amazon EFS visibili ai tuoi utenti. `HomeDirectoryMappings`

> **Note**
>
> In caso `HomeDirectoryType` `LOGICAL` affermativo, devi fornire le mappature utilizzando il parametro. `HomeDirectoryMappings` Se, invece, `HomeDirectoryType` è`PATH`, si fornisce un percorso assoluto utilizzando il `HomeDirectory` parametro. Non puoi avere entrambi `HomeDirectory` e `HomeDirectoryMappings` nel tuo modello.

- Tipo: stringa

Valori validi: `PATH | LOGICAL`

Campo obbligatorio: no

Role

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che controlla l'accesso degli utenti al bucket Amazon S3 o al file system Amazon EFS. Le policy associate a questo ruolo determineranno il livello di accesso che desideri offrire agli utenti quando trasferiscono i file da e verso il bucket Amazon S3 o il file system Amazon EFS. Il ruolo IAM deve contenere anche una relazione di trust che consente al server di accedere alle proprie risorse durante la manutenzione delle richieste di trasferimento degli utenti.

> **Note**
>
> Il ruolo IAM che controlla l'accesso degli utenti al bucket Amazon S3 per server `Domain=S3` con o al file system EFS per server con. `Domain=EFS`
> Le policy associate a questo ruolo determinano il livello di accesso che desideri fornire agli utenti durante il trasferimento di file da e verso i bucket S3 o i file system EFS.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

SshPublicKeyCount

Speciifica il numero di chiavi pubbliche SSH archiviate per l'utente specificato.

Tipo: integer

Campo obbligatorio: no

UserName

Speciifica il nome dell'utente il cui ARN è stato specificato. I nomi utente vengono utilizzati per scopi di autenticazione.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ListedWorkflow

Contiene l'identificatore, la descrizione testuale e Amazon Resource Name (ARN) per il flusso di lavoro.

Indice

Arn

Speciifica l'Amazon Resource Name (ARN) univoco per il flusso di lavoro.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 1600 caratteri.

Modello: `arn:\S+`

Campo obbligatorio: no

Description

Specifica la descrizione testuale per il flusso di lavoro.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `[\w- ]*`

Campo obbligatorio: no

WorkflowId

Un identificatore univoco per il flusso di lavoro.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

LoggingConfiguration

È costituito dal ruolo di registrazione e dal nome del gruppo di log.

Indice

LoggingRole

L'Amazon Resource Name (ARN) del ruolo AWS Identity and Access Management (IAM) che consente a un server di attivare la CloudWatch registrazione Amazon per Amazon S3 o Amazon EFSEvents. Una volta impostato, puoi visualizzare l'attività degli utenti nei tuoi log. CloudWatch

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: no

LogGroupName

Il nome del gruppo di CloudWatch registrazione per il AWS Transfer Family server a cui appartiene questo flusso di lavoro.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 512 caratteri.

Modello: `[\.\-_/#A-Za-z0-9]*`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

PosixProfile

L'identità POSIX completa, incluso ID utente (`Uid`), ID gruppo (`Gid`) e qualsiasi ID gruppo secondario (`SecondaryGids`), che controlla l'accesso degli utenti ai file system Amazon EFS. Le autorizzazioni POSIX impostate su file e directory nel file system determinano il livello di accesso che gli utenti ottengono durante il trasferimento dei file da e verso i file system Amazon EFS.

Indice

Gid

L'ID gruppo POSIX utilizzato per tutte le operazioni EFS da questo utente.

Tipo: long

Intervallo valido: valore minimo di 0. Valore massimo pari a 4294967295.

Campo obbligatorio: sì

Uid

L'ID utente POSIX utilizzato per tutte le operazioni EFS da questo utente.

Tipo: long

Intervallo valido: valore minimo di 0. Valore massimo pari a 4294967295.

Campo obbligatorio: sì

SecondaryGids

Gli ID gruppo POSIX secondari utilizzati per tutte le operazioni EFS da questo utente.

Tipo: array di lunghezze

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 16 elementi.

Intervallo valido: valore minimo di 0. Valore massimo pari a 4294967295.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ProtocolDetails

Le impostazioni del protocollo configurate per il server.

Indice

As2Transports

Indica il metodo di trasporto per i messaggi AS2. Attualmente è supportato solo HTTP.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento.

Valori validi: `HTTP`

Campo obbligatorio: no

PassiveIp

Indica la modalità passiva, per i protocolli FTP e FTPS. Inserisci un singolo indirizzo IPv4, ad esempio l'indirizzo IP pubblico di un firewall, router o load balancer. Ad esempio:

```
aws transfer update-server --protocol-details PassiveIp=0.0.0.0
```

Sostituisci `0.0.0.0`nell'esempio precedente con l'indirizzo IP effettivo che desideri utilizzare.

> **Note**
>
> Se modifichi il valore `PassiveIp`, per applicare la modifica dovrai arrestare e riavviare il server Transfer Family. Per informazioni dettagliate sull'utilizzo della modalità passiva (PASV) in un ambiente NAT, consultate Configurazione del server FTPS dietro un firewall o NAT con. AWS Transfer Family

Valori speciali

`AUTO` e `0.0.0.0` sono valori speciali per il parametro `PassiveIp`. Il valore `PassiveIp=AUTO` è assegnato per impostazione predefinita ai server di tipo FTP e FTPS. In questo caso, il server risponde automaticamente con uno degli IP dell'endpoint all'interno della risposta PASV. `PassiveIp=0.0.0.0` dispone di un'applicazione più specifica per il suo utilizzo. Ad esempio, se disponi di un ambiente Network Load Balancer (NLB) ad alta disponibilità (HA)

in cui sono presenti 3 sottoreti, puoi specificare un solo indirizzo IP utilizzando il parametro `PassiveIp`. Questo riduce l'efficacia della disponibilità elevata. In questo caso, puoi specificare `PassiveIp=0.0.0.0`. Ciò indica al client di utilizzare lo stesso indirizzo IP della connessione Control e di utilizzare tutte le AZ per le proprie connessioni. Nota, tuttavia, che non tutti i client FTP supportano la risposta. `PassiveIp=0.0.0.0` FileZilla e WinSCP lo supporta. Se stai utilizzando altri client, verifica se il tuo client supporta la risposta `PassiveIp=0.0.0.0`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 15 caratteri.

Campo obbligatorio: no

SetStatOption

Utilizza `SetStatOption` per ignorare l'errore generato quando il client tenta di utilizzare `SETSTAT` su un file che stai caricando su un bucket S3.

Alcuni client di trasferimento file SFTP possono tentare di modificare gli attributi dei file remoti, inclusi timestamp e autorizzazioni, utilizzando i comandi, ad esempio `SETSTAT` durante il caricamento del file. Tuttavia, questi comandi non sono compatibili con i sistemi di archiviazione degli oggetti, come Amazon S3. A causa di questa incompatibilità, i caricamenti di file da questi client possono causare errori anche quando il file viene caricato correttamente.

Imposta il parametro su `ENABLE_NO_OP` per fare in modo che il server Transfer Family ignori il comando `SETSTAT` e carichi i file senza dover modificare il client SFTP. Sebbene l'`SetStatOption``ENABLE_NO_OP`impostazione ignori l'errore, genera una voce di registro in Amazon CloudWatch Logs, in modo da poter determinare quando il client sta effettuando una `SETSTAT` chiamata.

> **Note**
>
> Se desideri mantenere il timestamp originale per il file e modificare altri attributi del file utilizzando `SETSTAT`, puoi utilizzare Amazon EFS come archiviazione back-end con Transfer Family.

- Tipo: stringa

Valori validi: `DEFAULT | ENABLE_NO_OP`

Campo obbligatorio: no

TlsSessionResumptionMode

Una proprietà utilizzata con i server Transfer Family che utilizzano il protocollo FTPS. TLS Session Resumption fornisce un meccanismo per riprendere o condividere una chiave segreta negoziata tra il controllo e la connessione dati per una sessione FTPS. `TlsSessionResumptionMode` determina se il server riprende o meno le sessioni negoziate recenti tramite un ID di sessione univoco. Questa proprietà è disponibile durante le chiamate `CreateServer` e `UpdateServer`. Se un valore `TlsSessionResumptionMode` non è specificato durante `CreateServer`, viene impostato su `ENFORCED` per impostazione predefinita.

- `DISABLED`: il server non elabora le richieste client di ripresa della sessione TLS e crea una nuova sessione TLS per ogni richiesta.
- `ENABLED`: il server elabora e accetta i client che eseguono la ripresa della sessione TLS. Il server non rifiuta le connessioni dati client che non eseguono l'elaborazione client di ripresa della sessione TLS.
- `ENFORCED`: il server elabora e accetta i client che eseguono la ripresa della sessione TLS. Il server rifiuta le connessioni dati client che non eseguono l'elaborazione client di ripresa della sessione TLS. Prima di impostare il valore su `ENFORCED`, testa i tuoi client.

> **Note**
>
> Non tutti i client FTPS eseguono la ripresa della sessione TLS. Pertanto, se scegli di forzare la ripresa della sessione TLS, impedisci qualsiasi connessione da client FTPS che non eseguono la negoziazione del protocollo. Per determinare se è possibile utilizzare o meno il valore `ENFORCED`, devi testare i tuoi client.

- Tipo: stringa

Valori validi: `DISABLED | ENABLED | ENFORCED`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

S3FileLocation

Speciifica i dettagli per la posizione del file utilizzato nel flusso di lavoro. Applicabile solo se utilizzi lo storage S3.

Indice

Bucket

Speciifica il bucket S3 che contiene il file utilizzato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 63 caratteri.

Modello: `[a-z0-9][\.\-a-z0-9]{1,61}[a-z0-9]`

Campo obbligatorio: no

Etag

Il tag dell'entità è un hash dell'oggetto. L'ETag riflette solo i cambiamenti ai contenuti di un oggetto, non i suoi metadata.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 65536.

Modello: `.+`

Campo obbligatorio: no

Key

Il nome assegnato al file quando è stato creato in Amazon S3. La chiave dell'oggetto viene utilizzata per recuperare l'oggetto.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `[\P{M}\p{M}]*`

Campo obbligatorio: no

VersionId

Speciifica la versione del file.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri.

Modello: `.+`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

S3InputFileLocation

Speciifica la posizione del file Amazon S3 di input dal cliente. Se viene utilizzato all'internocopyStepDetails.DestinationFileLocation, dovrebbe essere la destinazione della copia S3.

È necessario fornire il secchio e la chiave. La chiave può rappresentare un percorso o un file. Ciò è determinato dal fatto che il valore della chiave venga terminato o meno con il carattere barra (/). Se il carattere finale è «/», il file viene copiato nella cartella e il suo nome non cambia. Se invece il carattere finale è alfanumerico, il file caricato viene rinominato con il valore del percorso. In questo caso, se esiste già un file con quel nome, viene sovrascritto.

Ad esempio, se il percorso è`shared-files/bob/`, i file caricati vengono copiati nella cartella`shared-files/bob/`,. Se il percorso è*`shared-files/today`*, ogni file caricato viene copiato nella *`shared-files`* cartella e denominato*`today`*: ogni caricamento sovrascrive la versione precedente del file bob.

Indice

Bucket

Specifica il bucket S3 per il file di input del cliente.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 63 caratteri.

Modello: `[a-z0-9][\.\-a-z0-9]{1,61}[a-z0-9]`

Campo obbligatorio: no

Key

Il nome assegnato al file quando è stato creato in Amazon S3. La chiave dell'oggetto viene utilizzata per recuperare l'oggetto.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 1024 caratteri.

Modello: `[\P{M}\p{M}]*`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

S3StorageOptions

Le opzioni di storage di Amazon S3 configurate per il tuo server.

Indice

DirectoryListingOptimization

Speciifica se le prestazioni per le tue directory Amazon S3 sono ottimizzate o meno. Questa opzione è disabilitata per impostazione predefinita.

Per impostazione predefinita, le mappature delle home directory hanno un valore di. `TYPE` `DIRECTORY` Se si abilita questa opzione, è necessario impostarla esplicitamente su `FILE` se si desidera che una mappatura abbia un file di destinazione. `HomeDirectoryMapEntry` `Type`

-Tipo: stringa

Valori validi: `ENABLED | DISABLED`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

S3Tag

Specifica la coppia chiave-valore assegnata a un file durante l'esecuzione di una fase di tagging.

Indice

Key

Il nome assegnato al tag creato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 128 caratteri.

Modello: `([\p{L}\p{Z}\p{N}_.:/=+\-@]*)`

Campo obbligatorio: sì

Value

Il valore che corrisponde alla chiave.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `([\p{L}\p{Z}\p{N}_.:/=+\-@]*)`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ServiceMetadata

Un oggetto contenitore per i dettagli della sessione associati a un flusso di lavoro.

Indice

UserDetails

Server ID (`ServerId`), Session ID (`SessionId`) e user (`UserName`) costituisconoUserDetails.

Tipo: oggetto UserDetails

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

SftpConnectorConfig

Contiene i dettagli per un oggetto connettore SFTP. L'oggetto connettore viene utilizzato per trasferire file da e verso il server SFTP di un partner.

> **Note**
>
> Poiché il tipo di `SftpConnectorConfig` dati viene utilizzato sia per la creazione che per l'aggiornamento dei connettori SFTP, `TrustedHostKeys` i relativi parametri `UserSecretId` sono contrassegnati come non obbligatori. Ciò è un po' fuorviante, in quanto non sono necessari quando si aggiorna un connettore SFTP esistente, ma sono necessari quando si crea un nuovo connettore SFTP.

Indice

TrustedHostKeys

La parte pubblica della chiave host, o delle chiavi, utilizzate per identificare il server esterno a cui ci si connette. È possibile utilizzare il `ssh-keyscan` comando sul server SFTP per recuperare la chiave necessaria.

I tre elementi standard in formato chiave pubblica SSH sono `<key type><body base64>`, e uno opzionale`<comment>`, con spazi tra ogni elemento. Specificate solo `<key type>` e`<body base64>`: non inserite la `<comment>` parte della chiave.

Come chiave host affidabile, AWS Transfer Family accetta le chiavi RSA ed ECDSA.

- Per le chiavi RSA, la stringa è. `<key type>` `ssh-rsa`
- Per le chiavi ECDSA, la `<key type>` stringa è o `ecdsa-sha2-nistp256` `ecdsa-sha2-nistp384``ecdsa-sha2-nistp521`, a seconda della dimensione della chiave generata.

Eseguite questo comando per recuperare la chiave host del server SFTP, dove si trova il nome del server SFTP. `ftp.host.com`

```
ssh-keyscan ftp.host.com
```

Questo stampa la chiave dell'host pubblico sullo standard output.

```
ftp.host.com ssh-rsa AAAAB3Nza...<long-string-for-public-key
```

Copia e incolla questa stringa nel `TrustedHostKeys` campo del `create-connector` comando o nel campo Trusted host keys della console.

Tipo: matrice di stringhe

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 10 elementi.

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

UserSecretId

L'identificatore del segreto (in AWS Secrets Manager) che contiene la chiave privata, la password o entrambe dell'utente SFTP. L'identificatore deve essere l'Amazon Resource Name (ARN) del segreto.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

SshPublicKey

Fornisce informazioni sulla chiave pubblica Secure Shell (SSH) associata a un utente Transfer Family per lo specifico server abilitato al protocollo di trasferimento file (come identificato da). `ServerId` Le informazioni restituite includono la data di importazione della chiave, il contenuto della chiave pubblica e il relativo ID. Un utente può memorizzare più di una chiave SSH pubblica associata al proprio nome utente su un server specifico.

Indice

DateImported

Speciifica la data in cui la chiave pubblica è stata aggiunta all'utente Transfer Family.

Tipo: Timestamp

Campo obbligatorio: sì

SshPublicKeyBody

Specifica il contenuto della chiave pubblica SSH come specificato dall'`PublicKeyId`.

AWS Transfer Family accetta le chiavi RSA, ECDSA ed ED25519.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 2048 caratteri.

Campo obbligatorio: sì

SshPublicKeyId

Speciifica che il `SshPublicKeyId` parametro contiene l'identificatore della chiave pubblica.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza fissa di 21.

Modello: `key-[0-9a-f]{17}`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Tag

Crea una coppia chiave-valore per una risorsa specifica. I tag sono metadati che è possibile utilizzare per cercare e raggruppare una risorsa per vari scopi. È possibile applicare tag a server, utenti e ruoli. Una chiave di tag può assumere più di un valore. Ad esempio, per raggruppare i server a fini contabili, è possibile creare un tag chiamato `Group` e assegnare i valori `Research` e `Accounting` a quel gruppo.

Indice

Key

Il nome assegnato al tag che crei.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 128 caratteri.

Campo obbligatorio: sì

Value

Contiene uno o più valori assegnati al nome chiave creato.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

TagStepDetails

Ogni tipo di passo ha una propria `StepDetails` struttura.

Le coppie chiave/valore utilizzate per etichettare un file durante l'esecuzione di una fase del flusso di lavoro.

Indice

Name

Il nome del passaggio, utilizzato come identificatore.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 30.

Modello: `[\w-]*`

Campo obbligatorio: no

SourceFileLocation

Speciifica il file da utilizzare come input per la fase del flusso di lavoro: l'output del passaggio precedente o il file originariamente caricato per il flusso di lavoro.

- Per utilizzare il file precedente come input, immettere`${previous.file}`. In questo caso, questa fase del flusso di lavoro utilizza come input il file di output della fase precedente del flusso di lavoro. Si tratta del valore di default.
- Per utilizzare la posizione del file originariamente caricato come input per questo passaggio, inserisci`${original.file}`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. La lunghezza massima è 256 caratteri.

Modello: `\$\{(\w+.)+\w+\}`

Campo obbligatorio: no

Tags

Array che contiene da 1 a 10 coppie chiave/valore.

Tipo: matrice di oggetti S3Tag

Membri dell'array: numero minimo di 1 elemento. Numero massimo di 10 elementi.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

UserDetails

Specificate il nome utente, l'ID del server e l'ID di sessione per un flusso di lavoro.

Indice

ServerId

L'identificatore univoco assegnato dal sistema per un'istanza del server di trasferimento.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `s-([0-9a-f]{17})`

Campo obbligatorio: sì

UserName

Una stringa univoca che identifica un utente Transfer Family associato a un server.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. Lunghezza massima di 100.

Modello: `[\w][\w@.-]{2,99}`

Campo obbligatorio: sì

SessionId

L'identificatore univoco assegnato dal sistema per una sessione che corrisponde al flusso di lavoro.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 3. La lunghezza massima è 32 caratteri.

Modello: `[\w-]*`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue AWS :

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

WorkflowDetail

Specifica l'ID del flusso di lavoro da assegnare e il ruolo di esecuzione utilizzato per l'esecuzione del flusso di lavoro.

Oltre a un flusso di lavoro da eseguire quando un file viene caricato completamente, `WorkflowDetails` può contenere anche un ID del flusso di lavoro (e ruolo di esecuzione) per l'esecuzione di un flusso di lavoro in caso di caricamento parziale. Un caricamento parziale si verifica quando la sessione del server si disconnette mentre il file è ancora in fase di caricamento.

Indice

ExecutionRole

Include le autorizzazioni necessarie per le operazioni S3, EFS e Lambda che Transfer può assumere, in modo che tutte le fasi del flusso di lavoro possano funzionare sulle risorse richieste

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 20. La lunghezza massima è 2048 caratteri.

Modello: `arn:.*role/\S+`

Campo obbligatorio: sì

WorkflowId

Un identificatore univoco per il flusso di lavoro.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 19.

Modello: `w-([a-z0-9]{17})`

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

WorkflowDetails

Container per il tipo di dati `WorkflowDetail`. Viene utilizzato da azioni che attivano un flusso di lavoro per iniziare l'esecuzione.

Indice

OnPartialUpload

Un trigger che avvia un flusso di lavoro se un file viene caricato solo parzialmente. Puoi collegare un flusso di lavoro a un server che viene eseguito ogni volta che si verifica un caricamento parziale.

Un caricamento parziale si verifica quando un file è aperto quando la sessione si disconnette.

> **Note**
>
> `OnPartialUpload`può contenere al massimo un `WorkflowDetail` oggetto.

Tipo: matrice di oggetti WorkflowDetail

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Campo obbligatorio: no

OnUpload

Un trigger che avvia un flusso di lavoro: il flusso di lavoro inizia a essere eseguito dopo il caricamento di un file.

Per rimuovere un flusso di lavoro associato da un server, è possibile fornire un oggetto `OnUpload` vuoto, come nel seguente esempio.

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details '{"OnUpload":[]}'
```

> **Note**
>
> `OnUpload`può contenere al massimo un `WorkflowDetail` oggetto.

Tipo: matrice di oggetti WorkflowDetail

Membri dell'array: numero minimo di 0 elementi. Numero massimo di 1 elemento.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

WorkflowStep

L'elemento di base di un flusso di lavoro.

Indice

CopyStepDetails

Dettagli per un passaggio che esegue una copia del file.

È costituito dai valori seguenti:

- Una descrizione
- Una posizione Amazon S3 per la destinazione della copia del file.
- Un contrassegno che indica se sovrascrivere o meno un file esistente con lo stesso nome. Il valore predefinito è `FALSE`.

Tipo: oggetto CopyStepDetails

Campo obbligatorio: no

CustomStepDetails

Dettagli per un passaggio che richiama una AWS Lambda funzione.

È costituito dal nome della funzione lambda, dalla destinazione e dal timeout (in secondi).

Tipo: oggetto CustomStepDetails

Campo obbligatorio: no

DecryptStepDetails

Dettagli su un passaggio che decrittografa un file crittografato.

È costituito dai valori seguenti:

- Un nome descrittivo
- Una posizione Amazon S3 o Amazon Elastic File System (Amazon EFS) per la decrittografia del file di origine.
- Una posizione S3 o Amazon EFS per la destinazione della decrittografia dei file.
- Un contrassegno che indica se sovrascrivere o meno un file esistente con lo stesso nome. Il valore predefinito è `FALSE`.
- Il tipo di crittografia utilizzato. Attualmente è supportata solo la crittografia PGP.

Tipo: oggetto DecryptStepDetails

Campo obbligatorio: no

DeleteStepDetails

Dettagli per un passaggio che elimina il file.

Tipo: oggetto DeleteStepDetails

Campo obbligatorio: no

TagStepDetails

Dettagli per un passaggio che crea uno o più tag.

Puoi specificare uno o più tag. Ogni tag è costituito da una coppia chiave-valore.

Tipo: oggetto TagStepDetails

Campo obbligatorio: no

Type

Attualmente sono supportati i seguenti tipi di passaggio.

- **`COPY`** - Copiare il file in un'altra posizione.
- **`CUSTOM`**- Esegui un passaggio personalizzato con un obiettivo di AWS Lambda funzione.
- **`DECRYPT`** - Decrittografare un file crittografato prima che è stato caricato.
- **`DELETE`** - Eliminare il file.
- **`TAG`** - Aggiungere un tag al file.

Tipo: stringa

Valori validi: `COPY | CUSTOM | TAG | DELETE | DECRYPT`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2

- AWS SDK per Ruby V3

Effettuare richieste API

Oltre a utilizzare la console, puoi utilizzare l'AWS Transfer FamilyAPI per configurare e gestire i tuoi server in modo programmatico. Questa sezione descrive le operazioni AWS Transfer Family, la firma delle richieste per l'autenticazione e la gestione degli errori. Per informazioni sulle regioni e gli endpoint disponibili per Transfer Family, consulta AWS Transfer Familyendpoint e quote nel Riferimenti generali di AWS

> **Note**
>
> Puoi anche utilizzare gli AWS SDK per sviluppare applicazioni con Transfer Family;. Gli AWS SDK per Java, .NET e PHP racchiudono l'API Transfer Family sottostante, semplificando le attività di programmazione. Per informazioni sul download delle librerie SDK, consulta Librerie di codice di esempio.

Argomenti

- Intestazioni di richiesta obbligatorie per Transfer Family
- Input e firma delle richieste Transfer Family
- Risposte agli errori
- Librerie disponibili

Intestazioni di richiesta obbligatorie per Transfer Family

Questa sezione descrive le intestazioni obbligatorie a cui devi inviare con ogni richiesta POST. AWS Transfer Family Devi includere intestazioni HTTP per identificare le informazioni principali sulla richiesta, tra cui l'operazione che vuoi richiamare, la data della richiesta e le informazioni che indicano la tua autorizzazione come mittente della richiesta. Le intestazioni fanno distinzione tra maiuscole e minuscole, ma l'ordine delle intestazioni non è importante.

L'esempio seguente mostra le intestazioni utilizzate nell'ListServersoperazione.

```
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}
```

Di seguito sono riportate le intestazioni che devono essere incluse nelle richieste POST a Transfer Family. Le intestazioni mostrate di seguito che iniziano con «x-amz» sono specifiche per. AWS Tutte le altre intestazioni elencate sono intestazioni comuni usate in transazioni HTTP.

Intestazione	Descrizione
`Authorization`	L'intestazione di autorizzazione è obbligatoria. Il formato è la firma di richiesta Sigv4 standard, documentata nelle richieste dell'API di firma. AWS
`Content-Type`	Utilizza `application/x-amz-json-1.1` come tipo di contenuto per tutte le richieste a Transfer Family. `Content-Type: application/x-amz-json-1.1`
`Host`	Utilizza l'intestazione host per specificare l'endpoint Transfer Family a cui inviare la richiesta. Ad esempio, `transfer.us-east-1.amazonaws.com` è l'endpoint per la regione Stati Uniti orientali (Ohio). Per ulteriori informazioni sugli endpoint disponibili per Transfer Family, vedere AWS Transfer Familyendpoint e quote nel. Riferimenti generali di AWS `Host: transfer.` *`region`*`.amazonaws.com`
`x-amz-date`	È necessario fornire il timestamp nell'intestazione HTTP o nell'`Date`intestazione. AWS `x-amz-date` (Alcune librerie client HTTP non consentono di impostare l'intestazione `Date`) Quando è presente un'`x-amz-date` intestazione, Transfer Family ignora qualsiasi `Date`

Intestazione	Descrizione
	intestazione durante l'autenticazione della richiesta. Il `x-amz-date` formato deve essere ISO8601, nel formato YYYYMMDD'T'HHMMSS'Z'. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	Questa intestazione specifica la versione dell'API e l'operazione richiesta . I valori dell'intestazione target sono formati concatenando la versione API con il nome API e usano il formato seguente. `x-amz-target: TransferService. operationName` Il valore OperationName (`ListServers` ad esempio) può essere trovato dall'elenco delle API,. ListServers
`x-amz-security-token`	Questa intestazione è richiesta quando le credenziali utilizzate per firmare la richiesta sono temporanee o credenziali di sessione (per i dettagli, consulta Using temporary credentials with AWS resources nella IAM User Guide). Per ulteriori informazioni, consulta Aggiungere la firma alla richiesta HTTP nelRiferimenti generali di Amazon Web Services.

Input e firma delle richieste Transfer Family

Tutti gli input della richiesta devono essere inviati come parte del payload JSON nel corpo della richiesta. Per le azioni in cui tutti i campi di richiesta sono facoltativi, ad esempio`ListServers`, è comunque necessario fornire un oggetto JSON vuoto nel corpo della richiesta, ad esempio. `{}` La struttura della richiesta/risposta del payload Transfer Family è documentata, ad esempio, nel riferimento all'API esistente. DescribeServer

Transfer Family supporta l'autenticazione tramite AWS Signature Version 4. Per i dettagli, consulta la sezione Richieste AWS API di firma.

Risposte agli errori

Quando si verifica un errore, le informazioni dell'intestazione della risposta contengono:

- Tipo di contenuto: `application/x-amz-json-1.1`
- Un codice di stato HTTP `4xx` o `5xx` appropriato

Il corpo di una risposta di errore contiene informazioni relative all'errore. La risposta di errore di esempio seguente mostra la sintassi di output degli elementi della risposta comuni a tutte le risposte di errore.

```
{
    "__type": "String",
    "Message": "String", <!-- Message is lowercase in some instances -->
    "Resource": String,
    "ResourceType": String
    "RetryAfterSeconds": String
}
```

La tabella seguente illustra i campi della risposta di errore JSON mostrata nella sintassi precedente.

__type

Una delle eccezioni a una chiamata API Transfer Family.

Tipo: stringa

Messaggio o messaggio

Uno dei messaggi dei codici di errore delle operazioni in .

> **Note**
>
> Alcune eccezioni utilizzano `message` e altre utilizzano`Message`. Puoi controllare il codice dell'interfaccia per determinare il caso corretto. In alternativa, puoi testare ogni opzione per vedere quale funziona.

Tipo: stringa

Resource (Risorsa)

La risorsa per la quale viene invocato l'errore. Ad esempio, se si tenta di creare un utente già esistente, `Resource` è il nome utente dell'utente esistente.

Tipo: stringa

ResourceType

Il tipo di risorsa per cui viene richiamato l'errore. Ad esempio, se si tenta di creare un utente già esistente, `ResourceType` è`User`.

Tipo: stringa

RetryAfterSeconds

Il numero di secondi di attesa prima di riprovare il comando.

Tipo: stringa

Esempi di risposte agli errori

Il seguente corpo JSON viene restituito se si chiama l'`DescribeServer`API e si specifica un server che non esiste.

```
{
  "__type": "ResourceNotFoundException",
  "Message": "Unknown server",
  "Resource": "s-11112222333344444",
  "ResourceType": "Server"
}
```

Il seguente corpo JSON viene restituito se l'esecuzione di un'API causa la limitazione.

```
{
   "__type":"ThrottlingException",
   "RetryAfterSeconds":"1"
}
```

Il seguente corpo JSON viene restituito se si utilizza l'`CreateServer`API e non si dispone di autorizzazioni sufficienti per creare un server Transfer Family.

```
{
  "__type": "AccessDeniedException",
  "Message": "You do not have sufficient access to perform this action."
}
```

Il seguente corpo JSON viene restituito se si utilizza l'`CreateUser`API e si specifica un utente già esistente.

```
{
  "__type": "ResourceExistsException",
  "Message": "User already exists",
  "Resource": "Alejandro-Rosalez",
  "ResourceType": "User"
}
```

Librerie disponibili

AWSfornisce librerie, codice di esempio, tutorial e altre risorse per gli sviluppatori di software che preferiscono creare applicazioni utilizzando API specifiche del linguaggio anziché gli strumenti da riga di comando e l'API Query. Queste librerie forniscono funzioni di base (non incluse nelle API), come l'autenticazione delle richieste, i nuovi tentativi di richiesta e la gestione degli errori, in modo che sia più facile iniziare. Vedi Strumenti su cui basarsi AWS

Per le librerie e il codice di esempio in tutte le lingue, vedi Codice di esempio e librerie.

Parametri comuni

L'elenco seguente contiene i parametri utilizzati da tutte le azioni per firmare le richieste di Signature Version 4 con una stringa di query. Qualsiasi parametro specifico di un'operazione è riportato nell'argomento relativo all'operazione. Per ulteriori informazioni sull'utilizzo di Signature Version 4, consulta la pagina Firma delle richieste API AWS nella Guida per l'utente di IAM.

Action

azione da eseguire.

Tipo: stringa

Campo obbligatorio: sì

Version

Versione dell'API per cui è scritta la richiesta, espressa nel formato AAAA-MM-GG.

Tipo: stringa

Campo obbligatorio: sì

X-Amz-Algorithm

Algoritmo hash utilizzato per creare la firma della richiesta.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Valori validi: `AWS4-HMAC-SHA256`

Obbligatorio: condizionale

X-Amz-Credential

Il valore dell'ambito delle credenziali, che è una stringa che include la chiave di accesso, la data, la regione di destinazione, il servizio richiesto e una stringa di terminazione ("aws4_request"). Il valore viene espresso nel seguente formato: chiave_accesso/AAAAMMGG/regione/servizio/aws4_request.

Per ulteriori informazioni, consulta la pagina Creazione di una richiesta API AWS firmata nella Guida per l'utente di IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Date

La data utilizzata per creare la firma. Il formato deve essere il formato di base ISO 8601 (YYYYMMDD'T'HHMMSS'Z'). Ad esempio, la seguente combinazione data/ora è un valore X-Amz-Date valido: `20120325T120000Z`.

Condition: X-Amz-Date è facoltativo per tutte le richieste; può essere utilizzato per sovrascrivere la data utilizzata per firmare le richieste. Se l'intestazione Date è specificata nel formato base ISO 8601, X-Amz-Date non è richiesto. Quando utilizzi X-Amz-Date, sostituisce sempre il valore dell'intestazione Date. Per ulteriori informazioni, consulta la pagina Elementi di una firma di richiesta API AWS nella Guida per l'utente di IAM.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Security-Token

Il token di sicurezza provvisorio ottenuto tramite una chiamata ad AWS Security Token Service (AWS STS). Per un elenco di servizi che supportano le credenziali di sicurezza temporanee da AWS STS, consulta la pagina Servizi AWS che funzionano con IAM nella Guida per l'utente di IAM.

Condizione: se utilizzi le credenziali di sicurezza temporanee fornite da AWS STS, devi includere il token di sicurezza.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Signature

Specifica la firma con codifica esadecimale calcolata dalla stringa da firmare e dalla chiave di firma derivata.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-SignedHeaders

Specifica tutte le intestazioni HTTP incluse come parte della richiesta canonica. Per ulteriori informazioni sulla specifica delle intestazioni firmate, consulta la pagina Creazione di una richiesta API AWS firmata nella Guida per l'utente di IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

Errori comuni

In questa sezione sono riportati gli errori comuni delle azioni API per tutti i servizi AWS. Per gli errori specifici di un'azione API per questo servizio, consulta l'argomento per quell'azione API.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

IncompleteSignature

La firma della richiesta non è conforme agli standard AWS.

Codice di stato HTTP: 400

InternalFailure

L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto interno sconosciuto.

Codice di stato HTTP: 500

InvalidAction

L'azione o l'operazione richiesta non è valida. Verifica che l'operazione sia digitata correttamente.

Codice di stato HTTP: 400

InvalidClientTokenId

Il certificato X.509 o l'ID chiave di accesso AWS forniti non sono presenti nei nostri record.

Codice di stato HTTP: 403

NotAuthorized

Non disponi delle autorizzazioni per eseguire questa azione.

Codice di stato HTTP: 400

OptInRequired

L'ID chiave di accesso AWS necessita di una sottoscrizione al servizio.

Codice di stato HTTP: 403

RequestExpired

La richiesta ha raggiunto il servizio più di 15 minuti dopo il date stamp della richiesta o più di 15 minuti dopo la data di scadenza della richiesta (ad esempio per URL prefirmati) oppure il date stamp della richiesta è più di 15 minuti nel futuro.

Codice di stato HTTP: 400

ServiceUnavailable

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 503

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

ValidationError

L'input non riesce a soddisfare i vincoli specificati da un servizio AWS.

Codice di stato HTTP: 400

Cronologia dei documenti per AWS Transfer Family

La tabella seguente descrive la documentazione per questa versione di AWS Transfer Family.

- Versione API: transfer-2018-11-05
- Ultimo aggiornamento della documentazione: 23 aprile 2024

Modifica	Descrizione	Data
Possibilità per i connettori SFTP di elencare file e directory remote	Transfer Family ha aggiunto la possibilità per i nostri clienti di utilizzare i connettori SFTP per elencare i file archiviati in server SFTP remoti. Per maggiori dettagli, consulta Elenca il contenuto di una directory remota.	23 aprile 2024
Possibilità di utilizzare il certificato TLS autofirmato di un partner commerciale con lo scambio di messaggi AS2	AWS Transfer Family ha aggiunto la possibilità di importare e utilizzare il certificato TLS pubblico e autofirmato di un partner commerciale per l'invio di messaggi dell'Applicability Statement 2 (AS2) al relativo server tramite HTTPS.	12 aprile 2024
Aggiunta di politiche di sicurezza per i connettori SFTP	AWS Transfer Family ha aggiunto politiche di sicurezza da utilizzare con i connettori SFTP. Per informazioni dettagliate, vedi Politiche AWS Transfer Family di sicurezza per i connettori SFTP.	5 aprile 2024

Modifica	Descrizione	Data
Integrazione con Amazon EventBridge	AWS Transfer Family ora pubblica automaticamente gli eventi su Amazon EventBrid ge per tutte le operazioni di trasferimento di file. Per informazioni dettagliate, vedi Gestione Transfer Family degli eventi tramite Amazon EventBridge.	8 febbraio 2024
Aggiunta di nuove politiche di sicurezza	AWS Transfer Family ha aggiunto nuove politiche di sicurezza FIPS e non FIPS. Inoltre, la politica di sicurezza predefinita assegnata ai server è sempre la politica di sicurezza più recente. Per informazioni dettagliate, vedi Politiche di sicurezza per AWS Transfer Family i server.	5 febbraio 2024
Support per indirizzi IP statici per connettori SFTP e AS2	Transfer Family ora fornisce indirizzi IP statici per connettor i SFTP e AS2. Ciò consente la connessione con server SFTP remoti protetti da controlli IP allowlist. Per AS2, stiamo introducendo gli indirizzi IP statici per le risposte MDN asincrone dai server AS2.	16 gennaio 2024

Modifica	Descrizione	Data
La guida per l'utente è stata riorganizzata per allinearl a maggiormente all'ultima versione di. AWS Transfer Family	Transfer Family ha aggiunto diverse funzionalità sin dalla sua nascita, rendendo necessaria una ristrutturazione della guida.	3 gennaio 2024
Miglioramenti alla mappatura delle directory logiche Ottimizzazione delle prestazio ni degli elenchi Amazon S3	Transfer Family ora supporta mappature di directory logiche fino a 2,1 MB. Ora puoi anche dichiarare se la mappatura di un utente si riferisce a un file. Per ulteriori informazioni, consulta Regole per l'utilizzo delle directory logiche. Quando crei o aggiorni un server che utilizza Amazon S3 per lo storage, ora puoi ottimizzare le prestazioni di elencazione delle tue directory (o cartelle) S3. Per ulteriori informazioni, consulta Configurazione di un endpoint server SFTP, FTPS o FTP.	17 novembre 2023
Porta alternativa per server SFTP con endpoint VPC (Virtual Private Cloud)	Ora puoi abilitare una porta alternativa non standard per i tuoi server SFTP Transfer Family con endpoint VPC. Per ulteriori informazioni, consulta Crea un server in un cloud privato virtuale.	17 novembre 2023

Modifica	Descrizione	Data
Support per connettori SFTP	I connettori SFTP estendono le capacità AWS Transfer Family di comunicazione con server remoti sia nel cloud che in locale. Per ulteriori informazioni, consulta Inviare e recuperare file utilizzando un connettore SFTP.	25 luglio 2023
Support per l'autenticazione AS2 Basic	Transfer Family ora supporta l'utilizzo dell'autenticazione di base per i server che utilizzano il protocollo Applicability Statement 2 (AS2). Per ulteriori informazioni, consulta Autenticazione di base per connettori AS2.	30 giugno 2023
Support per la registrazione JSON strutturata	Transfer Family ora supporta la fornitura di log JSON strutturati ad Amazon CloudWatch, il raggruppamento di flussi di log in gruppi di log personalizzati e l'esecuzione di query di log comuni tra protocolli. Per ulteriori informazioni, consulta CloudWatch Registrazione Amazon per AWS Transfer Family.	24 giugno 2023

Modifica	Descrizione	Data
Support per diversi metodi di autenticazione	Transfer Family supporta l'autenticazione tramite una password, una coppia di chiavi pubblica/privata o entrambe. È disponibile per i server che utilizzano il protocollo SFTP e un provider di identità personalizzato. Per ulteriori informazioni, consulta Crea un server compatibile con SFTP.	17 maggio 2023
Support per la decrittografia Pretty Good Privacy (PGP) con file che Transfer Family elabora con flussi di lavoro	Transfer Family ha il supporto integrato per la decrittog rafia Pretty Good Privacy (PGP). Puoi utilizzare la decrittografia PGP su file caricati tramite SFTP, FTPS o FTP su Amazon Simple Storage Service (Amazon S3) o Amazon Elastic File System (Amazon EFS). Per ulteriori informazioni, consulta Genera e gestisci le chiavi PGP e Usa la decrittografia PGP nel tuo flusso di lavoro.	21 dicembre 2022
Supporto completamente gestito per il protocollo di trasferimento file Applicability Statement 2 (AS2) con server Transfer Family	È possibile creare server che utilizzano il protocollo AS2 per l'invio e la ricezione di informazioni da e verso partner commerciali che si trovano all'interno o all'ester no dell'ambiente. AWS Per ulteriori informazioni, consulta Configurazione di AS2.	25 luglio 2022

Modifica	Descrizione	Data
Support per i banner di visualizzazione durante la creazione di un server	È possibile aggiungere messaggi personalizzati durante la creazione dei server. È possibile visualizzare un messaggio di preautenticazione (tutti i protocolli) e un messaggio di post-autenticazione (per server FTP e FTPS). Per ulteriori informazioni, consulta Crea un server compatibile con SFTP, Creare un server compatibile con FTPS o Crea un server abilitato all'FTP.	17 febbraio 2022
Support AWS Lambda come provider di identità	Ora puoi connetterti a un provider di identità personalizzato utilizzando AWS Lambda i relativi server Transfer Family. In precedenza, era necessario fornire un Amazon API Gateway URL per integrare un provider di identità personalizzato. Per ulteriori informazioni, consulta Utilizzo AWS Lambda per integrare il proprio provider di identità.	16 novembre 2021

Modifica	Descrizione	Data
Support per flussi di lavoro di trasferimento gestito di file	I flussi di lavoro di trasferim ento file gestito forniscono astrazioni di elaborazione post-caricamento per le attività più comuni che attualmen te esegui manualmente. Per ulteriori informazioni, consulta AWS Transfer Family flussi di lavoro gestiti.	2 settembre 2021
Support per AWS Directory Service for Microsoft Active Directory	Oltre ai provider di identità personalizzati e gestiti dal servizio, ora puoi utilizzare AWS Directory Service for Microsoft Active Directory per gestire l'accesso degli utenti per l'autenticazione e l'autorizzazione. Per ulteriori informazioni, consulta Utilizzo del provider di identità AWS Directory Service.	24 maggio 2021
Nuovo Regioni AWS	AWS Transfer Family è ora disponibile nella regione Africa (Città del Capo). Per ulteriori informazioni sugli endpoint Transfer Family, vedere AWS Transfer Family endpoint e quote nel. Riferimenti generali di AWS	24 febbraio 2021

Modifica	Descrizione	Data
Nuovo Regioni AWS	AWS Transfer Family è ora disponibile nelle regioni Asia Pacifico (Hong Kong) e Medio Oriente (Bahrain). Per ulteriori informazioni sugli endpoint Transfer Family, vedere AWS Transfer Family endpoint e quote nel. Riferimenti generali di AWS	17 febbraio 2021
Support per Amazon EFS come archivio dati	Transfer Family ora supporta i trasferimenti di file da e verso Amazon Elastic File System (Amazon EFS). Amazon EFS è un file system NFS elastico semplice, scalabile e completamente gestito. Per ulteriori informazioni, consulta Configurazione di un file system Amazon EFS.	06 gennaio 2021
Support per AWS WAF	Transfer Family ora supporta AWS WAF un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le operazioni delle API dagli attacchi. Per ulteriori informazioni, consulta Aggiungi un firewall per applicazioni Web.	24 novembre 2020

Modifica	Descrizione	Data
Support per più gruppi di sicurezza in un cloud privato virtuale (VPC)	Ora puoi collegare più gruppi di sicurezza a un server in un VPC. Per ulteriori informazioni, consulta Crea un server in un cloud privato virtuale.	15 ottobre 2020
Nuovo Regioni AWS	Transfer Family è ora disponibile nelle AWS GovCloud (US) regioni. Per ulteriori informazioni sugli endpoint Transfer Family for AWS GovCloud (US) Regions, vedere AWS Transfer Family endpoint e quote in. Riferimenti generali di AWS Per informazioni sull'utilizzo di Transfer Family nelle AWS GovCloud (US) regioni, consulta AWS Transfer Familyla Guida AWS GovCloud (US) per l'utente.	30 settembre 2020
È ora possibile collegare al server una politica di sicurezza con algoritmi crittografici supportati	Ora puoi allegare al tuo server una politica di sicurezza che contiene un set di algoritmi crittografici supportati. Per ulteriori informazioni, consulta Politiche di sicurezza per AWS Transfer Family i server.	12 agosto 2020

Modifica	Descrizione	Data
Supporto per gli endpoint Federal Information Processing Standard (FIPS)	Gli endpoint compatibili con FIPS sono ora disponibili in Nord America. Regioni AWS Per le regioni disponibili, consulta gli AWS Transfer Family endpoint e le quote nel. Riferimenti generali di AWS Per abilitare FIPS per un endpoint server compatibile con SFTP, vedere. Crea un server compatibile con SFTP Per abilitare FIPS per un endpoint server abilitato per FTPS, vedere. Creare un server compatibile con FTPS Per abilitare FIPS per un endpoint server abilitato all'FTP, vedere. Crea un server abilitato all'FTP	12 agosto 2020
Aumento della lunghezza dei caratteri del nome utente e caratteri aggiuntivi consentiti	I nomi utente possono ora contenere segni (@) e punti (.) e possono avere una lunghezza massima di 100 caratteri. Per aggiungere un utente, consultaGestione degli utenti per gli endpoint del server.	12 agosto 2020

Modifica	Descrizione	Data
Support per la creazione automatica di ruoli Amazon CloudWatch Logging AWS Identity and Access Management (IAM)	Transfer Family ora supporta la creazione automatica di un ruolo IAM CloudWatch di registrazione per visualizzare l'attività dell'utente finale. Per ulteriori informazioni, consulta Crea un server compatibile con SFTP, Creare un server compatibile con FTPS o Crea un server abilitato all'FTP.	30 luglio 2020
AWS Transfer Family ora supporta Source IP come fattore di autorizzazione.	Transfer Family aggiunge il supporto per l'utilizzo degli indirizzi IP di origine degli utenti finali come fattore di autorizzazione, consentendoti di applicare un ulteriore livello di sicurezza quando autorizzi l'accesso tramite Secure File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS) o File Transfer Protocol (FTP). Per ulteriori informazioni, consulta Lavorare con provider di identità personalizzati.	9 giugno 2020

Modifica	Descrizione	Data
AWS Transfer for SFTP è ora disponibile AWS Transfer Family e aggiunge il supporto per FTP e FTPS.	Ora puoi utilizzare due protocolli aggiuntivi per i trasferimenti di file degli utenti: File Transfer Protocol Secure (FTPS) e File Transfer Protocol (FTP). Gli utenti possono spostare, eseguire, proteggere e integrare flussi di lavoro basati su FTP su SSL (FTPS) e FTP in testo semplice AWS, oltre al supporto SFTP (Secure File Transfer Protocol) esistente.	23 aprile 2020
Support per gruppi di sicurezza del cloud privato virtuale (VPC) e indirizzi IP elastici	Ora puoi creare una lista di indirizzi IP in entrata utilizzando i gruppi di sicurezza, fornendo un ulteriore livello di sicurezza per i server. Puoi anche associare indirizzi IP elastici all'endpoint del tuo server. In questo modo, puoi consentire agli utenti protetti da firewall di consentire l'accesso a quell'endpoint. Per ulteriori informazioni, consulta Crea un server in un cloud privato virtuale.	10 gennaio 2020

Modifica	Descrizione	Data
Support per lavorare in un VPC	Ora puoi creare un server in un VPC. Puoi utilizzare il server per trasferire dati tramite client da e verso un bucket Amazon S3 senza dover utilizzare la rete Internet pubblica. Per ulteriori informazioni, consulta Crea un server in un cloud privato virtuale.	27 marzo 2019
Prima versione di rilasciata. AWS Transfer Family	Questa versione iniziale include la configurazione di direzioni, descrive come iniziare e fornisce informazi oni su configurazione client, configurazione utente e monitoraggio attività.	25 Novembre 2018

Glossario AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.