



Guida per l'utente

AWS Transfer Family



AWS Transfer Family: Guida per l'utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è AWS Transfer Family?	1
Come AWS Transfer Family funziona	4
Post del blog pertinenti per Transfer Family	5
Prerequisiti	9
Regioni, endpoint e quote	9
Iscriviti per AWS	10
Configurare l'archiviazione	10
Configurazione di un bucket Amazon S3	11
Configurazione di un file system Amazon EFS	16
Crea un ruolo e una policy IAM	19
Creazione di un ruolo utente	20
Come funzionano le politiche di sessione	24
Esempio di politica di read/write accesso	27
Tutorial Transfer Family	31
Inizia a usare gli endpoint del server	32
Prerequisiti	32
Passaggio 1: accedi alla console AWS Transfer Family	33
Fase 2: Creare un SFTP-enabled server	33
Passaggio 3: Aggiungere un utente gestito dal servizio	34
Passaggio 4: Trasferire un file utilizzando un client	36
Creare un flusso di lavoro di decrittografia	38
Fase 1: Configurare un ruolo di esecuzione	38
Fase 2: Creare un flusso di lavoro gestito	40
Fase 3: Aggiungere il flusso di lavoro a un server e creare un utente	41
Fase 4: Creare una coppia di key pair PGP	43
Passaggio 5: Memorizza la chiave privata PGP in Gestione dei segreti AWS	43
Fase 6: Crittografare un file	45
Passaggio 7: Esegui il flusso di lavoro e visualizza i risultati	45
Crea e usa connettori SFTP	46
Tipi di uscita del connettore	47
Fase 1: Creare le risorse di supporto necessarie	48
Fase 2: Creare e testare un connettore SFTP	54
Passaggio 3: invio e recupero di file utilizzando il connettore SFTP	60
Procedure per creare un server Transfer Family da utilizzare come server SFTP remoto	64

Utilizza un provider di identità personalizzato	67
Prerequisiti	67
Fase 1: Creare uno stack CloudFormation	68
Passaggio 2: verifica la configurazione del metodo API Gateway per il tuo server	69
Fase 3: Visualizzare i dettagli del server Transfer Family	70
Fase 4: Verifica che l'utente sia in grado di connettersi al server	72
Passaggio 5: verifica la connessione SFTP e il trasferimento dei file	72
Passaggio 6: Limita l'accesso al bucket	73
Aggiorna Lambda se usi Amazon EFS	75
Configurare una configurazione AS2	76
Fase 1: Creare certificati per AS2	78
Fase 2: Importazione dei certificati come risorse di certificati Transfer Family	81
Fase 3: Crea profili per te e il tuo partner commerciale	83
Fase 4: Creare un server Transfer Family che utilizzi il protocollo AS2	84
Fase 5: Crea un accordo tra te e il tuo partner	87
Passaggio 6: crea un connettore tra te e il tuo partner	89
Passaggio 7: Prova a scambiare file su AS2 utilizzando Transfer Family	90
Configura un'app web di base	92
Prerequisiti	92
Fase 1: Creare le risorse di supporto necessarie	92
Fase 2: Creare un'app web Transfer Family	93
Passaggio 3: configura la condivisione Cross-origin delle risorse (CORS) per il tuo bucket	94
Passaggio 4: aggiungi un utente alla tua app web Transfer Family	96
Fase 5: registrare una sede in Amazon S3 e creare una concessione di accesso	97
Passaggio 6: accedi alla tua app web Transfer Family come utente	99
Fasi successive	100
Integra Okta come provider di identità per app web	100
Configura l'app Web con accesso selettivo a più bucket	103
Prerequisiti	103
Fase 1: Creare un'app web Transfer Family	104
Passaggio 2: configura i ruoli IAM per l'accesso a S3	105
Fase 3: configurare S3 Access Grants	107
Fase 4: Registrare le posizioni dei bucket S3	108
Fase 5: Creare concessioni di accesso	108
Passaggio 6: configura la politica CORS per i bucket S3	109
Fase 7: Verifica la configurazione	110

Conclusioni	110
Transfer Family per SFTP, FTPS, FTP	111
Opzioni del provider di identità	111
AWS Transfer Family matrice del tipo di endpoint	113
Configurazione di un endpoint server Transfer Family	117
Crea un SFTP-enabled server	119
Crea un FTPS-enabled server	127
Crea un FTP-enabled server	136
Creare un server in un VPC	145
Lavorare con nomi host personalizzati	170
FTP/FTPS Considerazioni sull'NLB	174
Trasferisci file tramite un endpoint del server	174
SFTP/FTPS/FTP Comandi disponibili	177
Trova il tuo endpoint Amazon VPC	179
setstatEvita gli errori	181
Usa OpenSSH	37
Usa WinSCP	183
Usa Cyberduck	36
Usa FileZilla	186
Usa un client Perl	188
Usa LFTP	188
Elaborazione successiva al caricamento	188
Messaggi SFTP	189
Gestisci gli utenti	192
Confronto tra Amazon EFS e Amazon S3	192
Directory logiche	193
Quote di gruppo Active Directory	194
Service-managed utenti	195
Provider di identità personalizzato	205
Servizio di directory per MS AD	243
Servizio di directory per Entra ID	254
Usa le directory logiche	261
Comprendere chroot e la struttura delle cartelle	262
Regole per l'utilizzo delle directory logiche	262
Implementazione di directory logiche	264
Esempi di configurazioni di directory logiche	267

Configurazione di directory logiche per Amazon EFS	269
AWS Lambda Risposta personalizzata	270
Accedi a FSx per i file system NetApp ONTAP	270
Panoramica di	271
Prerequisiti	272
Come funziona lo storage FSx con Transfer Family	273
Creazione di un punto di accesso S3 per FSx	274
Utilizzo degli alias dei punti di accesso S3 con FSx	276
Configurazione di Transfer Family per lo storage FSx	279
Gestione degli utenti per lo storage FSx	280
Configurazione dei client per il trasferimento di file	282
Risoluzione dei problemi di storage FSx	283
App web Transfer Family	285
Regioni AWS per le app web Transfer Family	286
Compatibilità del browser per le app AWS Transfer Family Web	286
Come creare un'app web Transfer Family	286
Configura il tuo provider di identità	289
Configura i ruoli IAM	291
Configurare un'app web Transfer Family	293
Crea un'app web Transfer Family	294
Assegnazione di indirizzi IP	296
Crea un'app web Transfer Family in un VPC	297
Crea un'app web Transfer Family	298
Post-creation passaggi	299
Cross-origin politica di condivisione delle risorse (CORS)	300
Limitazione dell'accesso a un endpoint VPC specifico	301
Assegna o aggiungi utenti o gruppi a un'app web Transfer Family	302
Configura la condivisione Cross-origin delle risorse (CORS) per il tuo bucket	305
Configurazione delle concessioni di accesso ad Amazon S3	307
Usa un URL personalizzato	313
Registrazione per le app web Transfer Family	316
Abilitazione degli eventi relativi ai dati di Amazon S3	316
Esempi di log di autenticazione	319
Visualizzazione delle voci di registro	326
Risoluzione dei problemi relativi alle app Web	327
Risolvi gli errori di rete	327

Risolvi i problemi relativi alla mancata visualizzazione del bucket configurato	328
Risolvi gli errori relativi agli URL personalizzati	328
Risolvi errori vari	329
Bucket S3 duplicati visualizzati nell'app Web	330
Istruzioni per l'utente finale	331
Quote per le app Web	331
Utenti di IAM Identity Center	331
Third-party utenti finali	332
Interfaccia utente finale Transfer Family	333
Operazioni disponibili	334
Connettori SFTP	336
Creazione di connettori SFTP	336
Scelta del tipo di uscita del connettore SFTP	337
Scelta della modalità di indirizzamento IP	338
Archivia le credenziali in Secrets Manager	339
Crea un connettore SFTP con uscita gestita dal servizio	341
Crea un connettore SFTP con uscita VPC-based	351
Prova un connettore SFTP	363
Connettività VPC	364
Utilizzo di connettori SFTP	365
Trasferimento dei file	366
Elenca il contenuto delle directory remote	368
Sposta ed elimina file sul server remoto	369
Monitoraggio dei connettori SFTP	371
Utilizza l'API del connettore per interrogare lo stato delle richieste di trasferimento di file	372
Visualizza gli eventi del connettore SFTP in Amazon EventBridge	372
Visualizza i log dei connettori SFTP in Amazon CloudWatch	372
Monitoraggio dei connettori di tipo VPC in uscita	373
Gestione dei connettori SFTP	375
Aggiorna i connettori SFTP	375
Visualizza i dettagli del connettore SFTP	376
Quote per i connettori SFTP	377
Quote per i connettori SFTP	377
Ridimensionamento dei connettori SFTP	379
Architetture di riferimento	380
Post del blog	380

Workshop	380
Soluzioni	381
Architetture di riferimento VPC	381
Transfer Family per AS2	384
Casi d'uso di AS2	385
Modelli AS2 CloudFormation	390
Personalizzazione dei modelli AS2	390
Verifica della distribuzione AS2	391
Le migliori pratiche per la distribuzione dei modelli AS2	391
Configurare AS2	392
Configurazioni AS2	393
Quote AS2	395
Caratteristiche e funzionalità di AS2	398
Gestisci i certificati AS2	400
Importa certificati AS2	401
Rotazione dei certificati AS2	403
Crea profili AS2	405
Creare un server AS2	406
Creare un server AS2 utilizzando la console Transfer Family	406
Crea un server AS2 utilizzando un modello	409
Creare un accordo AS2	413
Configura i connettori AS2	414
Crea un connettore AS2	415
Algoritmi dei connettori AS2	418
Autenticazione di base per connettori AS2	419
Abilita l'autenticazione di base per i connettori AS2	421
Visualizza i dettagli del connettore	424
Trasferisci messaggi AS2	426
Ricevi messaggi AS2	427
Configura HTTPS per AS2	428
Trasferisci file con connettori AS2	434
Nomi e posizioni dei file	436
Codici di stato	439
File JSON di esempio	440
Intestazioni HTTP personalizzate per AS2	442
Panoramica del modello	442

Come funziona	443
Caratteristiche chiave	443
Dettagli di implementazione	443
Distribuzione e utilizzo	445
Monitora AS2	446
Codici di stato AS2	447
Codici di errore AS2	448
Monitoraggio della scadenza dei certificati	461
DaysUntilExpiry parametro	461
Le migliori pratiche per il monitoraggio dei certificati	461
Esempi di configurazioni di allarme	462
Gestione dei flussi di lavoro di elaborazione dei file	464
Crea un flusso di lavoro	466
Configura ed esegui un flusso di lavoro	468
Visualizza i dettagli del flusso di lavoro	470
Utilizza passaggi predefiniti	473
Copia il file	473
Decrittografa il file	478
Tag: file	484
Eliminare il file	485
Variabili denominate per i flussi di lavoro	486
Esempio di workflow di etichettatura ed eliminazione	486
Utilizza passaggi di elaborazione dei file personalizzati	491
Utilizzo consecutivo di più funzioni Lambda	493
Accesso a un file dopo l'elaborazione personalizzata	493
Eventi di esempio inviati al AWS Lambda momento del caricamento del file	494
Esempio di funzione Lambda per una fase del flusso di lavoro personalizzata	495
Autorizzazioni IAM per un passaggio personalizzato	496
Politiche IAM per i flussi di lavoro	497
Relazioni di fiducia nel workflow	499
Esempio di ruolo di esecuzione: decrittografia, copia e tag	499
Esempio di ruolo di esecuzione: Esegui la funzione ed elimina	501
Gestione delle eccezioni per un flusso di lavoro	502
Monitora l'esecuzione del workflow	503
CloudWatch registrazione per un flusso di lavoro	503
CloudWatch metriche per i flussi di lavoro	506

Crea un flusso di lavoro da un modello	506
Rimuovere un flusso di lavoro da un server Transfer Family	510
Restrizioni e limiti	511
Gestione dei server	514
Visualizza un elenco di server	514
Eliminare un server	515
Visualizza i dettagli del server SFTP	516
Visualizza i dettagli del server AS2	517
Supporto IPv6	519
Limitazioni IPv6	520
Configurazione di IPv6 per i server	520
Usa ALB per il server pubblico AS2 dual-stack	521
Modifica i dettagli del server	523
Modifica i protocolli di trasferimento dei file	526
Modifica l'endpoint del server	528
Modifica la registrazione	529
Modifica la politica di sicurezza	530
Cambia il flusso di lavoro gestito	532
Cambia i banner di visualizzazione per il tuo server	533
Metti il tuo server online o offline	533
Modifica la configurazione del provider di identità	534
Passaggio a un provider di identità gestito dal servizio	534
Passaggio al AWS Directory Service	535
Passaggio a un provider di identità personalizzato	535
Conservazione degli utenti durante le transizioni tra provider di identità	540
Considerazioni importanti sulla modifica dei provider di identità	540
Gestisci le chiavi dell'host del server	540
Quando importare le chiavi dell'host	541
Aggiungere una chiave host del server aggiuntiva	542
Eliminare una chiave host del server	544
Ruota le chiavi dell'host del server	545
Informazioni aggiuntive sulla chiave dell'host del server	546
Monitora l'utilizzo all'interno della console	547
Gestione dei controlli di accesso	554
Creazione di una policy di accesso ai bucket S3	555
Creazione di una politica di sessione	556

Esempio di politica di sessione	557
Sostituzioni annidate per le politiche di sessione	560
Gestione dinamica delle autorizzazioni	560
Comprendere l'architettura delle autorizzazioni Transfer Family	560
Due approcci alla gestione delle autorizzazioni	561
Implementazione delle politiche di	562
Implementazione per tipo di utente	563
Esempio: semplificazione della gestione dei ruoli con policy di sessione	563
CloudTrail disboscamento	566
Abilitare la registrazione CloudTrail	568
Abilitazione degli eventi relativi ai dati di Amazon S3	568
Esempio di registrazione per la creazione di un server	569
Registri di accesso ai dati	570
Esempio di immissione del registro per un accesso corretto ai dati	570
Operazioni comuni di accesso ai dati	573
CloudWatch registrazione	574
Tipi di CloudWatch registrazione per Transfer Family	574
Creazione della registrazione per i server	577
Creazione della registrazione per i server	579
Aggiornamento della registrazione per un server	580
Visualizzazione della configurazione del server	583
Gestione della registrazione per i flussi di lavoro	585
Configurazione di un ruolo per CloudWatch	588
Visualizzazione dei flussi di log di Transfer Family	590
Creazione di CloudWatch allarmi Amazon	594
Registrazione delle chiamate API S3 nei log di accesso S3	595
Esempi per limitare il problema confuso dei deputati	595
CloudWatch struttura di log per Transfer Family	597
Log strutturati JSON per Transfer Family	597
Log precedenti per Transfer Family	600
Esempi di voci di CloudWatch registro	603
Esempio di voci del registro delle sessioni di trasferimento	604
Esempi di voci di registro per i connettori SFTP	605
Esempi di voci di registro per connettori VPC Lattice	607
Esempi di voci di registro relative agli errori dell'algoritmo di scambio di chiavi	608
Utilizzo delle metriche CloudWatch	609

Dimensioni Transfer Family	614
Notifiche all'utente	614
CloudWatch interrogazioni	615
Gestione degli eventi utilizzando EventBridge	618
Transfer Family eventi	619
Eventi dei server SFTP, FTPS e FTP	619
Eventi del connettore SFTP	622
Eventi AS2	623
Invio di Transfer Family eventi	624
Creazione di modelli di eventi	626
Test dei modelli di Transfer Family eventi per gli eventi	627
Permissions	627
Risorse aggiuntive	627
Riferimento ai dettagli sugli eventi	628
Eventi del server	629
Eventi del connettore	636
Eventi AS2	643
Sicurezza	650
Vantaggi della sicurezza della connettività VPC	651
Modello di sicurezza VPC Lattice	651
Best practice di sicurezza per la connettività VPC	652
Politiche di sicurezza per i server	652
Algoritmi crittografici	654
Dettagli della politica di sicurezza	665
Politiche di sicurezza per i connettori SFTP	683
Algoritmi crittografici	683
Dettagli sulla politica di sicurezza del connettore SFTP	684
Post-Quantum politiche di sicurezza	686
Informazioni sullo scambio di chiavi ibride post-quantistiche in SSH	687
Come utilizzarlo	687
Come eseguire il test	689
Protezione dei dati	692
Crittografia dei dati in Transfer Family	693
Crittografia dei dati a riposo	695
Gestione delle chiavi	696
Panoramica degli algoritmi	696

autenticazione SSH	697
Algoritmi PGP	698
Genera chiavi SSH	699
Ruota le chiavi SSH	705
Genera chiavi PGP	707
Gestire le chiavi PGP	709
Client PGP supportati	713
Gestione dell'identità e degli accessi	715
Destinatari	715
Autenticazione con identità	715
Gestione dell'accesso tramite policy	717
Come AWS Transfer Family funziona con IAM	719
Identity-based esempi di politiche	723
Tag-based esempi di politiche	726
Risoluzione dei problemi di identità e accesso in	729
Chiavi di condizione IAM	732
Convalida della conformità	734
Resilienza	734
Endpoint VPC per API	735
Controllo dell'accesso tramite le policy degli endpoint VPC	736
Creare un endpoint VPC	737
Sicurezza dell'infrastruttura	737
Considerazioni su NLB e NAT	738
Sicurezza dell'infrastruttura di connettività VPC	739
Firewall per applicazioni Web	740
Cross-service prevenzione sostitutiva confusa	741
Ruoli utente Transfer Family	743
Ruoli del flusso di lavoro Transfer Family	745
Ruoli del connettore Transfer Family	746
logging/invoctionRuoli Transfer Family	747
AWS politiche gestite	749
AWSTransferConsoleFullAccess	750
AWSTransferFullAccess	750
AWSTransferLoggingAccess	750
AWSTransferReadOnlyAccess	750
Aggiornamenti delle policy	750

Moduli Transfer Family Terraform	752
server SFTP	752
Connettori SFTP	752
AS2	753
Scambio di dati B2B	753
Risoluzione dei problemi Transfer Family	754
Problemi di autenticazione	754
Errori di autenticazione— SSH/SFTP	755
Problema relativo ai realms non corrispondenti di AD gestito	755
I limiti dei gruppi di Active Directory sono stati superati	756
Problemi di autenticazione vari	756
Risolvi i problemi relativi ad Amazon API Gateway	757
Risolvi i problemi relativi al test del tuo provider di identità	759
Bucket Amazon S3 duplicati nell'app Web	330
Problemi relativi al connettore SFTP	760
Risolvi i problemi relativi all'aggiunta di chiavi host affidabili per il connettore SFTP	760
La negoziazione chiave fallisce	761
Limitazione del connettore SFTP	761
Ottimizzazione delle prestazioni del connettore SFTP	762
Risolvi i problemi di connettività VPC	763
Problemi vari del connettore SFTP	766
Problemi di connettività SFTP	766
Risolvi i problemi di connettività SFTP	767
Risolveti i problemi relativi al client SFTP	767
Risolvi i problemi di caricamento dei file	768
Risolvi i problemi relativi al connettore SFTP di tipo di uscita VPC	769
Problemi relativi ai provider di identità personalizzati	771
Risolvi gli errori di integrazione dell'API Gateway	771
Risoluzione dei problemi relativi ai timeout delle funzioni Lambda	772
Risolvi i problemi di timeout Lambda coerenti	773
Risolvi i problemi relativi alle eccezioni <code>KeyError</code>	774
Problemi del flusso di lavoro	774
Risolvi i problemi relativi ai flussi di lavoro gestiti	774
Risolvi i problemi di decrittografia del flusso di lavoro	777
Problemi con EFS	781
Risolvi i problemi di Amazon EFS	781

Problemi di archiviazione e crittografia	784
Risolvi i problemi relativi alle politiche per i bucket Amazon S3 crittografati	784
Risolvi i problemi relativi all'eccezione ResourceNotFound	784
Problemi di monitoraggio e avviso	785
Risolvi i problemi relativi alle metriche mancanti o incomplete CloudWatch	785
Risolvi i problemi relativi agli eventi mancanti EventBridge	786
Cross-region problemi di trasferimento	787
Risolvi i problemi relativi alle autorizzazioni di trasferimento tra regioni	788
Risolvi i problemi relativi alle prestazioni dei trasferimenti tra regioni	789
Problemi di distribuzione di Terraform	790
Risolvi gli errori di creazione delle risorse Terraform	791
Risolvi i problemi di gestione dello stato di Terraform	792
Problemi di integrazione con WAF	793
Risolvi i problemi del blocco del traffico legittimo da parte di WAF	793
Risolvi i problemi di integrazione WAF con provider di identità personalizzati	794
Service-managed problemi relativi agli utenti	794
Risolvi i problemi relativi agli utenti gestiti dal servizio	795
Problemi con AS2	796
Risolvi i problemi relativi a AS2	796
Problemi relativi ai certificati AS2	796
Problemi di ricezione MDN AS2	797
Problemi di monitoraggio della scadenza dei certificati	797
Riferimento API	799
Cronologia dei documenti	801
.....	dcccxvii

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, FTP e trasferimenti basati su browser Web direttamente da e verso i servizi di archiviazione. AWS È possibile 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 clienti, i partner e i team interni o 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 draft-ietf-secsh-filexfer-02.txt.

- Protocollo di trasferimento file sicuro (FTPS)
- Protocollo di trasferimento file (FTP)
- Dichiarazione di applicabilità 2 (AS2)
- Browser-based trasferimenti

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.
- Subscription-based distribuzione dei dati con i tuoi 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
- Business-to-business Transazioni (B2B)
- Integrazioni con i sistemi di pianificazione delle risorse aziendali (ERP) e di gestione delle relazioni con i clienti (CRM)

Di seguito sono riportati alcuni casi d'uso comuni per l'utilizzo delle app web Transfer Family:

- Accesso semplificato ai dati in Amazon S3 per una gamma più ampia e diversificata di utenti aziendali
- Gestione centralizzata dell'accesso ai dati per la tua forza lavoro
- Visualizzazione di Amazon S3 Access Grants tramite un'interfaccia gestita

Con Transfer Family, puoi accedere a un server abilitato al protocollo di trasferimento file AWS (o a un'interfaccia web di trasferimento file gestito), 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 quanto riguarda i server, è necessario innanzitutto associare il nome host all'endpoint del server, quindi aggiungere gli utenti e fornire 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.

Per le app web Transfer Family, determina le impostazioni di configurazione e applica personalizzazioni opzionali. Dopo aver eseguito questa operazione, gli utenti possono accedere e trasferire direttamente i dati da e verso Amazon S3.

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](#)
- [App web 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 o browser Web:

- Secure File Transfer Protocol (SFTP): versione 3

Il documento ufficiale IETF si trova qui: [SSH File Transfer](#) Protocol draft-ietf-secsh-filexfer-02.txt.

- Protocollo di trasferimento file sicuro (FTPS)
- Protocollo di trasferimento file (FTP)
- Dichiarazione di applicabilità 2 (AS2)
- Browser-based trasferimenti

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 Latency-based routing, 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 e trasferimento dei dati tramite compressing/decompressing Transfer encrypting/decrypting Family. Ciò fornisce una visibilità completa per il monitoraggio e la verificabilità. Per ulteriori dettagli, consultare [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](#): Windows-only un client grafico.
- [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 SFTP/FTPS endpoint 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
Implementa Okta come provider di identità personalizzato per AWS Transfer Family	11 agosto 2025
Automatizzazione dell'elaborazione dei reclami sanitari cartacei in formato elettronico con AWS	29 maggio 2025
Modalità d'uso AWS Transfer Family e per la protezione da malware GuardDuty	30 aprile 2025
In che modo FICO modernizza i trasferimenti di file con l'automazione ETL utilizzando AWS Transfer Family	24 aprile 2025

Titolo e link del post del blog	Data
Annuncio di app AWS Transfer Family Web per trasferimenti di file Amazon S3 completamente gestiti	1 dicembre 2024
Sei suggerimenti per migliorare la sicurezza del tuo server AWS Transfer Family	24 settembre 2024
Semplifica l'autenticazione di Active Directory con un provider di identità personalizzato per AWS Transfer Family	12 agosto 2024
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

Titolo e link del post del blog	Data
Creazione di una piattaforma di trasferimento file nativa per il cloud utilizzando flussi di lavoro AWS Transfer Family	5 gennaio 2022
Abilitazione della gestione delle chiavi self-service degli utenti con AWS Transfer Family e 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 Gestione dei segreti AWS	05 novembre 2020
Centralizza l'accesso ai dati utilizzando AWS Transfer Family e Gateway di archiviazione AWS	22 giugno 2020
Utilizzo di Amazon EFS per AWS Lambda le tue applicazioni serverless	18 giugno 2020

Titolo e link del post del blog	Data
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
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.

Per informazioni sul supporto IPv6 per AWS Transfer Family i server, consulta [Supporto IPv6 per i server Transfer Family](#) il capitolo Gestione dei server.

Argomenti

- [AWS Regioni, endpoint e quote supportati per i server Transfer Family](#)
- [Iscriviti per AWS](#)
- [Configurare lo storage da utilizzare con i server AWS Transfer Family](#)
- [Crea un ruolo e una policy IAM](#)

AWS Regioni, endpoint e quote supportati per i server Transfer Family

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 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

Per le app web Transfer Family, le regioni supportate sono elencate in [Regioni AWS per le app web Transfer Family](#). Per le quote relative alle app web Transfer Family, vedi. [Quote per le app Web](#)

Iscriviti 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. Aprire <https://portal.aws.amazon.com/billing/signup>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

Per informazioni sui prezzi e da utilizzare per Calcolatore dei prezzi AWS 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

Configurare lo storage da utilizzare con i server 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](#)

- [Punti di accesso Amazon S3](#)
- [Comportamento di Amazon S3 HeadObject](#)
 - [Concedi la possibilità di scrivere ed elencare solo file](#)
 - [Un gran numero di oggetti a zero byte che causano problemi di latenza](#)
- [Configurazione di un file system Amazon EFS](#)
 - [Proprietà dei file Amazon EFS](#)
 - [Configurazione degli utenti Amazon EFS per Transfer Family](#)
 - [Configurazione degli utenti Transfer Family su Amazon EFS](#)
 - [Crea un utente root Amazon EFS](#)
- [Comandi Amazon EFS supportati](#)

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, assegna 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 Amazon S3 Multi-Region Access Point.

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. Zero-byte gli oggetti vengono creati per rappresentare il percorso di una cartella quando si crea una directory vuota utilizzando `mkdir` o utilizzando la console Amazon S3. La chiave per questi oggetti termina con una barra in avanti. 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 [HeadObject](#) Simple 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 *amzn-s3-demo-bucket* con il nome del tuo bucket.

 Note

Per risolvere il problema del comportamento di caricamento di WinSCP, assicurati di aggiungere la "arn:aws:s3:::amzn-s3-demo-bucket/*.*filepart" riga elencata nella seguente politica di esempio. Questa riga garantisce la corretta gestione degli oggetti.filepart per evitare errori.

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

```
}
```

Note

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 FTP](#) argomento.

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. Tenere 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 cartella 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 `HeadObject` chiamate. 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.

Tenere 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, assegna 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 Unix-style modalità. Questo valore di modalità definisce le autorizzazioni per l'esecuzione di azioni su quell'oggetto.

Inoltre, sui Unix-style sistemi, gli utenti e i gruppi sono mappati su identificatori numerici, che Amazon EFS utilizza 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 farlo [Crea 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 alle directory UID/GID e specificate. Se UID/GID/directories 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 Family](#) argomento.

Crea un utente root Amazon EFS

Se la tua organizzazione ritiene opportuno abilitare l'accesso come utente root 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).

Tip

Non lasciate che questo account superutente esista più a lungo del necessario. Oppure, se mantieni l'account utente root, assicurati di mantenerlo ben protetto.

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 Auto-generate politica in base alla cartella home. Questa è una scorciatoia utile se desideri limitare l'accesso degli utenti alle proprie cartelle. Inoltre, è possibile visualizzare i dettagli sulle politiche di sessione e un esempio in [Come 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](#)
- [Come funzionano le politiche di sessione](#)
- [Esempio di politica di read/write accesso](#)

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. Questa procedura è descritta in [Per 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 read/write accesso](#).
3. Stabilisci una relazione di fiducia tra AWS Transfer Family e il ruolo IAM. Questa procedura è descritta in [Per stabilire una relazione di trust](#).

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

Per creare una policy IAM per AWS Transfer Family

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, scegli Policy e 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 read/write l'accesso o limitare gli utenti alla loro home directory. Per ulteriori informazioni, consulta [Esempio di politica di read/write accesso](#).

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 pannello 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. 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. Esempio:

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

Note

Negli esempi precedenti, sostituisci ciascuno di essi *user input placeholder* con le tue informazioni.

Per dettagli sul problema del deputato confuso e altri esempi, vedi [Cross-service confusa prevenzione sostitutiva](#).

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.

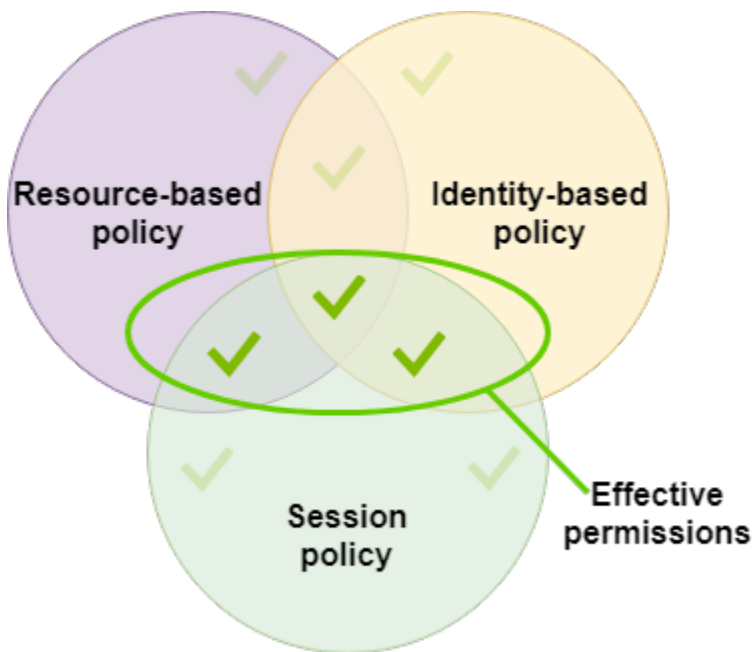
Consulta anche

- 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 [read/write accesso](#), 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. Tenere 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>CreateUserazione 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 [Protezione e crittografia dei dati](#).
- Per utilizzare le policy di sessione per creare autorizzazioni di accesso basate sugli attributi utente senza creare ruoli IAM separati per ogni utente, consulta. [Approcci di gestione dinamica delle autorizzazioni](#)

```
{
  "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 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 [HomeDirectory](#) and [Implementazione 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'accesso dell'utente put e quello dello stesso percorso, `/home/bob/amazon/stuff/`

Esempio di politica di read/write accesso

Concedi read/write l'accesso al bucket Amazon S3

Il seguente esempio di policy per AWS Transfer Family read/write concedere l'accesso agli oggetti nel tuo bucket Amazon S3.

Tenere presente quanto segue:

- Sostituisci `amzn-s3-demo-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:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
```

```

        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
}
]
}

```

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, sostituiscilo *region* con la tua regione, *account-id* 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:us-east-1:123456789012: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:us-east-1:123456789012: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](#)- Crea un server SFTP Transfer Family con un utente gestito dal servizio e trasferisci i file utilizzando un client.
- [Configurazione e utilizzo dei connettori SFTP](#)- Configura un connettore SFTP per trasferire file tra lo storage Amazon S3 e un server SFTP.
- [Configurazione di un metodo Amazon API Gateway come provider di identità personalizzato](#)- Configura un metodo Amazon API Gateway come provider di identità personalizzato per il caricamento di file su un AWS Transfer Family server.
- [Configurazione di un flusso di lavoro gestito per la decrittografia di un file](#)- Crea un flusso di lavoro gestito per decrittografare i file, caricare file crittografati su Amazon S3 e visualizzare i contenuti decrittografati.
- [Configurazione di una configurazione AS2](#)- Configura un server AS2 Transfer Family, inclusa l'importazione di certificati, la creazione di profili e accordi, la configurazione opzionale del connettore AS2 e il test.
- I seguenti tutorial ti guidano nella creazione e configurazione delle applicazioni web Transfer Family. Scegli il tutorial più adatto alle tue esigenze:

[Tutorial: configurazione di un'app web Transfer Family di base](#)- Scopri come creare e configurare un'applicazione web Transfer Family.

[Tutorial: configurazione dell'app AWS Transfer Family Web con accesso selettivo a più bucket](#)- Configura un'applicazione web Transfer Family con autorizzazioni granulari per bucket Amazon S3 per un singolo utente.

Argomenti

- [Guida introduttiva agli endpoint del server AWS Transfer Family](#)
- [Configurazione di un flusso di lavoro gestito per la decrittografia di un file](#)
- [Configurazione e utilizzo dei connettori SFTP](#)
- [Configurazione di un metodo Amazon API Gateway come provider di identità personalizzato](#)
- [Configurazione di una configurazione AS2](#)
- [Tutorial: configurazione di un'app web Transfer Family di base](#)

- [Tutorial: configurazione dell'app AWS Transfer Family Web con accesso selettivo a più bucket](#)

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 SFTP-enabled server con endpoint accessibile pubblicamente utilizzando lo storage Amazon S3, aggiungere un utente con autenticazione gestita dal servizio e trasferire un file con Cyberduck.

Argomenti

- [Prerequisiti](#)
- [Passaggio 1: accedi alla console AWS Transfer Family](#)
- [Fase 2: Creare un SFTP-enabled server](#)
- [Passaggio 3: Aggiungere un utente gestito dal servizio](#)
- [Passaggio 4: Trasferire un file utilizzando un client](#)

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, agli utenti che trasferiscono file da e verso l'esterno AWS tramite Transfer Family, `AmazonS3FullAccess` 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:

- `AWSTransferConsoleFullAccess` concede all'utente SFTP le autorizzazioni per creare risorse Transfer Family.

- IAMFullAccess(o in particolare una politica che consenta la creazione di ruoli IAM) è necessaria 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: CreateVpcEndpoint ed ec2: DeleteVpcEndpoints alla tua policy. Per informazioni sulla limitazione dell'accesso agli endpoint VPC per motivi di sicurezza, consulta. [Limitazione dell'accesso agli endpoint VPC per i server Transfer Family](#)

Note

Le IAMFullAccesspolicy AmazonS3FullAccess, di per sé, non sono necessarie per l'uso generale di AWS Transfer Family. Sono presentati 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.

Passaggio 1: accedi alla console AWS Transfer Family

Per accedere a Transfer Family

1. Accedi a Console di gestione AWS 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 SFTP-enabled server

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 SFTP-enabled server

1. Seleziona Server dal riquadro 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. Scegli Next (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 i server AWS Transfer Family](#)

 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 i dettagli sulla creazione di utenti, consulta [Gestione degli utenti per gli endpoint del server](#).

Passaggio 3: Aggiungere un utente gestito dal servizio

Per aggiungere un utente al SFTP-enabled server

1. Nella pagina Server, seleziona il server a cui desideri 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,, 0—9 A-Z, carattere di sottolineatura '_', trattino '-', punto '.' e nel segno '@'. Il nome utente non può iniziare con un trattino '-', punto '.' o dal segno '@'.
4. Per Access, scegli il ruolo IAM in cui hai creato. [Crea un ruolo e una policy IAM](#) 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, vedere [Genera chiavi SSH per gli utenti che gestiscono il 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, consultare [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 SFTP-enabled server.

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 /amzn-s3-demo-bucket/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 /amzn-s3-demo-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](#)
- [Fase 2: Creare un flusso di lavoro gestito](#)
- [Fase 3: Aggiungere il flusso di lavoro a un server e creare un utente](#)
- [Fase 4: Creare una coppia di key pair PGP](#)
- [Passaggio 5: Memorizza la chiave privata PGP in Gestione dei segreti AWS](#)
- [Fase 6: Crittografare un file](#)
- [Passaggio 7: Esegui il flusso di lavoro e visualizza i risultati](#)

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 in [Politiche 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 in [Per 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 `amzn-s3-demo-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:::amzn-s3-demo-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ],
    },
    {
        "Sid": "DecryptSecret",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/transfer/*"
    }
]
}

```

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 `amzn-s3-demo-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 l'esecuzione di 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 creato [Fase 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 Gestione dei segreti AWS 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, `amzn-s3-demo-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 che gestiscono il 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. Se scegli ECC, puoi scegliere tra BrainPool e Curve25519 per la NIST curva ellittica.

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 Gestione dei segreti AWS.

Passaggio 5: Memorizza la chiave privata PGP in Gestione dei segreti AWS

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 [Gestione dei segreti AWS Pricing](#).

Per memorizzare una chiave privata PGP in Secrets Manager

1. Accedi a Console di gestione AWS e apri la Gestione dei segreti AWS 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 Key/value coppie, scegli la Key/valuescheda.
 - Chiave: **InvioPGPPrivateKey**.
 - valore: incolla il testo della tua chiave privata nel campo del valore.
6. Scegli Aggiungi riga e, nella sezione Key/valuecoppie, scegli la Key/valuescheda.
 - Chiave: **InvioPGPPassphrase**.
 - 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. Scegli Next (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**, assegna 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 Gestione dei segreti AWS 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* sostituisilo 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

Important

Quando crittografate i file per utilizzarli con i AWS Transfer Family flussi di lavoro, assicuratevi sempre di specificare un destinatario non anonimo utilizzando il parametro. -r
La crittografia anonima (senza specificare un destinatario) può causare errori di decrittografia nel flusso di lavoro perché il sistema non sarà in grado di identificare quale chiave utilizzare per la decrittografia. Le informazioni di debug relative a questo problema sono disponibili all'indirizzo. [Risolvi i problemi di crittografia dei destinatari anonimi](#)

Passaggio 7: Esegui il flusso di lavoro e visualizza 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: /amzn-s3-demo-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
```

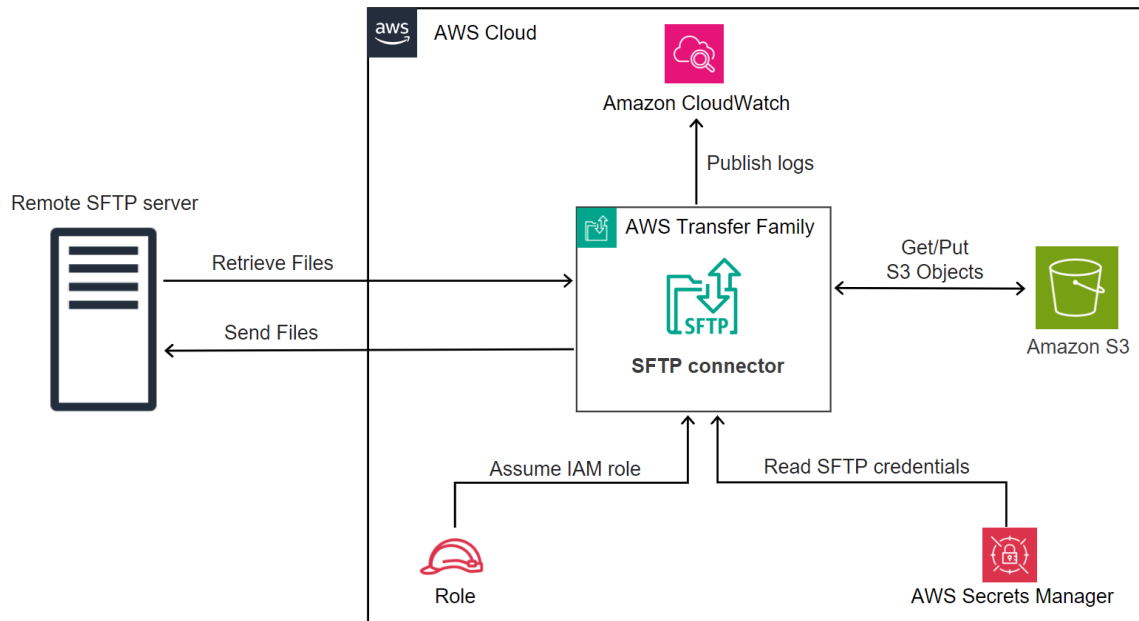
In caso di successo, il `ls` comando elenca il `testfile.txt` file. È possibile scaricare questo file e verificare che sia uguale al file originale crittografato in precedenza.

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 con tipi di uscita gestiti dal servizio e VPC_LATTICE, e quindi trasferire file tra lo storage Amazon S3 e un server SFTP.

Un connettore SFTP recupera le credenziali SFTP da cui autenticarsi in un server SFTP remoto e stabilire una connessione. Gestione dei segreti AWS Il connettore invia o recupera file dal server remoto e li archivia in Amazon S3. Puoi scegliere tra l'uscita gestita dal servizio (utilizzando l'infrastruttura AWS gestita) o l'uscita VPC (routing attraverso il tuo VPC Cross-VPC utilizzando Resource Access). 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.



Il seguente post sul blog fornisce 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

Tipi di uscita del connettore

I connettori SFTP supportano due tipi di uscita che determinano il modo in cui il connettore indirizza il traffico verso i server SFTP remoti:

- **SERVICE_MANAGED** (impostazione predefinita): utilizza l'infrastruttura gestita AWS Transfer Family con indirizzi IP statici per le connessioni in uscita.
- **VPC**: indirizza il traffico attraverso il tuo VPC utilizzando Cross-VPC Resource Access, abilitando la connettività degli endpoint privati e l'uso dei tuoi gateway NAT.

Questo tutorial copre entrambi i tipi di uscita. Scegli il tipo di uscita VPC quando devi:

- Connect a server SFTP privati nel tuo VPC (indirizzi IP privati)
- Connettiti ai server SFTP locali tramite Direct Connect o VPN
- Indirizza il traffico degli endpoint pubblici attraverso il tuo VPC per i controlli di sicurezza
- Usa i tuoi indirizzi IP elastici per le connessioni in uscita

Argomenti

- [Fase 1: Creare le risorse di supporto necessarie](#)
- [Fase 2: Creare e testare un connettore SFTP](#)
- [Passaggio 3: invio e recupero di file utilizzando il connettore SFTP](#)
- [Procedure per creare un server Transfer Family da utilizzare come server SFTP remoto](#)

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 Gestione dei segreti AWS segreto che memorizzi le credenziali utilizzate dal connettore SFTP per accedere al server SFTP remoto.: [Crea e archivia un segreto in Gestione dei segreti AWS](#)

Per i connettori di tipo VPC in uscita, sono inoltre necessari:

- Un VPC con sottoreti e gruppi di sicurezza appropriati

- Un Resource Gateway (sono richieste almeno 2 zone di disponibilità): [Creare un Resource Gateway \(solo tipo di uscita VPC\)](#)
- Una configurazione delle risorse che punta al tuo server SFTP: [Creare una configurazione delle risorse \(solo tipo di uscita VPC\)](#) Per ulteriori informazioni, consulta [Configurazione delle risorse](#) nella Guida per l'utente di Amazon VPC Lattice.

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.

JSON

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

```

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

```

Sostituisci gli elementi come segue:

- Perché `amzn-s3-demo-bucket`, il tutorial utilizza **`sftp-server-storage-east`**.
- Perché *region*, il tutorial utilizza **`us-east-1`**.
- Perché *account-id*, usa il tuo Account AWS ID.
- Perché *SecretName-6RandomCharacters* siamo **using `sftp-connector1`** per il nome (avrà sei caratteri a caso 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, vedi [Utente e ruolo di accesso combinati](#).

Crea e archivia un segreto in Gestione dei segreti AWS

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 [Gestione dei segreti AWS Pricing](#).

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. Accedi a Console di gestione AWS e apri la Gestione dei segreti AWS 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 Key/value coppie, scegli la Key/valuescheda.
 - 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. Scegli Next (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.

Creare un Resource Gateway (solo tipo di uscita VPC)

Per i connettori di tipo VPC in uscita, devi creare un Resource Gateway nel tuo VPC. Il Resource Gateway funge da punto di ingresso per Cross-VPC l'accesso alle risorse.

Per creare un Resource Gateway

1. Esegui il comando seguente per creare un Resource Gateway (sostituisci l'ID VPC e gli ID di sottorete con i tuoi valori):

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

Note

I Resource Gateway richiedono sottoreti in almeno 2 zone di disponibilità.

2. Prendi nota dell'ID Resource Gateway riportato nella risposta per utilizzarlo nel passaggio successivo.

Creare una configurazione delle risorse (solo tipo di uscita VPC)

Create una configurazione delle risorse che punti al vostro server SFTP. Può trattarsi di un indirizzo IP privato per i server nel tuo VPC o di un nome DNS pubblico per server esterni. Per ulteriori informazioni sulle configurazioni delle risorse, consulta le configurazioni [delle risorse](#) nella Amazon VPC Lattice User Guide.

Per creare una configurazione delle risorse

1. Per un server SFTP privato, esegui:

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

2. Per un server SFTP pubblico (solo nome DNS), esegui:

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

Note

Gli endpoint pubblici devono utilizzare nomi DNS, non indirizzi IP.

3. Annotare l'ARN di configurazione delle risorse dalla risposta da utilizzare durante la creazione del connettore.

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, consultare [Creazione di 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 SFTP, quindi scegli Crea connettore SFTP.
3. Per il tipo di uscita, scegli una delle seguenti opzioni:

- Servizio gestito (impostazione predefinita): utilizza l'infrastruttura gestita AWS Transfer Family con indirizzi IP statici per le connessioni in uscita.
- VPC Lattice: indirizza il traffico attraverso il tuo VPC utilizzando Resource Access. Cross-VPC Scegli questa opzione per la connettività privata degli endpoint o per utilizzare i tuoi gateway NAT.

 Important

Non è possibile modificare il tipo di uscita dopo aver creato il connettore. Scegliete con attenzione in base ai vostri requisiti di connettività.

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

- Per l'URL, immettete 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
```

1111aaaa2222bbbb3Sostituiscilo con il tuo ID server Transfer Family.

- Per il ruolo Access, inserisci il ruolo che abbiamo creato in precedenza, **sftp-connector-role**.
- Per l'ARN di configurazione delle risorse (solo il tipo di uscita VPC Lattice), inserisci l'ARN della configurazione della risorsa che hai creato in precedenza:

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

- Per il ruolo Logging, scegliete un ruolo che includa una politica di fiducia nell'elemento Principal. `transfer.amazonaws.com`

Suggerimento: oltre ad aggiungere Transfer Family come entità attendibile, puoi aggiungere la policy `AWSTransferLoggingAccess` AWS gestita al ruolo. Questa politica è descritta in dettaglio in [AWSTransferLoggingAccess](#).

Connector configuration

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

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

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

URL of the remote (target) SFTP server

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

Choose an IAM role

▼

↺

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

Choose a logging role

▼

↺

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 [SftpConnectorConfig](#) sui tipi di dati.
- Per il numero massimo di connessioni simultanee, seleziona un valore intero compreso tra 1 e 5: il valore predefinito è 5.

SFTP configuration [Info](#)**Connector credentials** [Info](#)

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


[Store a new secret](#)
Trusted host keys - optional [Info](#)

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

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

[Remove](#)
[Add trusted host key](#)
Maximum concurrent connections [Info](#)

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

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

Puoi anche creare connettori usando **AWS Command Line Interface**

- Per creare un connettore SFTP con uscita gestita dal servizio, esegui il seguente comando:

```
aws transfer create-connector \
  --url "sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-
rsa AAAAB3NzaC..."
```

- Per creare un connettore SFTP con uscita, esegui il seguente comando VPC-based :

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

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

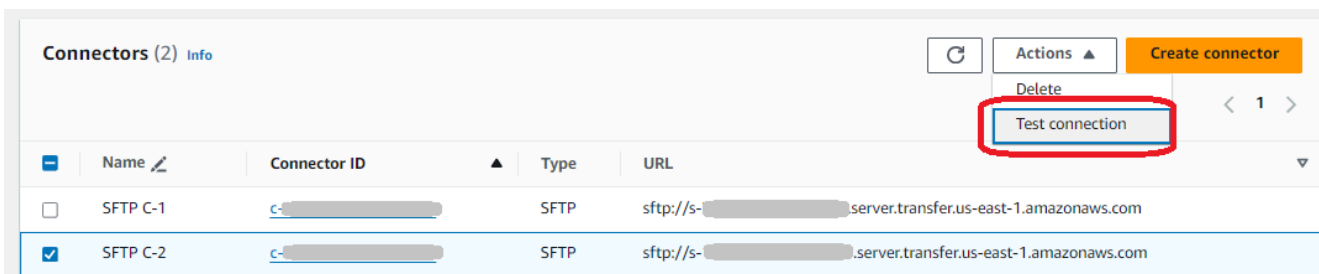
Note

Per i connettori di tipo VPC in uscita, la risoluzione DNS può richiedere alcuni minuti dopo la creazione. Durante questo periodo, lo stato del connettore sarà PENDING e TestConnection restituirà «Connettore non disponibile». Attendi che lo stato diventi ACTIVE prima di tentare il trasferimento di file.

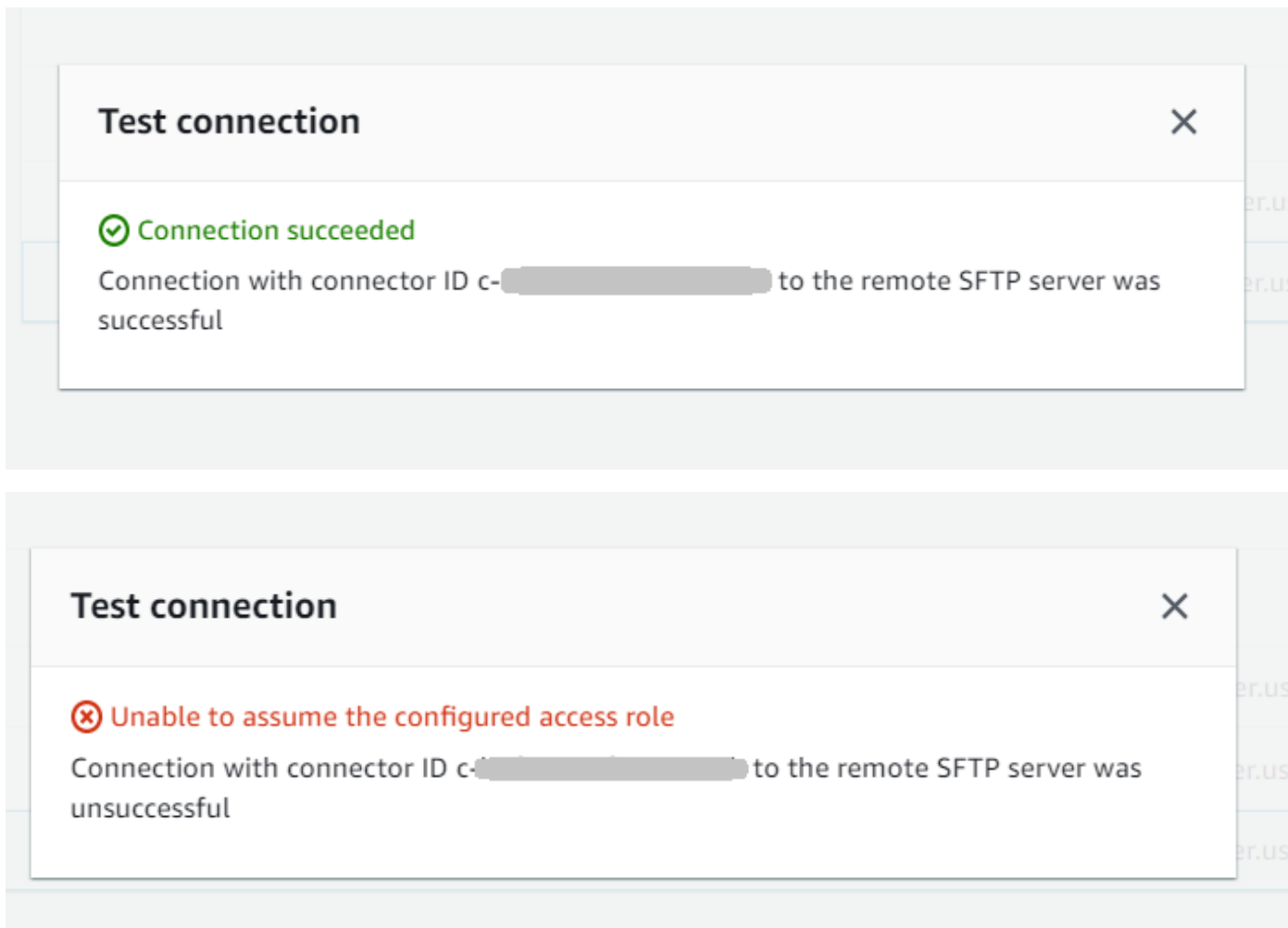
Test a connector using the console

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 SFTP 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 (sostituiscilo *connector-id* con l'ID del connettore effettivo):

```
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"
  }

```

Quando descrivi un connettore di tipo di uscita VPC, la risposta include i nuovi campi:

```

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

```

Tieni presente che `ServiceManagedEgressIpAddresses` è nullo per i connettori di tipo VPC in uscita poiché il traffico viene indirizzato attraverso il tuo VPC anziché attraverso l'infrastruttura gestita. AWS

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 di 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.

- Inviame 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.

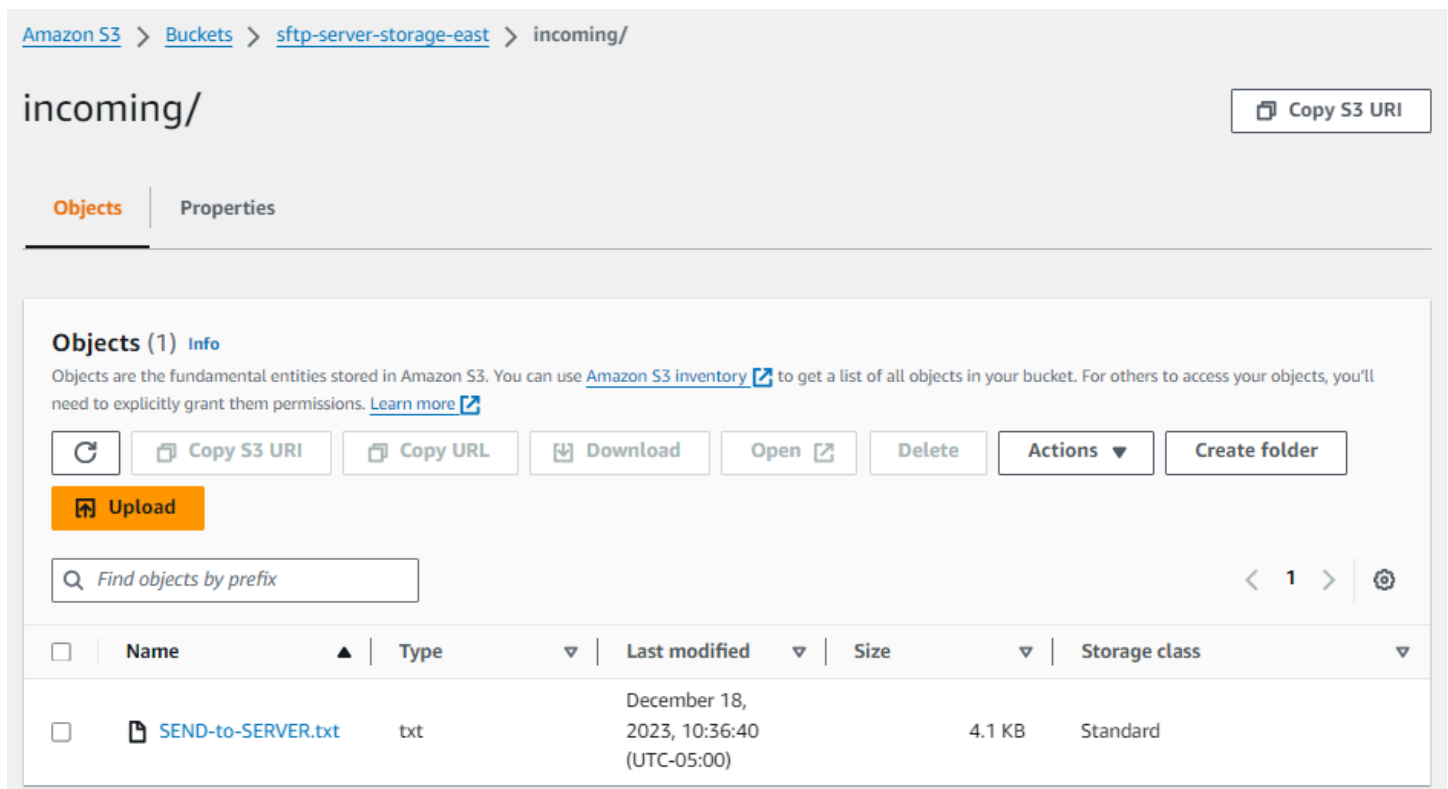
Note

Nei seguenti comandi, sostituiscilo *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 "/sftp-server-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.



The screenshot shows the Amazon S3 console interface. The breadcrumb navigation at the top reads: [Amazon S3](#) > [Buckets](#) > [sftp-server-storage-east](#) > [incoming/](#). The main heading is 'incoming/' with a 'Copy S3 URI' button. Below this are tabs for 'Objects' (selected) and 'Properties'. The 'Objects (1) Info' section contains a descriptive paragraph and a row of action buttons: Refresh, Copy S3 URI, Copy URL, Download, Open, Delete, Actions, and Create folder. An 'Upload' button is also present. A search bar labeled 'Find objects by prefix' is below the buttons. The object list table has columns: Name, Type, Last modified, Size, and Storage class. It contains one entry: 'SEND-to-SERVER.txt' (txt) with a last modified date of 'December 18, 2023, 10:36:40 (UTC-05:00)', a size of '4.1 KB', and a storage class of 'Standard'.

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

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

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 "/sftp-server-
storage-east/incoming"
```

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

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

incoming/ Copy S3 URI

Objects | Properties

Objects (1) Info

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

Refresh
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder

Upload

Find objects by prefix < 1 > ⚙

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

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

Risoluzione dei problemi relativi ai connettori di tipo VPC in uscita

Se riscontri problemi con i connettori di tipo VPC in uscita, controlla quanto segue:

- Lo stato del connettore è IN SOSPESO: la risoluzione DNS per i connettori VPC può richiedere alcuni minuti. Attendi che lo stato diventi ATTIVO prima di tentare la connessione.
- Timeout di connessione: verificate che i gruppi di sicurezza consentano il traffico sulla porta 22 tra le sottoreti Resource Gateway e il server SFTP di destinazione.
- Errori di configurazione delle risorse: assicurati che la configurazione delle risorse punti all'indirizzo IP o al nome DNS corretti e che il Resource Gateway si trovi nello stesso VPC del server SFTP (per endpoint privati). Per ulteriori informazioni, consulta [Configurazione delle risorse](#) nella Guida per l'utente di Amazon VPC Lattice.
- Problemi relativi agli endpoint pubblici: per gli endpoint pubblici, assicurati di utilizzare un nome DNS, non un indirizzo IP, nella configurazione delle risorse. Verifica che il tuo VPC disponga di un gateway NAT per l'accesso a Internet in uscita.
- Disponibilità AZ: i Resource Gateway richiedono sottoreti in almeno 2 zone di disponibilità. Non tutte le AZ supportano VPC Lattice: controlla le AZ supportate nella tua regione.

Considerazioni sui costi per il tipo di uscita VPC:

- VPC Lattice costa \$0.006/GB per l'elaborazione dei dati in qualità di fornitore di risorse (fatturato direttamente da VPC Lattice)
- AWS Transfer Family assorbe i \$0.01/GB costi di consumo delle risorse (primo 1 PB)
- Per gli endpoint pubblici tramite VPC, potrebbero essere applicati costi aggiuntivi per il gateway NAT e il trasferimento dei dati
- Nessun costo aggiuntivo per Transfer Family oltre lo standard di \$0.40/GB commissione per l'elaborazione dei dati

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. Tenere 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 **sftp-server-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 disponi già di 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 SFTP-enabled server](#) 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 `ins-1-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::sftp-server-storage-east"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": [
        "arn:aws:s3::sftp-server-storage-east/*",
        "arn:aws:s3::sftp-server-storage-east/*"
      ]
    }
  ],
}
```

```
{
  "Sid": "GetConnectorSecretValue",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue"
  ],
  "Resource": "arn:aws:secretsmanager:us-east-1:111122223333:secret:aws/
transfer/sftp-connector1-6RandomCharacters"
}
]
```

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](#)
- [Fase 1: Creare uno stack CloudFormation](#)
- [Passaggio 2: verifica la configurazione del metodo API Gateway per il tuo server](#)
- [Fase 3: Visualizzare i dettagli del server Transfer Family](#)
- [Fase 4: Verifica che l'utente sia in grado di connettersi al server](#)
- [Passaggio 5: verifica la connessione SFTP e il trasferimento dei file](#)
- [Passaggio 6: Limita l'accesso al bucket](#)
- [Aggiorna Lambda se usi Amazon EFS](#)

Prerequisiti

Prima di creare le risorse Transfer Family in 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, consulta [Configurazione 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 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 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 modello, scegli Scegli un modello esistente.
4. Copia questo link, [modello di stack Basic](#), e incollalo nel campo URL di Amazon S3.
5. Fare clic su Avanti.
6. Specificate i parametri, incluso un nome per lo stack. Assicuratevi di fare quanto segue:
 - Sostituite i valori predefiniti per Username e 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 UserRoleArn con 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 UserPublicKey1 campo. 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 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](#).

 Non abilitare la memorizzazione nella cache dell'API Gateway

Non abilitate la memorizzazione nella cache per il metodo API Gateway quando lo utilizzate come provider di identità personalizzato per Transfer Family. La memorizzazione nella cache è inappropriata e non valida per le richieste di autenticazione perché:

- Ogni richiesta di autenticazione è unica e richiede una risposta in tempo reale, non una risposta memorizzata nella cache
- La memorizzazione nella cache non offre vantaggi poiché Transfer Family non invia mai richieste duplicate o ripetute all'API Gateway.
- L'attivazione della memorizzazione nella cache farà sì che l'API Gateway risponda con dati non corrispondenti, con conseguenti risposte non valide alle richieste di autenticazione

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

1. Apri la console API Gateway all'indirizzo <https://console.aws.amazon.com/apigateway/>.

2. Scegli l'API del modello di base di Transfer Custom Identity Provider generata dal 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 aver distribuito correttamente il metodo API Gateway, 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 CloudFormation stack, viene creato automaticamente un server Transfer Family.

Per visualizzare i dettagli del server Transfer Family

1. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Scegli lo stack che hai creato.
3. Scegli la scheda Risorse.

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

L'ARN del server viene visualizzato nella colonna ID fisico della TransferServer. 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/> e nella pagina Server scegli il nuovo server.

L'ID del server corrisponde all'ID visualizzato per la TransferServer in 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. 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. 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 CloudFormation stack:

- CreateServer: true
- UserHomeDirectory: /amzn-s3-demo-bucket1
- 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`

UserPublicKey1 È una chiave pubblica che hai generato come parte di una coppia di public/private chiavi.

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

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. Esempio:

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

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

```
sftp> pwd
Remote working directory: /amzn-s3-demo-bucket1
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 CloudFormation stack ed ***lambda-identifier*** è l'identificatore della funzione.

3. Nella scheda Codice, selezionate `index.js` per visualizzare il codice della 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, pari o superiori a 0, che rappresentano 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 AS2-enabled server 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 in [Fase 1: Creare certificati per AS2](#).

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

Questo processo è descritto in [Fase 2: Importazione dei certificati come risorse di certificati Transfer Family](#).

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

Questo processo è descritto in [Fase 3: Crea profili per te e il tuo partner commerciale](#).

4. 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 4: 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.

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

Questo processo è descritto in [Fase 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 in [Passaggio 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:

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

Fase 1: Creare certificati per AS2

Entrambe le parti in uno scambio AS2 necessitano di X.509 certificati. 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, [Portecle](#) è 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=R00TCA" \  
-key root-ca-key.pem \  
-out root-ca.pem
```

L'-subjargomento è composto dai seguenti valori.

	Nome	Description
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	Description
		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'organizzazione 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 AS2-enabled server, 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: 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, consulta [the 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).

Note

Se disponi di un file che contiene sia un certificato che la relativa catena, puoi fornire quel file al `import-certificate` comando utilizzando solo il `certificate` parametro. Esempio:

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

Se utilizzate il `certificate` parametro per caricare sia il certificato che la relativa catena, non utilizzate il `certificate-chain` parametro.

Se si combinano il certificato e la relativa catena, la chiave viene formattata utilizzando gli standard PEM convenzionali, che includono una nuova riga «\n» ogni 64 caratteri. Il certificato archiviato è funzionalmente equivalente a quello che hai caricato, con la sola differenza che la `DescribeCertificate` risposta tramite il AWS CLI conterrà questi caratteri di nuova riga.

```
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 `partnerCertificateId`. 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 `partnerCertificateId`. Nella sezione successiva, questo ID del certificato viene denominato *partner-signing-cert-id*.

Fase 3: 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, consulta [the 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 partner. Nella sezione successiva, questo ID viene denominato *partner-profile-id*.

 Note

Nei comandi precedenti, *MYCORP* sostituisco con il nome della tua organizzazione e *PARTNER-COMPANY* con il nome dell'organizzazione del tuo partner commerciale.

Fase 4: Creare un server Transfer Family che utilizzi il protocollo AS2

Questa procedura spiega come creare un AS2-enabled server 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, consulta [Creare un server AS2 utilizzando la console Transfer Family](#).

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

Quando crei il tuo AS2-enabled server per Transfer Family utilizzando il `create-server` comando, viene creato automaticamente un endpoint VPC per te. 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 AS2-enabled

1. Eseguire il seguente 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-serveroperazione. 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 AS2-enabled server è accessibile, utilizza 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, ti consigliamo vivamente di configurarlo in modo da poter visualizzare lo stato dei tuoi messaggi e risolvere i problemi di configurazione.

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, consulta [the section called “Creare un accordo 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 read/write accesso 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) per archiviare i file AS2. Ti consigliamo di specificare directory separate per diversi tipi di file.
- 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

Ad esempio, salvate il codice seguente in un file `agreementDetails.json`. Sostituisci ogni *user input placeholder* con le tue informazioni.

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

Note

Per utilizzare una singola directory di base anziché directory separate, rimuovete la `CustomDirectories` riga e le relative righe di directory dal codice precedente e utilizzate invece il seguente parametro:

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

Non utilizzate sia una directory di base che parametri di directory separati, altrimenti il comando avrà esito negativo.

Quindi, eseguire il comando riportato di seguito.

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

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, consulta [the 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",
  "PreserveContentType": "FALSE",
  "SigningAlgorithm": "SHA256"
}
```

Note

Infatti `EncryptionAlgorithm`, non specificate `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` e `myfile2.txt`, i file vengono archiviati come `/path-defined-in-the-agreement/processed/original_filename.messageId.original_extension`. Qui, i file vengono archiviati come `/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile1.messageId.txt` e `/amzn-s3-demo-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 "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-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.

Tutorial: configurazione di un'app web Transfer Family di base

Questo tutorial spiega come configurare un'app web Transfer Family. Le app web Transfer Family offrono un'interfaccia semplice per il trasferimento di dati da e verso Amazon S3 tramite un browser Web. Per una documentazione dettagliata su questa funzionalità, consulta [App web Transfer Family](#).

Tutorial sull'app Web: prerequisiti

- Crea un'istanza di account o un'istanza organizzativa di AWS IAM Identity Center. Per informazioni dettagliate, vedi [Configura il tuo provider di identità per le app web Transfer Family](#).

Se non utilizzi IAM Identity Center come provider di identità, [Integra Okta come provider di identità per app web](#) illustra come utilizzare un provider di identità alternativo (in questo caso Okta).

- È necessario un bucket Amazon S3 da utilizzare per interagire con la tua app web Transfer Family. Per maggiori dettagli, consultare [Configurazione di un bucket Amazon S3](#).

Note

Questo tutorial presuppone che tu stia utilizzando la directory IAM Identity Center per il tuo provider di identità. In caso contrario, consulta [Configura il tuo provider di identità per le app web Transfer Family](#) prima di procedere con questo tutorial.

Dopo aver completato il tutorial, l'utente può accedere e interagire con l'app web che hai creato.

Fase 1: Creare le risorse di supporto necessarie

Devi aggiungere un utente alla tua directory IAM Identity Center. Sono inoltre necessari due ruoli: uno da utilizzare come ruolo di portatore di identità per la tua app Web e un secondo da utilizzare per

configurare una concessione di accesso ad Amazon S3. Per il tutorial, consentiamo ai AWS servizi di creare questi ruoli per noi.

Aggiunta di un utente

1. Accedi a Console di gestione AWS e apri la AWS IAM Identity Center console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. Dal riquadro di navigazione a sinistra, scegli Utenti.
3. Scegli Aggiungi utente e specifica i dettagli dell'utente.

Specificate un nome utente, un indirizzo e-mail e altre informazioni richieste. Puoi scegliere di inviare un'e-mail all'utente con le istruzioni per impostare la password oppure generare una password monouso da condividere con lui.

4. Scegli Avanti e, facoltativamente, assegna il nuovo utente a uno o più gruppi.
5. Scegli Avanti e rivedi le tue scelte.

Se tutto sembra corretto, scegli Aggiungi utente per creare il nuovo utente con i dettagli che hai specificato.

Per il tutorial, l'utente di esempio è Bob Stiles, nome utente bobstiles e indirizzo email bobstiles@example.com.

Fase 2: Creare un'app web Transfer Family

Per creare un'app web Transfer Family

1. Accedi a Console di gestione AWS e apri la AWS Transfer Family console all'indirizzo <https://console.aws.amazon.com/transfer/>.
2. Nel riquadro di navigazione a sinistra, scegli App Web.
3. Scegli Crea app web.

Per l'accesso tramite autenticazione, tieni presente che il servizio trova automaticamente l' AWS IAM Identity Center istanza che hai configurato come prerequisito.

4. Nel riquadro Tipo di autorizzazione, seleziona Crea e utilizza un nuovo ruolo di servizio. Il servizio crea per te il ruolo di portatore di identità. Un ruolo di portatore di identità include l'identità di un utente autenticato nelle sue sessioni.

5. Nel riquadro Unità dell'app Web, accetta il valore predefinito di 1 o, se necessario, imposta un valore più alto.
6. Aggiungi un tag per aiutarti a organizzare le tue app Web. Per il tutorial, inserisci il nome per la chiave e l'app web Tutorial per il valore.

 Tip

È possibile modificare il nome dell'app Web direttamente dalla pagina dell'elenco delle app Web dopo averla creata.

7. Scegli Avanti per aprire la pagina dell'app Web Design. In questa schermata, fornisci le seguenti informazioni.

Facoltativamente, puoi fornire un titolo per la tua app web. Puoi anche caricare file di immagini per il tuo logo e la tua favicon.

- Per il titolo della pagina, personalizza il titolo della scheda del browser che gli utenti visualizzano quando si connettono all'app web. Se non inserisci nulla per il titolo della pagina, per impostazione predefinita è Transfer Web App.
- Per il logo, carica un file di immagine. La dimensione massima del file per l'immagine del logo è di 50 KB.
- Per la favicon, carica un file di immagine. La dimensione massima del file per la tua favicon è di 20 KB.

8. Scegli Avanti, quindi scegli Crea app web.

Per offrire un'esperienza personalizzata, puoi fornire agli utenti un URL personalizzato per accedere alla tua app web Transfer Family. Per informazioni dettagliate, vedi [Aggiorna il tuo endpoint di accesso con un URL personalizzato](#).

Passaggio 3: configura la condivisione Cross-origin delle risorse (CORS) per il tuo bucket

Devi configurare la condivisione delle risorse tra le origini (CORS) per tutti i bucket utilizzati dalla tua app web. Una configurazione CORS è un documento che definisce le regole che identificano le origini a cui consentirai l'accesso al tuo bucket. Per ulteriori informazioni su CORS, vedere [Configuring cross-origin resource sharing \(CORS\)](#).

Per configurare la condivisione Cross-origin delle risorse (CORS) per il tuo bucket Amazon S3

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegli Bucket dal pannello di navigazione a sinistra e cerca il tuo bucket nella finestra di dialogo di ricerca, quindi scegli la scheda Autorizzazioni.
3. Nella condivisione Cross-origin delle risorse (CORS), scegli Modifica e incolla il codice seguente. **AccessEndpoint** Sostituiscilo con l'effettivo endpoint di accesso per la tua app web. Assicurati di non inserire barre finali, perché così facendo si generano errori quando gli utenti tentano di accedere alla tua app web.
 - Esempio errato: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Esempio corretto: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`

Se stai riutilizzando un bucket per più app Web, aggiungi i relativi endpoint di accesso alle app Web all'elenco. AllowedOrigins

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

```

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

```

4. Scegliete Salva modifiche per aggiornare il CORS.

Passaggio 4: aggiungi un utente alla tua app web Transfer Family

Aggiungi l'utente che hai creato in precedenza in IAM Identity Center.

Per assegnare utenti a un'app web Transfer Family

1. Vai all'app web che hai creato in precedenza.
2. Seleziona Assegna utenti e gruppi.

The screenshot shows the AWS IAM Identity Center console for a web application named 'webapp-'. At the top, there are buttons for 'Assign users and groups' (highlighted in orange), 'Clear customization', and 'Delete'. Below this is the 'Web app details' section, which includes:

- Access endpoint:** <https://webapp-...transfer-webapp.us-east-2.on.aws>
- Web app endpoint:** <https://webapp-...webapp.us-east-2.on.aws>
- Web app units:** 1
- Identity provider:** AWS IAM Identity Center
- IAM role:** [redacted]
- Instance ARN:** arn:aws:sso:::instance/ssoins-[redacted]

Below the details is a tabbed interface with 'Users' and 'Groups'. The 'Users' tab is active, showing 'Users (2)'. A search bar labeled 'Find resources' is present. Below the search bar is a table with columns: 'Display name', 'User ID', and 'Username'. There are two rows of user data, each with a checkbox on the left and a link icon on the right.

3. Per assegnare l'utente che hai creato in precedenza in IAM Identity Center, seleziona **Assegna utenti e gruppi esistenti** e seleziona **Avanti**.
 - a. Cerca l'utente in base al nome visualizzato. Tieni presente che nessun utente viene visualizzato finché non inizi a inserire i criteri di ricerca. Per aggiungere **Bob Stiles**, inserisci bob nella casella di ricerca. Se non riesci a trovare il tuo utente, accedi alla console di gestione IAM Identity Center, trova l'utente, quindi copia e incolla il nome visualizzato qui.
 - b. Scegli l'**Bob Stiles** utente, quindi scegli **Assegna**.

Fase 5: registrare una sede in Amazon S3 e creare una concessione di accesso

Dopo aver assegnato un utente alla tua app web, devi registrare un bucket e creare una concessione di accesso per quell'utente.

Note

È necessario disporre di un'istanza S3 Access Grants prima di poter procedere. Per i dettagli, consulta [Creare un'istanza S3 Access Grants](#) nella Guida per l'utente di Amazon Simple Storage Service.

Per registrare una sede e creare una concessione di accesso

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegli **Access Grants** dal riquadro di navigazione a sinistra.
3. Scegli **Visualizza dettagli** per visualizzare i dettagli della tua istanza S3 Access Grants.
4. Seleziona la scheda **Sedi**, quindi scegli **Registra posizione**.
5. Inserisci le informazioni che seguono.
 - Per l'ambito, cerca un bucket o inserisci il nome del tuo bucket e, facoltativamente, un prefisso. Nota che l'ambito inizia con la stringa. **s3://**
 - Per il ruolo IAM, scegli **Crea nuovo ruolo per fare** in modo che Amazon S3 crei un ruolo. Questo ruolo consente a S3 Access Grants di accedere all'ambito di localizzazione specificato.

Scegli Registra sede per continuare.

6. Seleziona la scheda Sovvenzioni, quindi scegli Crea sovvenzione e fornisci i seguenti dettagli.

- Per Ubicazione, seleziona Sfoglia sedi e scegli la sede che hai registrato nel passaggio precedente.
- Per Subprefix, inserisci * per indicare che la concessione di accesso si applica all'intero bucket.
- Per Autorizzazioni, seleziona Lettura e scrittura.
- Per il tipo di beneficiario, scegli Directory identity da IAM Identity Center.
- Per il tipo di identità Directory, seleziona Utente.
- In IAM Identity Center user/ ID, copia e incolla l'ID utente per **Bob Stiles**. Questo ID è disponibile nel riquadro Utenti dell'app web Transfer Family.

7. Scegli Crea sovvenzione.

Viene creata la concessione di accesso.

Passaggio 6: accedi alla tua app web Transfer Family come utente

Ora accediamo all'URL dell'app web e accediamo come utente assegnato in precedenza.

Per accedere all'app web Transfer Family

1. Vai alla tua app web
2. Scegli l'endpoint Access dal riquadro dei dettagli dell'app Web.

The screenshot shows the AWS IAM console interface for a web application. At the top, there's a header with the app name 'webapp-' followed by a redacted ID. To the right are buttons: 'Assign users and groups' (orange), 'Clear customization' (blue), and 'Delete' (blue). Below this is a 'Web app details' section with an 'Edit' button. It contains two columns of information. The left column has 'Access endpoint' (with an 'Info' link), 'Web app endpoint', and 'Web app units' (with an 'Info' link). The right column has 'Identity provider', 'IAM role', and 'Instance ARN'. A red rectangle highlights the 'Access endpoint' text and its external link icon. Below the details section are tabs for 'Users' and 'Groups'. The 'Users' tab is active, showing 'Users (1)'. Below this is a search bar and a table of users. A red rectangle highlights the first user, 'Bob Stiles', whose 'Username' is 'bobstiles'.

webapp- [redacted] Assign users and groups Clear customization Delete

Web app details Edit

Access endpoint [Info](#)
Share this with your users and add to your CORS policy.
[https://webapp-\[redacted\].transfer-webapp.us-east-2.on.aws](https://webapp-[redacted].transfer-webapp.us-east-2.on.aws)

Web app endpoint
[https://webapp-\[redacted\].transfer-webapp.us-east-2.on.aws](https://webapp-[redacted].transfer-webapp.us-east-2.on.aws)

Web app units [Info](#)
1

Identity provider
[AWS IAM Identity Center](#)

IAM role
[AWSTransferWebAppIdentityBearer-us-east-2](#)

Instance ARN
arn:aws:sso::instance/ssoins-[redacted]

Users **Groups**

Users (1) ⓘ Delete
After you assign users to your web app, set up user permissions to access your S3 data in [S3 Access Grants](#)

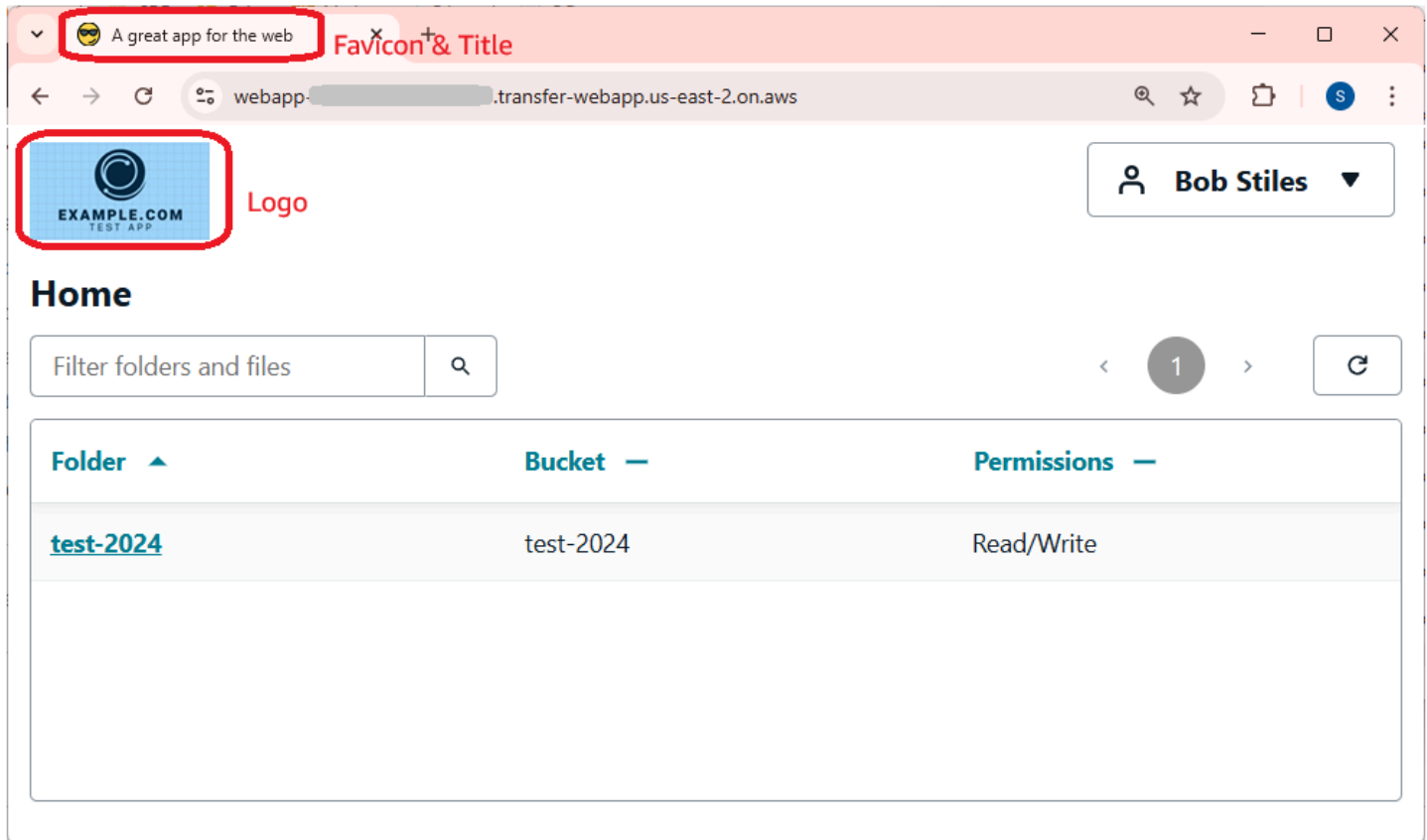
☐ **Display name** ☐ **User ID** ☐ **Username**

☐ [Bob Stiles](#) [\[redacted\]](#) **bobstiles**

3. Nella schermata di accesso, inserisci l'utente che hai creato **bobstiles**, quindi seleziona Avanti.
4. Inserisci la password che il sistema ha assegnato a questo utente al momento della creazione e seleziona Avanti.
5. Se la tua organizzazione richiede l'autenticazione a più fattori (MFA), devi configurarla subito. In caso contrario, vai avanti al passaggio 6.
 - a. Viene visualizzata una schermata per registrare il dispositivo MFA. Scegli una delle opzioni disponibili e seleziona Avanti.
 - b. Esegui i passaggi necessari per configurare l'MFA per questo utente: i passaggi dipendono dall'opzione MFA scelta.

- c. Potrebbe essere necessario impostare una nuova password per l'utente: se necessario, fallo ora. Il sistema potrebbe inoltre richiedere l'accesso nuovamente, utilizzando le nuove credenziali MFA configurate.

L'utente dovrebbe visualizzare una schermata simile alla seguente. Nota che questa schermata include la personalizzazione della favicon e del logo.



Fasi successive

Hai configurato con successo un'app web Transfer Family di base con accesso standard al bucket S3. Se hai bisogno di un controllo più granulare sulle autorizzazioni dei bucket, ad esempio per consentire agli utenti di scaricare da un bucket e caricarli su un altro, consulta. [Tutorial: configurazione dell'app AWS Transfer Family Web con accesso selettivo a più bucket](#)

Integra Okta come provider di identità per app web

Puoi integrare un provider di identità esterno con le app web Transfer Family. Questa sezione descrive come configurare Okta come provider di identità.

1. In Okta, crea un utente, un gruppo e un'applicazione. Per i dettagli su come eseguire questa operazione, consulta [Configurare SAML e SCIM con Okta e IAM Identity Center](#).

AWS IAM Identity Center

Active View Logs Monitor Imports

General Sign On Provisioning Import Assignments **Push Groups**

Push Groups to AWS IAM Identity Center

Push Groups Refresh App Groups Bulk Edit Search...

Pushed Groups	Group in Okta	Group in AWS IAM Identity Center	Last Push	Push Status
All	Examplegroup No description	Examplegroup No description	March 4, 2025 at 3:02:08 PM GMT+9	Active
Errors				
By name				
By rule				

2. Connect Okta e importa utenti e gruppi da Okta a. AWS IAM Identity Center Segui i passaggi da 1 a 4 in [Configurare SAML e SCIM con Okta e IAM Identity Center](#).

IAM Identity Center

Managing Instance
ssols-6684735b83d16df8

Dashboard
Users
Groups
Settings

Multi-account permissions
AWS accounts
Permission sets

Your identity source is currently configured as 'External identity provider'. To add new users or edit their attributes, you must do this using your external identity provider (IdP).

Users (2) Delete users

Users listed here can sign in to the AWS access portal to access AWS accounts and assigned cloud applications. [Learn more](#)

Username Find users < 1 >

	Username	Display name	Status	Created by
☐	Exampleuser	Example User	Enabled	SCIM
☐	johnstiles	John Stiles	Enabled	Manual

IAM Identity Center

Managing instance
ssoins-6684735b83d16df8

Dashboard

Users

Groups

Settings

Multi-account permissions

AWS accounts

Permission sets

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

Groups (2)

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

Find groups by group name

< 1 >

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

3. Verifica che l'origine dell'identità in IAM Identity Center sia SAML 2.0.

Settings

Details

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

Instance name - [Edit](#)

Region
US East (Ohio) | us-east-2

Instance ID
ssoins-

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

Organization ID
AWS Organizations not enabled

Instance ARN
[arn:aws:sso:::instance/ssoins-](#)

Identity source

Authentication

Management

Tags

Identity source

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

Identity source
External identity provider

Authentication method
SAML 2.0

Provisioning method
SCIM

AWS access portal URL
[https://.awsapps.com/start](#)

Identity store ID
d-

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

Actions

Integra Okta come provider di identità per app web

102

4. Assegna il tuo utente e il tuo gruppo, come descritto in. [Passaggio 4: aggiungi un utente alla tua app web Transfer Family](#)
5. Per evitare che gli utenti debbano utilizzare l'MFA quando accedono alla tua app web, esegui i seguenti passaggi in Okta.
 - a. Dalla console di amministrazione Okta, accedi a [Applicazioni] - [Applicazioni] e seleziona l'applicazione. AWS IAM Identity Center
 - b. Nella scheda Accedi, seleziona [Autenticazione utente] - Modifica.
 - c. Seleziona Solo password.

Dopo aver eseguito tutti gli altri passaggi del tutorial, l'utente dovrebbe essere in grado di accedere all'app web Transfer Family accedendo all'endpoint di accesso dell'app Web in un browser Web.

Tutorial: configurazione dell'app AWS Transfer Family Web con accesso selettivo a più bucket

Questo tutorial ti guida nella configurazione di un'app web Transfer Family con autorizzazioni specifiche per i bucket Amazon S3 per un singolo utente. Imparerai come configurare una soluzione che consenta agli utenti di scaricare da un bucket e caricarli su un altro, mantenendo la sicurezza. Questo è un tutorial avanzato che si basa sui concetti trattati nel tutorial di base. Se non conosci le app AWS Transfer Family Web, valuta la possibilità di iniziare con [Tutorial: configurazione di un'app web Transfer Family di base](#).

Prerequisiti

Prima di iniziare questo tutorial, hai bisogno di:

- IAM Identity Center è configurato nella stessa regione della tua app AWS Transfer Family web. Tieni presente che AWS consente una sola istanza di IAM Identity Center per AWS account per tutte le regioni.
- Almeno un utente configurato in IAM Identity Center.
- Due bucket S3: uno per i download e uno per i caricamenti.

 Note

Questo tutorial condivide molti prerequisiti con il tutorial di base sull'app web. Per ulteriori informazioni sulla configurazione di IAM Identity Center e sulla creazione di utenti, consulta [Tutorial: configurazione di un'app web Transfer Family di base](#).

Fase 1: Creare un'app web Transfer Family

Per creare un'app web Transfer Family

1. Accedi Console di gestione AWS e apri la AWS Transfer Family console all'indirizzo <https://console.aws.amazon.com/transfer/>.
2. Nel riquadro di navigazione a sinistra, scegli App Web.
3. Scegli Crea app web.

Per l'accesso tramite autenticazione, tieni presente che il servizio trova automaticamente l' AWS IAM Identity Center istanza che hai configurato come prerequisito.

4. Nel riquadro Tipo di autorizzazione, seleziona Crea e utilizza un nuovo ruolo di servizio. Il servizio crea per te il ruolo di portatore di identità. Un ruolo di portatore di identità include l'identità di un utente autenticato nelle sue sessioni.
5. Nel riquadro Unità dell'app Web, accetta il valore predefinito di 1 o, se necessario, imposta un valore più alto.
6. Aggiungi un tag per aiutarti a organizzare le tue app Web. Per il tutorial, inserisci il nome per la chiave e l'app web Tutorial per il valore.

 Tip

È possibile modificare il nome dell'app Web direttamente dalla pagina dell'elenco delle app Web dopo averla creata.

7. Scegli Avanti per aprire la pagina dell'app Web Design. In questa schermata, fornisci le seguenti informazioni.

Facoltativamente, puoi fornire un titolo per la tua app web. Puoi anche caricare file di immagini per il tuo logo e la tua favicon.

- Per il titolo della pagina, personalizza il titolo della scheda del browser che gli utenti visualizzano quando si connettono all'app web. Se non inserisci nulla per il titolo della pagina, per impostazione predefinita è Transfer Web App.
- Per il logo, carica un file di immagine. La dimensione massima del file per l'immagine del logo è di 50 KB.
- Per la favicon, carica un file di immagine. La dimensione massima del file per la tua favicon è di 20 KB.

8. Scegli Avanti, quindi scegli Crea app web.

Passaggio 2: configura i ruoli IAM per l'accesso a S3

Devi creare due ruoli IAM: uno con accesso solo per il download al primo bucket e un altro con accesso solo per il caricamento al secondo bucket.

Politica di fiducia per entrambi i ruoli

Utilizza la seguente politica di fiducia per entrambi i ruoli IAM:

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

Politica IAM per il bucket di download

Crea un ruolo IAM con la seguente policy per l'accesso in sola lettura al tuo bucket di download:

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

Important

Sostituisci `amzn-s3-demo-bucket1` con il nome effettivo del tuo bucket di download.

Politica IAM per il bucket di caricamento

Crea un altro ruolo IAM con la seguente politica per l'accesso in scrittura al tuo bucket di caricamento:

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

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

Important

Sostituisci amzn-s3-demo-bucket2 con il nome effettivo del tuo bucket di caricamento.

Fase 3: configurare S3 Access Grants

1. Apri la console S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Nel riquadro di navigazione, scegli Access Grants.
3. Fai clic su Crea istanza S3 Access Grants.
4. Seleziona l'opzione Aggiungi istanza IAM Identity Center e inserisci l'ARN dell'istanza del centro di identità.
5. Fai clic su Avanti, quindi su Annulla per completare la creazione dell'istanza S3 Access Grants senza procedere con ulteriori passaggi.

Questo passaggio crea l'istanza S3 Access Grants. Ora registrerai le sedi e creerai concessioni di accesso.

Fase 4: Registrare le posizioni dei bucket S3

Registra entrambi i bucket S3 come sedi con S3 Access Grants:

1. Nella console S3 Access Grants, vai su Posizioni e fai clic su Registra posizione.
2. Nell'ambito della posizione, scegli il bucket S3 specifico per i download (amzn-s3-demo-bucket1).
3. Quando ti viene richiesto di scegliere un ruolo IAM, seleziona il ruolo IAM da scaricare che hai creato in precedenza.
4. Completa il processo di registrazione.
5. Ripeti la procedura per registrare il bucket di caricamento (amzn-s3-demo-bucket2), selezionando il ruolo IAM di caricamento quando richiesto.

Fase 5: Creare concessioni di accesso

Crea due sovvenzioni, una per ogni sede registrata:

1. Nella console S3 Access Grants, vai a Grants e fai clic su Crea sovvenzione.
2. In Posizione, fai clic su Sfoglia posizione e seleziona la posizione del bucket di download (amzn-s3-demo-bucket1).
3. In Subprefix (opzionale), inserisci * per consentire l'accesso all'intero bucket oppure specifica un percorso, ad esempio per limitare l'accesso a un prefisso specifico. `folder1/folder2/*`

Using * imposterà l'ambito della concessione su `s3://bucket-name/*`, che consente l'accesso all'intero bucket. Per consentire l'accesso solo a un prefisso specifico, inserisci un percorso simile a `folder1/folder2/*`, che imposterà l'ambito della concessione su `s3://bucket-name/folder1/folder2/*`

4. In Autorizzazioni e accesso, seleziona Leggi per il bucket di download.
5. Nel tipo di assegnatario, scegli Directory identity da IAM Identity Center.
6. Per il tipo principale IAM, seleziona Utente e inserisci l'ID utente del tuo utente IAM Identity Center.
7. Completa il processo di creazione della sovvenzione.
8. Ripeti la procedura per creare una concessione per il bucket di caricamento (amzn-s3-demo-bucket2), ma seleziona le autorizzazioni. Read-write

Passaggio 6: configura la politica CORS per i bucket S3

Configura una policy CORS per entrambi i bucket S3 per consentire l'accesso tramite: AWS Transfer Family WebApp

1. Apri la console S3 e accedi al tuo bucket di download (amzn-s3-demo-bucket1).
2. Seleziona la scheda Autorizzazioni.
3. Scorri verso il basso fino alla sezione di condivisione Cross-origin delle risorse (CORS) e fai clic su Modifica.
4. Aggiungete la seguente configurazione CORS, sostituendola *WebAppEndpoint* con l'URL effettivo dell' WebApp endpoint:

Puoi trovare l'URL dell'endpoint della tua app Web nella console sotto AWS Transfer Family . WebApps Sarà simile a `https://webapp-*****.transfer-webapp.us-west-2.on.aws`.

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



```
    "access-control-expose-headers"  
  ],  
  "MaxAgeSeconds": 3000  
}  
]
```

5. Fai clic su Salva modifiche.
6. Ripeti la procedura per il tuo bucket di caricamento (amzn-s3-demo-bucket2).

Fase 7: Verifica la configurazione

1. Apri l'URL della tua app AWS Transfer Family web. Puoi trovare questo URL nella AWS Transfer Family console WebApps nel campo Access endpoint.
2. Accedi utilizzando le credenziali utente di IAM Identity Center che hai configurato con le concessioni di accesso.
3. Dopo l'accesso, dovresti vedere entrambe le posizioni S3 nella home page.
4. Vai al bucket di download (amzn-s3-demo-bucket1) e verifica di poter scaricare i file ma non caricarli.
5. Vai al bucket di caricamento (amzn-s3-demo-bucket2) e verifica di poter caricare i file.

Conclusioni

La configurazione è stata completata con successo con l'accesso selettivo al bucket S3 per un singolo utente. AWS Transfer Family WebApp Questa configurazione consente all'utente di scaricare da un bucket e caricarlo su un altro, mantenendo al contempo la sicurezza tramite i ruoli IAM e gli S3 Access Grants.

Questo approccio può essere esteso a più utenti creando sovvenzioni aggiuntive in S3 Access Grants per ogni utente, che consentono un controllo granulare sulle autorizzazioni di accesso ai bucket. Per informazioni sulla configurazione di base dell'app Web, consulta. [Tutorial: configurazione di un'app web Transfer Family di base](#)

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 matrice del tipo di endpoint](#)
- [Configurazione di un endpoint server SFTP, FTPS o FTP](#)
- [Considerazioni su FTP e FTPS Network Load Balancer](#)
- [Trasferimento di file su un endpoint server utilizzando un client](#)
- [Gestione degli utenti per gli endpoint del server](#)
- [Utilizzo di directory logiche per semplificare le strutture di directory Transfer Family](#)
- [Accedi ai file system FSx for NetApp ONTAP con Transfer Family](#)

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	Gateway Amazon API	AWS Lambda
Protocolli supportati	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
Key-based authentication	Sì	No	Sì	Sì
Autenticazione password	No	Sì	Sì	Sì
AWS Identity and Access	Sì	Sì	Sì	Sì

Azione	AWS Transfer Family servizio gestito	AWS Managed Microsoft AD	Gateway Amazon API	AWS Lambda
Management (IAM) e POSIX				
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, vedere [Aggiungi un firewall per applicazioni Web](#).
- C'è un post sul blog che descrive l'uso di una funzione Lambda integrata con Microsoft Entra ID (precedentemente Azure AD) come provider di identità Transfer Family. Per i dettagli, vedere [Autenticazione](#) con Azure Active Directory e. AWS Transfer Family AWS Lambda
- Forniamo diversi 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, puoi creare un SFTP-enabled server, un server, FTPS-enabled un FTP-enabled server o un AS2-enabled server.

Approfondimenti

- [Crea un SFTP-enabled server](#)
- [Creare un FTPS-enabled server](#)
- [Crea un FTP-enabled server](#)
- [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 VPC e VPC-connected ambienti, come un data center locale o una VPN. Direct Connect	Dall'interno di VPC e VPC-connected ambienti, come un data center locale tramite Direct Connect VPN.	Dall'interno di VPC e VPC-connected ambienti, come un data center locale tramite Direct Connect VPN.
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	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)
		indirizzi IP personali (Bring your own IP 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 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 VPC-hosted endpoint, i server SFTP Transfer Family possono funzionare sulla porta 22 (impostazione predefinita), 2222,	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)
	2223 o 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 consentiti o 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.
Tipo di indirizzo IP	IPv4 (impostazione predefinita) o dual-stack (IPv4 e IPv6)	Solo IPv4 (dual-stack non supportato)	IPv4 (impostazione predefinita) o dual-stack (IPv4 e IPv6)	Solo IPv4 (dual-stack non supportato)

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 tipo di endpoint VPC (`EndpointType=VPC`), che puoi usare come interfaccia interna o Internet, come descritto nella tabella precedente.

- Per i dettagli sulla deprecazione, vedere. [Interruzione dell'uso di VPC_ENDPOINT](#)
- Per informazioni sulla gestione delle autorizzazioni degli endpoint VPC, consulta. [Limitazione dell'accesso agli endpoint VPC per i server Transfer Family](#)

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 ad VPC-connected ambienti come un data center locale o una VPN. 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 “Crea un SFTP-enabled server”](#).

 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 FTPS-enabled server”](#).
- File Transfer Protocol (FTP): trasferimento di file non crittografato. Per informazioni dettagliate, vedi [the section called “Crea un FTP-enabled server”](#).
- Dichiarazione di applicabilità 2 (AS2): trasferimento di file per il trasporto di dati strutturati da azienda a azienda. Per informazioni dettagliate, vedi [the section called “Configurare AS2”](#). Per AS2, puoi creare rapidamente uno stack a scopo dimostrativo. CloudFormation 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 di AWS Directory Service per Microsoft Active Directory](#).

- Un provider di identità personalizzato. Transfer Family offre diverse opzioni per l'utilizzo di un provider di identità personalizzato, come descritto nell'[Lavorare con provider di identità personalizzati](#) argomento.

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 Calcolatore dei prezzi AWS ottenere una stima del costo di utilizzo di Transfer Family, consulta [AWS Transfer Family i prezzi](#).

Crea un SFTP-enabled server

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.

Tieni presente quanto segue

- I server SFTP per Transfer Family funzionano sulla porta 22. Per gli VPC-hosted endpoint, i server SFTP Transfer Family possono funzionare anche sulle porte 2222, 2223 o 22000. Per informazioni dettagliate, vedi [Crea un server in un cloud privato virtuale](#).
- Gli endpoint pubblici non possono limitare il traffico tramite gruppi di sicurezza. Per utilizzare i gruppi di sicurezza con il server Transfer Family, è necessario ospitare l'endpoint del server

all'interno di un cloud privato virtuale (VPC) come descritto in. [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 SFTP-enabled

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 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 di AWS Directory Service per Microsoft Active Directory](#)

 Note

- Cross-Account e le directory condivise non sono supportate per AWS Managed Microsoft AD.
- Per configurare un server con Directory Service come provider di identità, è necessario aggiungere alcune 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 tuo 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](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

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

☐ Service managed
Create and manage users within the service

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

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

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

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

AWS Lambda function

Choose a Lambda function ▼

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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

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

Cancel Previous **Next**

4. Scegli Next (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. Per il tipo di indirizzo IP, scegli IPv4 (impostazione predefinita) per la compatibilità con le versioni precedenti o per abilitare sia le connessioni IPv4 che IPv6 Dual-stack all'endpoint.

 Note

Dual-stack la modalità consente all'endpoint Transfer Family di comunicare con client abilitati sia per IPv4 che per IPv6. Ciò consente di passare gradualmente dai sistemi basati su IPv4 a quelli basati su IPv6 senza dover passare da un sistema all'altro in una sola volta.

- c. (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](#)

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

 Note

FIPS-enabled gli endpoint sono disponibili solo nelle regioni del Nord America. AWS Per le regioni disponibili, consulta gli [AWS Transfer Family endpoint e le quote in](#). Riferimenti generali di AWS Per ulteriori informazioni su FIPS, vedere [Federal Information Processing Standard \(FIPS\) 140-2](#).

- e. Scegli Next (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.

Scegli Next (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.

The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains two sections: 'Logging' and 'Logging role'. The 'Logging' section has a heading 'Log group Info' and a description: 'Choose the CloudWatch log group where your events will be delivered in a structured JSON format'. It features two radio buttons: 'Create a new log group' (unselected) and 'Choose an existing log group' (selected). Below these is a text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. The 'Logging role' section has a heading 'Logging role Info' and a description: 'Choose the IAM role that will be used to deliver events to your CloudWatch logs'. It features two radio buttons: 'Create a new role' (unselected) and 'Choose an existing role' (unselected). At the bottom, a blue information box states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Se scegli Crea gruppo di log, la CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) si apre sulla 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, consulta [AWS Transfer Family flussi di lavoro gestiti](#).

Managed workflows [Info](#)

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

W- [redacted] ▼ [Create a new Workflow](#)

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

W- [redacted] ▼ [Create a new Workflow](#)

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

[redacted] ▼

- c. 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 i server AWS Transfer Family](#)
- 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.

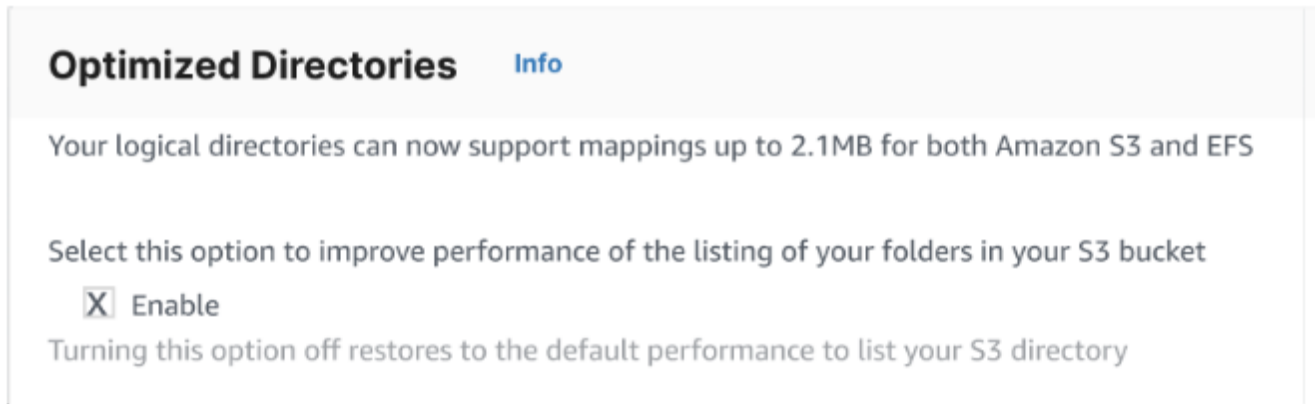
Dopo aver creato il server, puoi aggiungere chiavi host aggiuntive. Avere più chiavi host è utile se si desidera ruotare le chiavi o se si desidera disporre di diversi tipi di chiavi, ad esempio una chiave RSA e anche una chiave ECDSA.

Note

La sezione Server Host Key viene utilizzata solo per la migrazione degli utenti da un server esistente. SFTP-enabled

- e. (Facoltativo) Per Tag, per Chiave e Valore, inserite uno o più tag come coppie chiave-valore, quindi scegliete Aggiungi tag.
- f. Scegli Next (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-authentication Visualizza banner, inserisci il messaggio di testo che desideri mostrare agli utenti prima che si autenticino.
- 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 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.

Additional configuration

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

Select whether you want this server to ignore SetStat command

☐ Enable

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

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

☒ Enforce

☐ Enable

☐ Disable

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

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

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

1.2.3.4

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

8. 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 i dettagli sulla creazione di utenti, consulta [Gestione degli utenti per gli endpoint del server](#).

Creare un FTPS-enabled server

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.

Note

Per importanti considerazioni sui Network Load Balancer, consulta [Evita di posizionare AWS Transfer Family NLB e NAT davanti ai server](#)

Per creare un server FTPS-enabled

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 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 di AWS Directory Service per Microsoft Active Directory](#)

 Note

- Cross-Account e le directory condivise non sono supportate per AWS Managed Microsoft AD.
- Per configurare un server con Directory Service come provider di identità, è necessario aggiungere alcune 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 tuo 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](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory

Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity

Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. Scegli Next (Successivo).
5. In Scegli un endpoint, procedi come segue:

[i](#) 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

FIPS-enabled gli endpoint sono disponibili solo nelle regioni del Nord America. AWS Per le regioni disponibili, consulta gli [AWS Transfer Family endpoint e le quote in](#). Riferimenti generali di AWS Per ulteriori informazioni su FIPS, vedere [Federal Information Processing Standard \(FIPS\)](#) 140-2.

- c. Scegli Next (Successivo).

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

6. 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.

Scegli Next (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).

The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains two sections: 'Logging' and 'Logging role'. The 'Logging' section has a sub-header 'Log group' and a description: 'Choose the CloudWatch log group where your events will be delivered in a structured JSON format'. It offers two options: 'Create a new log group' (unselected) and 'Choose an existing log group' (selected). Below these is a text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. The 'Logging role' section has a sub-header 'Logging role' and a description: 'Choose the IAM role that will be used to deliver events to your CloudWatch logs'. It offers two options: 'Create a new role' (unselected) and 'Choose an existing role' (unselected). At the bottom, a blue information box states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Se scegli Crea gruppo di log, la CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) si apre sulla 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, consulta [AWS Transfer Family flussi di lavoro gestiti](#).

Managed workflows [Info](#)

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

w- [redacted] ▼ [Create a new Workflow](#)

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

w- [redacted] ▼ [Create a new Workflow](#)

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

[redacted] ▼

- c. 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 i server AWS Transfer Family](#)
- 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.

Optimized Directories [Info](#)

Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

- g. Scegli Next (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 del banner di Pre-authentication visualizzazione, inserisci il messaggio di testo che desideri mostrare agli utenti prima che si autenticino e, nella casella di testo del banner di Post-authentication visualizzazione, 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'[ProtocolDetails](#) argomento.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. 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 FTP-enabled server

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' VPC-hosted endpoint. Se è necessario che il server trasmetta i dati alla rete pubblica, è necessario utilizzare protocolli sicuri, come SFTP o FTPS.

Note

Per importanti considerazioni sui Network Load Balancer, consulta. [Evita di posizionare AWS Transfer Family NLB e NAT davanti ai server](#)

Per creare un server FTP-enabled

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 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 di AWS Directory Service per Microsoft Active Directory](#)

Note

- Cross-Account e le directory condivise non sono supportate per AWS Managed Microsoft AD.

- Per configurare un server con Directory Service come provider di identità, è necessario aggiungere alcune 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 tuo 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](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory

Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity

Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. Scegli Next (Successivo).
5. In Scegli un endpoint, procedi come segue:

[i](#) 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

FIPS-enabled gli endpoint non sono supportati per i server FTP.

- c. Scegli Next (Successivo).

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

6. 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.

Scegli Next (Successivo).

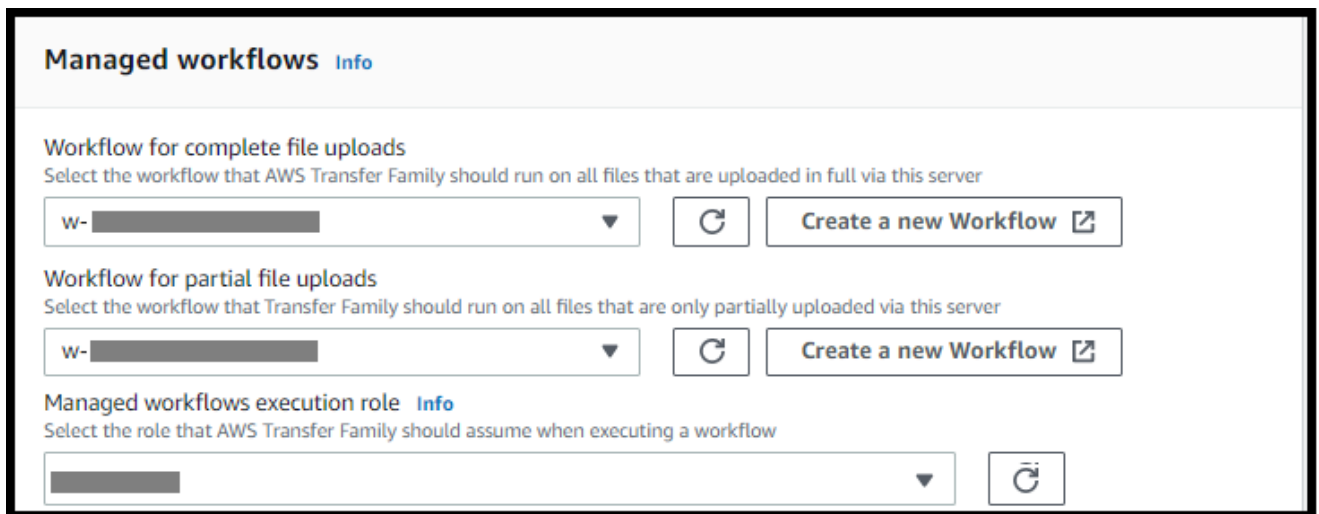
7. In Configura dettagli aggiuntivi, procedi come segue:

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

The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains two sections: 'Logging Info' and 'Logging role Info'. In the 'Logging Info' section, the 'Log group' is configured with the option 'Choose an existing log group' selected. Below this is a text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. The 'Logging role Info' section has two options: 'Create a new role' and 'Choose an existing role', both of which are currently disabled. A blue information box at the bottom states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Se scegli Crea gruppo di log, la CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) si apre sulla 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, consulta [AWS Transfer Family flussi di lavoro gestiti](#).



Managed workflows [Info](#)

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

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

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

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

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

[dropdown] [refresh]

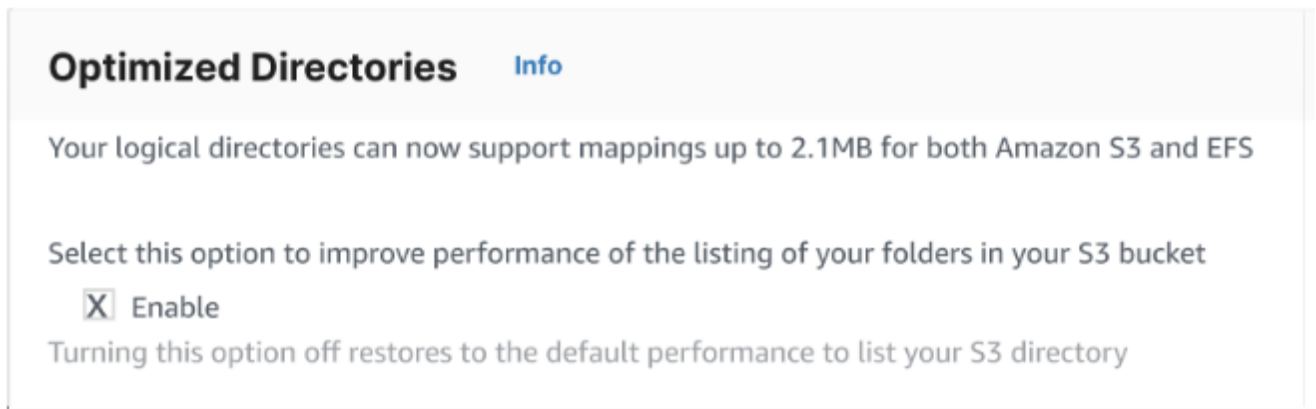
- c. Per le opzioni relative agli algoritmi crittografici, scegli una politica di sicurezza che contenga gli algoritmi crittografici abilitati per l'uso dal tuo server.

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. Scegli Next (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 del banner di Pre-authentication visualizzazione, inserisci il messaggio di testo che desideri mostrare agli utenti prima che si autenticano e, nella casella di testo del banner di Post-authentication visualizzazione, 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'[ProtocolDetails](#) argomento.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. 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_ENDPOINTultimo 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 nel modo seguente:

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 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.

 Note

AWS Transfer Family supporta endpoint dual-stack, permettendo al server di comunicare sia su IPv4 che su IPv6. Per abilitare il supporto dual-stack, seleziona l'opzione Abilita endpoint DNS dual-stack durante la creazione dell'endpoint VPC. Tieni presente che sia il VPC che le sottoreti devono essere configurati per supportare IPv6 prima di poter utilizzare questa funzionalità. Dual-stack il supporto è particolarmente utile quando si hanno client che devono connettersi utilizzando entrambi i protocolli.

Per informazioni sugli endpoint dei server dual-stack (IPv4 e IPv6), vedere. [Supporto IPv6 per i server Transfer Family](#)

Argomenti

- [Crea un endpoint server a cui è possibile accedere solo all'interno del tuo VPC](#)
- [Crea un endpoint con accesso a Internet per il tuo server](#)
- [Cambia il tipo di endpoint per il tuo server](#)
- [Interruzione dell'uso di VPC_ENDPOINT](#)
- [Limitazione dell'accesso agli endpoint VPC per i server Transfer Family](#)
- [Funzionalità di rete aggiuntive](#)
- [Aggiornamento del tipo di endpoint AWS Transfer Family del server da VPC_ENDPOINT a VPC](#)

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 protocolli, seleziona uno o più protocolli, quindi scegli Avanti. Per ulteriori informazioni sui protocolli, consulta [Fase 2: Creare un SFTP-enabled server](#).
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.

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 Interno per rendere l'endpoint accessibile solo ai client che utilizzano gli indirizzi IP privati dell'endpoint.

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.

- Per le regole in entrata per il gruppo di sicurezza, configura il traffico FTP e FTPS in modo che utilizzi Port range **21** per il canale di controllo e per il canale dati. **8192-8200**

 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.

[VPC](#) > [Security Groups](#) > [sg-\[redacted\]-default](#) > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- f. (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

FIPS-enabled gli endpoint sono disponibili solo nelle regioni del Nord America. AWS Per le regioni disponibili, consulta gli [AWS Transfer Family endpoint e le quote in](#). Riferimenti generali di AWS Per ulteriori informazioni su FIPS, vedere [Federal Information Processing Standard \(FIPS\)](#) 140-2.

- g. Scegli Next (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, vedere [Configura 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 all'uso dal tuo server.

 Note

Per impostazione predefinita, la politica `TransferSecurityPolicy-2024-01` 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 i server AWS Transfer Family](#).

- c. (Facoltativo: questa sezione riguarda solo la migrazione degli utenti da un SFTP-enabled server esistente.) 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.
 - d. (Facoltativo) Per Tag, per Chiave e Valore, inserite uno o più tag come coppie chiave-valore, quindi scegliete Aggiungi tag.
 - e. Scegli Next (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 i dettagli sulla creazione di utenti, consulta [Gestione 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. AWS Transfer Family <https://console.aws.amazon.com/transfer/>
2. Dal pannello di navigazione, seleziona Server, quindi scegli Crea server.
3. In Scegli protocolli, seleziona uno o più protocolli, quindi scegli Avanti. Per ulteriori informazioni sui protocolli, consulta [Fase 2: Creare un SFTP-enabled server](#).
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.

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.

Suggerimento: è necessario utilizzare una sottorete pubblica per le zone di disponibilità o configurare prima un gateway Internet se si desidera utilizzare una sottorete privata.

- f. Nella sezione Gruppi di sicurezza, scegli uno o più ID del gruppo di sicurezza esistente oppure 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.
- Per le regole in entrata per il gruppo di sicurezza, configura il traffico FTPS in modo che utilizzi Port range **21** per il canale di controllo e **8192-8200** per il canale dati.

 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.

[VPC](#) > [Security Groups](#) > [sg-\[redacted\]-default](#) > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- g. (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

FIPS-enabled gli endpoint sono disponibili solo nelle regioni del Nord America. AWS Per le regioni disponibili, consulta gli [AWS Transfer Family endpoint e le quote in](#). Riferimenti generali di AWS Per ulteriori informazioni su FIPS, vedere [Federal Information Processing Standard \(FIPS\)](#) 140-2.

h. Scegli Next (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, vedere [Configura 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 all'uso dal tuo server.

Note

Per impostazione predefinita, la politica TransferSecurityPolicy-2024-01 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 i server AWS Transfer Family](#).

- c. (Facoltativo: questa sezione riguarda solo la migrazione degli utenti da un SFTP-enabled server esistente.) 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.
- d. (Facoltativo) Per Tag, per Chiave e Valore, inserite uno o più tag come coppie chiave-valore, quindi scegliete Aggiungi tag.
- e. Scegli Next (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, consulta [AWS Transfer Family flussi di lavoro gestiti](#).

Managed workflows [Info](#)

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

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

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

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

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

[dropdown] [refresh]

7. 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 in base alle tue esigenze.

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. Scegli Save (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 ha interrotto 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 2020VPC. 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, consultare [Prezzi di AWS PrivateLink](#).

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 questo supporto a. FTPS/FTP EndpointType=VPC_ENDPOINT Abbiamo anche rimosso questo tipo di endpoint come opzione dalla AWS Transfer Family console.

Puoi modificare il tipo di endpoint per il tuo server utilizzando la console Transfer Family, l'API AWS CLI, gli SDK o. 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 Supporto AWS 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 Supporto AWS il team del tuo account.

Limitazione dell'accesso agli endpoint VPC per i server Transfer Family

Quando si crea un AWS Transfer Family server con un tipo di endpoint VPC, gli utenti e i responsabili IAM necessitano delle autorizzazioni per creare ed eliminare endpoint VPC. Tuttavia, le politiche di sicurezza della tua organizzazione possono limitare queste autorizzazioni. Puoi utilizzare le policy IAM per consentire la creazione e l'eliminazione di endpoint VPC specificamente per Transfer Family, mantenendo al contempo le restrizioni per altri servizi.

 Important

La seguente policy IAM consente agli utenti di creare ed eliminare endpoint VPC solo per i server Transfer Family, negando queste operazioni per altri servizi:

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateVpcEndpoint",
    "ec2:DeleteVpcEndpoints"
  ],
  "Resource": ["*"],
  "Condition": {
    "ForAnyValue:StringNotLike": {
      "ec2:VpceServiceName": [
        "com.amazonaws.INPUT-YOUR-REGION.transfer.server.*"
      ]
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:role/INPUT-YOUR-ROLE"
      ]
    }
  ]
}
```

```
}  
}
```

Sostituiscila **INPUT-YOUR-REGION** con la tua AWS regione (ad esempio **s-east-1**) e **INPUT-YOUR-ROLE** con il ruolo IAM a cui desideri concedere queste autorizzazioni.

Funzionalità di rete aggiuntive

AWS Transfer Family offre diverse funzionalità di rete avanzate che migliorano la sicurezza e la flessibilità quando si utilizzano configurazioni VPC:

- Supporto per l'ambiente VPC condiviso: puoi ospitare l'endpoint del server Transfer Family in un ambiente VPC condiviso. Per ulteriori informazioni, consulta [Utilizzo di endpoint ospitati da VPC in VPC condivisi con](#). AWS Transfer Family
- Autenticazione e sicurezza: puoi utilizzare un AWS Web Application Firewall per proteggere il tuo endpoint Amazon API Gateway. Per ulteriori informazioni, consulta [Proteggere AWS Transfer Family con AWS Web Application Firewall e Amazon API Gateway](#).

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

Puoi utilizzare Console di gestione 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](#)
- [Aggiornamento del tipo di endpoint del server utilizzando il Console di gestione AWS](#)
- [Aggiornamento del tipo di endpoint del server tramite CloudFormation](#)
- [Aggiornamento del server EndpointType tramite l'API](#)

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

È possibile identificare quali server VPC_ENDPOINT utilizzano il Console di gestione AWS.

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 operazioni delle [ListServers](#) API Amazon EC2 [DescribeRegion](#) e Transfer Family. Se disponi di molti AWS account, puoi eseguire l'autenticazione utilizzando i profili di sessione 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 file VPC.

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

1. Aprire 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 CloudFormation

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

```
AWS::Transfer::FormatVersion: '2010-09-09'
```


Description: 'Create AWS Transfer Server with VPC_ENDPOINT endpoint type'

Parameters:

SecurityGroupId:

Type: AWS::EC2::SecurityGroup::Id

SubnetIds:

Type: List<AWS::EC2::Subnet::Id>

VpcId:

Type: AWS::EC2::VPC::Id

Resources:

TransferServer:

Type: AWS::Transfer::Server

Properties:

Domain: S3

EndpointDetails:

VpcEndpointId: !Ref VPCEndpoint

EndpointType: VPC_ENDPOINT

IdentityProviderType: SERVICE_MANAGED

Protocols:

- SFTP

VPCEndpoint:

Type: AWS::EC2::VPCEndpoint

Properties:

ServiceName: com.amazonaws.us-east-1.transfer.server

SecurityGroupIds:

- !Ref SecurityGroupId

SubnetIds:

- !Select [0, !Ref SubnetIds]

- !Select [1, !Ref SubnetIds]

- !Select [2, !Ref SubnetIds]

VpcEndpointType: Interface

VpcId: !Ref VpcId

Il modello viene aggiornato con le seguenti modifiche:

- EndpointTypeÈ stato modificato inVPC.
- 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 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 CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
- b. Scegli lo stack utilizzato per creare il server Transfer Family.
- c. Scegliere 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:

Change set preview				
Changes (2)				
Search changes				
Action	Logical ID	Physical ID	Resource type	Replacement
	TransferServer	arn:aws:transfer:us-east-1:364810874344:server/s-6a7d04e12d494ec98	AWS::Transfer::Server	Conditional
	VPCEndpoint	vpce-04e685f8702849573 	AWS::EC2::VPCEndpoint	-

- f. Aggiornare lo stack.

3. Una volta completato l'aggiornamento dello stack, accedi alla console di gestione di Transfer Family all'indirizzo <https://console.aws.amazon.com/transfer/>.
4. Riavvia il server. Scegli il server in cui hai eseguito l'aggiornamento 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, vedere [Fase 2: Creare un SFTP-enabled server](#). Per ulteriori informazioni sulla modifica della configurazione di un server esistente, vedere [Modifica 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.

- Per gli endpoint IPv4, il nome host ha il seguente aspetto nella console:

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

- Per gli endpoint dual-stack, il nome host ha il seguente aspetto nella console:

`serverid.transfer-server.region.on.aws`

Note

Se il server dispone di un endpoint VPC, il formato del nome host è diverso da quelli descritti 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. 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"
```

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
```

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 Console di gestione AWS e apri la console Route 53 all'indirizzo <https://console.aws.amazon.com/route53/>.

Considerazioni su FTP e FTPS Network Load Balancer

Sebbene consigliamo di evitare i Network Load Balancer davanti ai AWS Transfer Family server, se l'implementazione FTP o FTPS richiede un NLB o NAT nel percorso di comunicazione del client, segui questi consigli:

- Per un NLB, utilizzate la porta 21 per i controlli sanitari, anziché le porte 8192-8200.
- Per il AWS Transfer Family server, abilita la ripresa della sessione TLS impostando.
`TlsSessionResumptionMode = ENFORCED`

Note

Questa è la modalità consigliata, in quanto offre una maggiore sicurezza:

- Richiede ai client di utilizzare la ripresa della sessione TLS per le connessioni successive.
- Fornisce garanzie di sicurezza più solide garantendo parametri di crittografia coerenti.
- Aiuta a prevenire potenziali attacchi di downgrade.
- Mantiene la conformità agli standard di sicurezza ottimizzando al contempo le prestazioni.

- Se possibile, abbandona l'utilizzo di un NLB per sfruttare appieno i limiti di AWS Transfer Family prestazioni e connessione.

Per ulteriori indicazioni sulle alternative NLB, contatta il team di gestione dei AWS Transfer Family prodotti tramite Support AWS . Per ulteriori informazioni su come migliorare il livello di sicurezza, consulta il post sul blog [Sei suggerimenti per migliorare la sicurezza del](#) tuo server. AWS Transfer Family

Le linee guida sulla sicurezza per gli NLB sono fornite in. [Evita di posizionare AWS Transfer Family NLB e NAT davanti ai server](#)

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 protocollo SCP non è supportato, in quanto considerato non sicuro. È possibile utilizzare il comando `scp` OpenSSH come descritto in [Utilizzo del comando scp](#)
- Il numero massimo di sessioni SFTP simultanee multiplex per connessione è 10.
- Per le connessioni inattive, il valore di timeout è 1800 secondi (30 minuti) per tutti i protocolli (). SFTP/FTP/FTPS Se non vi è alcuna attività dopo questo periodo, il client potrebbe essere disconnesso. Per le connessioni che non rispondono:
 - SFTP ha un timeout di 300 secondi (5 minuti) quando un client non risponde completamente.
 - FTPS e FTP hanno un timeout di non risposta di circa 10 minuti gestito dalla libreria sottostante.
- Amazon S3 e Amazon EFS (a causa del protocollo NFSv4) richiedono che i nomi dei file siano codificati. UTF-8 L'uso 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 Image/Binary la modalità.
- 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					
LABOR	PRODEZZA	LA MAGGIOR PARTE	PASSARE	RETR	STORMO
AUTENTICA ZIONE	LANG	MKD	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_R EAD	SSH_FXP_LINK	SSH_FXP_STAT quando il file richiesto è un collegamento simbolico	SSH_FXP_R EALPATH quando il percorso richiesto

Comandi SFTP non supportati

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, vedi [Genera chiavi SSH per gli utenti che gestiscono il servizio](#).

Argomenti

- [SFTP/FTPS/FTP Comandi disponibili](#)
- [Trova il tuo endpoint Amazon VPC](#)
- [setstat](#) Evita gli errori
- [Usa OpenSSH](#)
- [Usa WinSCP](#)
- [Usa Cyberduck](#)
- [Usa FileZilla](#)
- [Usa un client Perl](#)
- [Usa LFTP](#)
- [Elaborazione successiva al caricamento](#)
- [Messaggi SFTP](#)

SFTP/FTPS/FTP Comandi 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.

SFTP/FTPS/FTP Comandi

Comando	Simple Storage Service (Amazon S3)	Amazon EFS
cd	Supportata	Supportata
chgrp	Non supportata	Supportato (root owner solo)
chmod	Non supportata	Supportato (root solo)
chmtime	Non supportata	Supportata
chown	Non supportata	Supportato (root solo)
get	Supportata	Supportato (inclusa la risoluzione di collegamenti simbolici)
ln -s	Non supportata	Supportato
ls/dir	Supportato	Supportato
mkdir	Supportato	Supportato
put	Supportato	Supportato
pwd	Supportato	Supportata
rename	Supportato solo per i file	Supportata
	 Note La ridenominazione che sovrascriverebbe	 Note La ridenominazione che sovrascriverebbe un file o una directory

Comando	Simple Storage Service (Amazon S3)	Amazon EFS
	un file esistente non è supportata.	esistente non è supportata.
<code>rm</code>	Supportata	Supportata
<code>rmdir</code>	Supportato (solo cartelle vuote)	Supportata
<code>version</code>	Supportato	Supportata

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.

Per trovare il tuo endpoint Amazon VPC

1. Vai alla pagina dei dettagli del tuo server.
2. Nel riquadro dei dettagli dell'endpoint, seleziona il VPC.

Endpoint details

Edit

Status	Online	Custom hostname	-
Endpoint type	VPC (vpce- [redacted] [link icon])	Endpoint	-
VPC	vpc- [redacted]	Access	Info
FIPS Enabled	No	Internal	

3. 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.

VPC > Endpoints > vpce-[redacted]

vpce-[redacted] Actions

Details

Endpoint ID vpce-[redacted]	Status Available	Creation time Monday, April 4, 2022 at 10:51:31 EDT	Endpoint type Interface
VPC ID vpc-515e1d1e4 (no-name-specified)	Status message -	Service name com.amazonaws.us-east-2.transfer.server.c-0002	Private DNS names enabled No
DNS record IP type ipv4	IP address type ipv4	DNS names vpce-[redacted] [redacted].us-east-2-[redacted] -[redacted] [redacted].us-east-	

setstatEvita 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'UpdateServerAPI CreateServer o, utilizza l'ProtocolDetailsopzione 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'SetStatOptionENABLE_NO_OPimpostazione 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

Questa sezione contiene le istruzioni per trasferire file dalla riga di comando utilizzando OpenSSH.

Note

Questo client funziona solo con un SFTP-enabled server.

Argomenti

- [Utilizzo di OpenSSH](#)
- [Utilizzo del comando scp](#)

Utilizzo di OpenSSH

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 /amzn-s3-demo-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.

Utilizzo del comando **scp**

Transfer Family non supporta il protocollo SCP. Tuttavia, puoi usare il comando `scp` OpenSSH se hai bisogno di questa funzionalità.

Il consiglio per usare SCP su SFTP è di usare OpenSSH versione 9.0 o successiva. In OpenSSH versione 9 e successive, `scp` il comando utilizza per impostazione predefinita il protocollo SFTP per i trasferimenti di file anziché il protocollo SCP legacy.

 Important

Assicurati che il tuo server Transfer Family sia configurato per utilizzare l'accesso alle directory ottimizzato per S3.

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 i tuoi file. AWS upload/download 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](#).

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. In Nome utente, inserisci il nome dell'utente che hai creato per il tuo provider di identità specifico.

Suggerimento: 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 di AWS Directory Service per Microsoft Active Directory](#)
 - [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.

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 il trasferimento resume/transfer al nome di file temporaneo per, scegliete Disabilita.

 Important

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.

Suggerimento: se lasci selezionata questa opzione, i caricamenti di file di grandi dimensioni possono fallire in modi imprevedibili. Ad esempio, è possibile creare caricamenti multipartite orfani che prevedono costi per Amazon S3. Può verificarsi anche un danneggiamento silenzioso dei dati.

13. Esegui il trasferimento dei file.

È possibile utilizzare i metodi drag-and-drop 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](#).

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](#).
- Se utilizzi SFTP, inserisci: `sftp://hostname`
 - Se utilizzi FTPS, inserisci: `ftps://hostname`

Assicurati di sostituirlo *hostname* con l'endpoint del server attuale.

Se il tuo server utilizza un endpoint VPC, vedi. [Trova il tuo endpoint Amazon VPC](#)

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` 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.](#)

Usa LFTP

LFTP è un client FTP gratuito che consente agli utenti di eseguire trasferimenti di file tramite l'interfaccia a riga di comando dalla maggior parte delle macchine Linux.

Per i download di file di grandi dimensioni, LFTP presenta un problema noto con i pacchetti non funzionanti, che causa il fallimento del trasferimento dei file.

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'[HeadObject](#) operazione sull'oggetto S3 all'interno della funzione Lambda.

Key	Value
☐ Content-Type	text/plain
☐ x-amz-meta-user-agent	AWSTransfer
☐ x-amz-meta-user-agent-id	sftp_user@s-

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

Messaggi SFTP

Questa sezione descrive i messaggi lato client che è possibile ricevere durante o dopo i trasferimenti di file SFTP quando si utilizza un server Transfer Family. Per ulteriori informazioni su qualsiasi evento SFTP, controllate i log del client SFTP. È possibile utilizzare tali informazioni per risolvere eventuali errori o inoltrare tali informazioni al team di rete per aiutarlo a identificare il problema.

Messaggi SFTP lato client

Attività	Description
AUTH_FAILURE	L'utente non è riuscito a eseguire l'autenticazione. Può trattarsi di qualsiasi tipo di errore causato da un provider di identità personalizzato o da un utente gestito dal servizio. I dettagli dell'evento aiutano a chiarire la causa principale dell'errore.
CLOSE	Indica che un file o una directory aperti sono stati chiusi correttamente.
CONNECTED/DISCONNECTED	Indica il normale successo della connessione e le disconnessioni.
CREATE_SYMLINK	È stato creato un collegamento simbolico (con successo o meno).
DELETE	Un file è stato eliminato (con successo o meno).
ERRORE	Un errore generale e imprevisto. La descrizione associata contiene informazioni che possono aiutare l'utente o gli amministratori di rete a identificare il problema specifico.
EXIT_REASON	Emesso quando un errore imprevisto ha causato l'interruzione della sessione SFTP. Il messaggio associato all'evento descrive la causa.
MKDIR	È stata creata una cartella (con successo o meno).
APERTO	Un file è stato aperto per la lettura o la scrittura (con successo o senza successo)

Attività	Description
CHIUSURA_PARZIALE	Il client si è disconnesso dal server mentre un file era ancora aperto senza ricevere alcun messaggio CLOSE. Transfer Family archivia la parte ricevuta del file (che potrebbe in effetti essere il file completo) ed emette l'evento PARTIAL_CLOSE per avvisare il cliente del problema. L'integrazione dei flussi di lavoro riceve anche un <code>onPartialClose</code> evento per gestire il file in modo appropriato.
RENAME	Un file è stato rinominato (con successo o meno)
RMDIR	Una directory è stata eliminata (con successo o meno)
SETSTAT	Gli attributi di un file vengono modificati (con successo o meno).
	 Note Transfer Family non supporta SETSTAT se utilizzi Amazon S3 per lo storage. La setstat Evita gli errori sezione fornisce dettagli su come evitare SetStat errori disattivando l'impostazione. In questo modo si evita di ricevere un <code>messaggiofail unsupported error</code> : invece, si riceve un <code>success but do nothing</code> messaggio.
TLS_RESUME_FAILURE	Il server è configurato per imporre la ripresa della sessione TLS e il client non la supporta.

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.

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. 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.

Note

Per la distribuzione e la gestione automatizzate degli utenti con più chiavi SSH, vedere.

[Moduli Transfer Family Terraform](#)

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 Family impedisce 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
- Entrambe le chiavi di supporto public/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`

AWS Transfer Family supporta la specificazione di un `HomeDirectory` valore quando si utilizza `HomeDirectoryType LOGICAL`. Ciò si applica agli utenti di `Service Managed`, all'accesso ad `Active Directory` e alle implementazioni di `Custom Identity Provider`, laddove `HomeDirectoryDetails` siano forniti nella risposta.

Important

Quando si specifica un `HomeDirectory` con `LOGICAL HomeDirectoryType`, il valore deve essere mappato a una delle mappature delle directory logiche. Il servizio lo convalida sia durante la creazione degli utenti che durante gli aggiornamenti per evitare configurazioni che non funzionerebbero.

Comportamento predefinito

Per impostazione predefinita, se non viene specificato, `HomeDirectory` è impostato su `«/»` per la modalità `LOGICAL`. Questo comportamento rimane invariato e rimane compatibile con le definizioni utente esistenti.

- Assicurati di associare il tuo nome HomeDirectory a un Entry e non a un Target. Per ulteriori dettagli, consultare [Regole per l'utilizzo delle directory logiche](#).
- Per i dettagli su come è strutturata una directory virtuale, vedi [Struttura delle directory virtuali](#).

Considerazioni relative a Custom Identity Provider

Quando si utilizza un provider di identità personalizzato, ora è possibile specificare un HomeDirectory nella risposta mentre si utilizza HomeDirectoryType LOGICAL. La chiamata TestIdentityProvider API produrrà risultati corretti quando l>IDP personalizzato specifica un HomeDirectory in modalità LOGICAL.

Esempio di risposta IDP personalizzata con HomeDirectory e LOGICAL: HomeDirectoryType

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-user-role",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectory": "/marketing",
  "HomeDirectoryDetails": "[{\"Entry\":\"\\\\\"/\"\", \"Target\":\"\\\\\"/bucket/home\\\\\"\"}, {\"Entry\":\"\\\\\"/marketing\\\\\", \"Target\":\"\\\\\"/marketing-bucket/campaigns\\\\\"\"}]"]
}
```

Quote di gruppo Active Directory

AWS Transfer Family ha un limite predefinito di 100 gruppi di Active Directory per server. Se il tuo caso d'uso richiede più di 100 gruppi, prendi in considerazione l'utilizzo di una soluzione di provider di identità personalizzata, come descritto in [Semplificare l'autenticazione di Active Directory con un provider di identità personalizzato per AWS Transfer Family](#).

Questo limite si applica ai server che utilizzano i seguenti provider di identità:

- AWS Directory Service per Microsoft Active Directory
- AWS Servizio di Directory per i servizi di dominio Entra ID

Se devi richiedere un aumento del limite di servizio, consulta le [Servizio AWS quote](#) nel Riferimenti generali di AWS. Se il tuo caso d'uso richiede più di 100 gruppi, prendi in considerazione l'utilizzo di una soluzione di provider di identità personalizzata, come descritto in [Semplificare l'autenticazione di Active Directory con un provider di identità personalizzato per AWS Transfer Family](#).

Per informazioni sulla risoluzione dei problemi relative ai limiti dei gruppi di Active Directory, consulta [limiti dei gruppi di Active Directory sono stati superati](#).

Argomenti

- [Lavorare con utenti gestiti dal servizio](#)
- [Lavorare con provider di identità personalizzati](#)
- [Utilizzo di AWS Directory Service per Microsoft Active Directory](#)
- [Utilizzo di AWS Directory Service per Entra ID Domain Services](#)

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](#).

Se utilizzi un tipo di identità gestita dal servizio, aggiungi utenti al tuo server abilitato al protocollo di trasferimento file. In tal caso, ogni nome utente deve essere univoco sul server.

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, 0—9 A-Z, carattere di sottolineatura '_', trattino '-', punto '.' e nel segno '@'. Il nome utente non può iniziare con un trattino '-', punto '.' o dal 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 anche una relazione di fiducia con il AWS Transfer Family servizio, definita 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.

- Auto-generate politica basata sulla cartella home: genera una politica di sessione per te. Scegli Visualizza per vedere un oggetto JSON contenente i dettagli della politica.

 Note

Se scegli la Auto-generate politica in base alla cartella home, non selezionare Restricted per questo utente.

Per ulteriori informazioni sui criteri di sessione, consulta [Crea un ruolo e una policy IAM](#), [Creazione di una politica di sessione per un bucket Amazon S3](#), o [Approcci di gestione dinamica delle autorizzazioni](#).

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 è necessario applicare ulteriori controlli, utilizzare una politica di sessione.

Se si seleziona Limitato per questo utente, non è possibile selezionare la Auto-generate politica in base alla cartella home, poiché la cartella home 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 che gestiscono il 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 con [Trasferimento 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, vedere [Configurazione 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,, 0—9 A-Z, 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 e read/write autorizzazioni di montaggio. 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 Family supporto 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 trasferire AWS 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 che gestiscono il 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, ***USER-HOME-DIRECTORY*** dov'è la directory principale dell'utente SFTP:

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

In questo caso, dovrete 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 con [Trasferimento 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 riquadro 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 riquadro 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.

Edit configuration

User configuration

Access [Info](#)
User's IAM role for Amazon S3 access

Admin ▼ ↻

Policy [Info](#)
Scope down policy to apply to the user

☒ None
☐ Existing policy
☐ Select a policy from IAM

View

Home directory
User's login directory

Choose an S3 bucket ▼

Enter optional folder

☐ Restricted [Info](#)

Cancel Save

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 anche una relazione di fiducia con il AWS Transfer Family servizio, definita 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, consulta [Crea un ruolo e una policy IAM](#). Per ulteriori informazioni sulla creazione di una politica di sessione, consulta [Creazione 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. Scegli Salva per salvare le modifiche.

Come eliminare un utente

1. Apri la AWS Transfer Family console all'indirizzo <https://console.aws.amazon.com/transfer/>.
2. Seleziona Server dal riquadro 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 Secure Shell (SSH) File Transfer Protocol (SFTP). Per informazioni su come generare una coppia di chiavi SSH, vedere [Genera chiavi SSH per gli utenti che gestiscono il 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, vedere [Genera chiavi SSH per gli utenti che gestiscono il 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.

Lavorare con provider di identità personalizzati

AWS Transfer Family offre diverse opzioni ai provider di identità personalizzati per autenticare e autorizzare gli utenti a trasferimenti sicuri di file. Ecco gli approcci principali:

- [Soluzione personalizzata per provider di identità](#)—Questo argomento descrive la soluzione di provider di identità personalizzato Transfer Family, utilizzando un toolkit ospitato in GitHub

Note

Per la maggior parte dei casi d'uso, questa è l'opzione consigliata. In particolare, se è necessario supportare più di 100 gruppi Active Directory, la soluzione di provider di identità personalizzata offre un'alternativa scalabile senza limitazioni di gruppo. Questa soluzione è descritta nel post del blog, [Simplify Active Directory authentication with a custom identity provider for AWS Transfer Family](#).

- [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 Amazon API Gateway.

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](#).

- [Approcci di gestione dinamica delle autorizzazioni](#)—Questo argomento descrive gli approcci per la gestione dinamica delle autorizzazioni degli utenti utilizzando le policy di sessione.

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 tuo 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.

- 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 SFTP/FTPS endpoint 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](#).

Note

Per i provider di identità personalizzati, il nome utente deve contenere da un minimo di 3 a un massimo di 100 caratteri. È possibile utilizzare i seguenti caratteri nel nome utente: a—z,, 0—9 A-Z, carattere di sottolineatura '_', trattino '-', punto '.' e nel segno '@'. Il nome utente non può iniziare con un trattino '-', punto '.' o dal segno '@'.

Quando implementi un provider di identità personalizzato, prendi in considerazione le seguenti best practice:

- Implementa la soluzione nella stessa Account AWS area geografica dei tuoi server Transfer Family.
- Implementa il principio del privilegio minimo durante la configurazione dei ruoli e delle policy IAM.
- Utilizza funzionalità come l'elenco degli indirizzi IP consentiti e la registrazione standardizzata per una maggiore sicurezza.
- Testa a fondo il tuo provider di identità personalizzato in un ambiente non di produzione prima della distribuzione.

Argomenti

- [Soluzione personalizzata per provider di identità](#)
- [Utilizzo AWS Lambda per integrare il tuo provider di identità](#)
- [Utilizzo di Amazon API Gateway per integrare il tuo provider di identità](#)
- [Utilizzo di più metodi di autenticazione](#)
- [Supporto IPv6 per provider di identità personalizzati](#)

Soluzione personalizzata per provider di identità

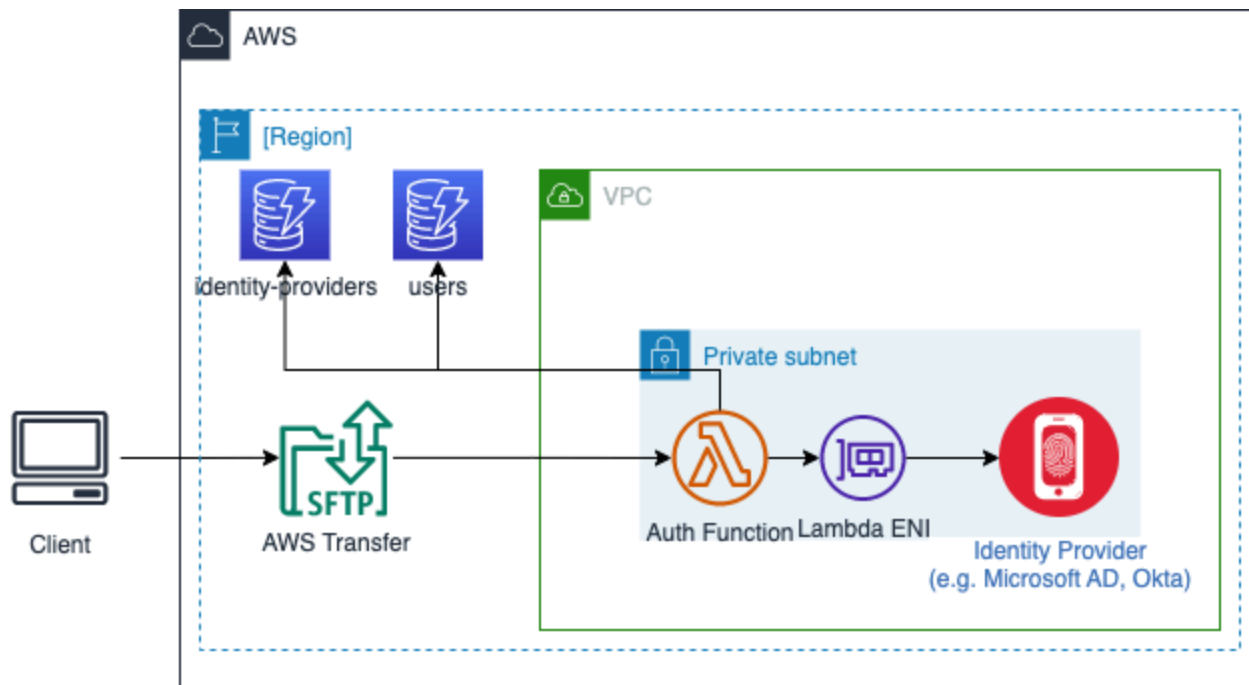
La soluzione per provider di identità AWS Transfer Family personalizzati è una soluzione modulare per provider di identità personalizzati che risolve molti casi d'uso comuni di autenticazione e autorizzazione delle aziende durante l'implementazione del servizio. Questa soluzione fornisce una base riutilizzabile per l'implementazione di provider di identità personalizzati con configurazione granulare delle sessioni per utente e separa la logica di autenticazione e autorizzazione, offrendo una base flessibile e di facile manutenzione per vari casi d'uso.

Con la soluzione AWS Transfer Family personalizzata per provider di identità, è possibile risolvere i casi d'uso comuni di autenticazione e autorizzazione aziendali. Questa soluzione modulare offre:

- Una base riutilizzabile per l'implementazione di provider di identità personalizzati
- Configurazione granulare della sessione per utente
- Logica di autenticazione e autorizzazione separate

Dettagli di implementazione per il toolkit di identità personalizzato

La soluzione fornisce una base flessibile e gestibile per vari casi d'uso. Per iniziare, consulta il toolkit all'indirizzo <https://github.com/aws-samples/toolkit-for-aws-transfer-family>, quindi segui le istruzioni di distribuzione nella sezione [Guida introduttiva](#).



Note

Se in precedenza hai utilizzato modelli ed esempi di provider di identità personalizzati, prendi in considerazione l'adozione di questa soluzione. In futuro, i moduli specifici del provider si standardizzeranno su questa soluzione. La manutenzione continua e i miglioramenti delle funzionalità verranno applicati a questa soluzione.

Questa soluzione contiene modelli standard per l'implementazione di un provider personalizzato che tenga conto dei dettagli, inclusa la registrazione, e della posizione in cui archiviare i metadati di sessione aggiuntivi necessari AWS Transfer Family, come il parametro `HomeDirectoryDetails`. Questa soluzione fornisce una base riutilizzabile per l'implementazione di provider di identità personalizzati con una configurazione granulare della sessione per utente e disaccoppia la logica di autenticazione del provider di identità dalla logica riutilizzabile che crea una configurazione che viene restituita a Transfer Family per completare l'autenticazione e stabilire le impostazioni per la sessione.

Il codice e le risorse di supporto per questa soluzione sono disponibili all'indirizzo. <https://github.com/aws-samples/toolkit-for-aws-transfer-family>

Il toolkit contiene le seguenti funzionalità:

- Un [AWS Serverless Application Model](#) modello che fornisce le risorse necessarie. Facoltativamente, distribuisce e configura Amazon API Gateway da incorporare AWS WAF, come descritto nel post del blog [Securing AWS Transfer Family with AWS Web Application Firewall and Amazon API Gateway](#).
- Uno schema [Amazon DynamoDB](#) per archiviare i metadati di configurazione sui provider di identità, incluse le impostazioni delle sessioni utente come `HomeDirectoryDetails`, e. `Role Policy`
- Un approccio modulare che consente di aggiungere nuovi provider di identità alla soluzione in futuro, sotto forma di moduli.
- Recupero degli attributi: recupera facoltativamente gli attributi del ruolo IAM e del profilo POSIX (UID e GID) dai provider di identità supportati, tra cui AD, LDAP e Okta.
- Supporto per più provider di identità connessi a un singolo server Transfer Family e a più server Transfer Family utilizzando la stessa implementazione della soluzione.
- Built-in Controllo degli elenchi di indirizzi IP consentiti, ad esempio gli elenchi di indirizzi IP consentiti che possono essere configurati facoltativamente per utente o per provider di identità.
- Registrazione dettagliata con supporto configurabile a livello di registro e tracciamento per facilitare la risoluzione dei problemi.

Prima di iniziare a implementare la soluzione personalizzata per un provider di identità, è necessario disporre delle seguenti risorse. AWS

- Un Amazon Virtual Private Cloud (VPC) con sottoreti private, con connettività Internet tramite un gateway NAT o un endpoint gateway DynamoDB.
- Autorizzazioni IAM appropriate per eseguire le seguenti attività:
 - Implementa il modello, `custom-idp.yaml` CloudFormation
 - Crea progetti AWS CodePipeline
 - Crea AWS CodeBuild progetti
 - Crea ruoli e politiche IAM

⚠ Important

È necessario distribuire la soluzione sullo stesso Account AWS server Transfer Family Regione AWS che contiene i server Transfer Family di destinazione.

Provider di identità supportati

L'elenco seguente contiene i dettagli dei provider di identità supportati per la soluzione di provider di identità personalizzata.

Provider	Flussi di password	Flussi a chiave pubblica	Multi-factor	Recupero degli attributi	Informazioni
Active Directory e LDAP	Sì	Sì	No	Sì	La verifica degli utenti può essere eseguita come parte del flusso di autenticazione a chiave pubblica.
Argon2 (hash locale)	Sì	No	No	No	Gli hash Argon2 vengono memorizzati nel record utente per i casi d'uso di autenticazione «locale»

Provider	Flussi di password	Flussi a chiave pubblica	Multi-factor	Recupero degli attributi	Informazioni
					basata su password.
Amazon Cognito	Sì	No	Sì*	No	Time-based One-Time Solo autenticazione a più fattori basata su password (TOTP). * L'SMS-based MFA non è supportata.
Inserisci ID (in precedenza Azure AD)	Sì	No	No	No	
Okta	Sì	Sì	Sì*	Sì	TOTP-based Solo MFA.
Chiavi pubbliche	No	Sì	No	No	Le chiavi pubbliche sono archiviate nel record utente in DynamoDB.
Secrets Manager	Sì	Sì	No	No	

Utilizzo AWS Lambda per integrare il tuo provider di identità

Questo argomento descrive come creare una AWS Lambda funzione che si connetta al 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.

Nella maggior parte dei casi d'uso, il modo consigliato per configurare un provider di identità personalizzato consiste nell'utilizzare il [Soluzione personalizzata per provider di identità](#).

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.

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

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

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

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

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

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

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

AWS Lambda function



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

☒ **Password OR public key**

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

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

Cancel Previous Next

Note

La scelta dei metodi di autenticazione è disponibile solo se abiliti SFTP come uno dei protocolli per il server Transfer Family.

- Assicurati che il valore predefinito, Usa AWS Lambda per connettere il tuo provider di identità, sia selezionato.
- 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, consulta [Configurazione 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:lambda:region:123456789012:function:my-lambda-auth-function",
      "Condition": {
        "ArnLike": {
          "AWS:SourceArn": "arn:aws:transfer:region:123456789012:server/server-id"
        }
      }
    }
  ]
}
```

Note

Nella politica di esempio precedente, sostituisci ciascuna *user input placeholder* 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 verrà quindi richiesto di inserire la tua 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

- [Valori Lambda validi](#)
- [Esempi di funzioni Lambda](#)
- [Verifica della configurazione](#)
- [Modelli di funzioni Lambda](#)

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	Description	Richiesto
Role	Specifica l'Amazon Resource Name (ARN) del ruolo IAM che controlla l'accesso degli utenti al bucket Amazon S3 o al file system Amazon EFS. Le policy associate a questo ruolo determinano il livello di accesso che desideri fornire ai tuoi utenti durante il trasferimento 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	Richiesto
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.	Necessario per lo storage di backup di Amazon EFS

Valore	Description	Richiesto
	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.	
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. Per ulteriori informazioni sull'utilizzo delle policy di sessione con provider di identità personalizzati, consulta gli esempi di policy di sessione in questo argomento.	Facoltativo

Valore	Description	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 suPATH, 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 suLOGICAL, 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	Description	Richiesto
HomeDirectory	La directory di destinazione di un utente quando accede al server utilizzando il client. Il formato dipende dal backend di archiviazione: • Per Amazon S3: /bucket-name/user-home-directory Ad esempio: /amzn-s3-demo-bucket/users/john • Per Amazon EFS: /fs-12345/user-home-directory Ad esempio: /fs-faa1a123/users/john  Important Il nome del bucket o l'ID del file system Amazon EFS devono essere inclusi nel percorso. L'omissione di queste informazioni comporterà l'errore «File non trovato» durante i trasferimenti di file.	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.

⚠ HomeDirectory Requisiti di formato

Quando utilizzate il `HomeDirectory` parametro, assicuratevi di includere il formato completo del percorso:

- Per lo storage Amazon S3: includi sempre il nome del bucket nel formato `/bucket-name/path`
- Per lo storage Amazon EFS: includi sempre l'ID del file system nel formato `/fs-12345/path`

Una causa comune degli errori «File not found» è l'omissione del nome del bucket o dell'ID del file system EFS dal `HomeDirectory` percorso. Se `HomeDirectory` si imposta su «Solo / senza l'identificatore di archiviazione», l'autenticazione avrà esito positivo, ma le operazioni sui file falliranno.

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 format depends on your storage backend:
      // For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
      // users/john')
      // For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
      HomeDirectory: '/my-transfer-bucket/users/example-user' // S3 example -
      // replace with your bucket name
      // HomeDirectory: '/fs-faa1a123/users/example-user' // EFS example - uncomment
      // for EFS
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
      // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
      // authentication failure
      response = {};
    }
  } else {
```

```
// Return HTTP status 200 but with no role in the response to indicate
authentication failure
response = {};
}
callback(null, response);
};
```

Logical home directory, Python

La 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 format depends on your storage backend:
            # For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
            # users/john')
            # For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
            'HomeDirectory': '/my-transfer-bucket/users/example-user', # S3 example -
            # replace with your bucket name
            # 'HomeDirectory': '/fs-faa1a123/users/example-user', # EFS example -
            # uncomment for EFS
            'HomeDirectoryType': "PATH" # Not strictly required, defaults to PATH

```

```

    }

    # Check if password is provided
    if event.get('password', '') == '':
        # If no password provided, return the user's SSH public key
        response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
        # Check if password is correct
        elif event['password'] != 'Password1234':
            # Return HTTP status 200 but with no role in the response to indicate
            authentication failure
            response = {}
        else:
            # Return HTTP status 200 but with no role in the response to indicate
            authentication failure
            response = {}

    return response

```

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 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 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 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 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\": \"\"
}
```

Modelli di funzioni Lambda

È possibile distribuire uno 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 FIPS-enabled AWS Transfer Family server CloudFormation specificando una politica FIPS-enabled di sicurezza nel modello. Le politiche di sicurezza disponibili sono descritte in [Politiche di sicurezza per i server AWS Transfer Family](#)

Per creare uno CloudFormation stack da utilizzare per l'autenticazione

1. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Segui le istruzioni per distribuire uno 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.

- [Gestione dei segreti AWS 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 Gestione dei segreti AWS 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.
- Okta-mfa modello di [stack: un modello](#) di base che viene utilizzato AWS Lambda con un AWS Transfer Family server per integrare Okta, con Multi Factor Authentication, come provider di identità personalizzato.
- [Modello Azure Active Directory](#): i dettagli per questo stack sono descritti nel post del blog [Authenticating to with Azure Active Directory and. AWS Transfer Family AWS 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.

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.

Nella maggior parte dei casi d'uso, il modo consigliato per configurare un provider di identità personalizzato consiste nell'utilizzare il [Soluzione personalizzata per provider di identità](#)

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 tuo 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 operazioni 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 metodo API Gateway come provider di identità personalizzato per Transfer Family, abilita IAM per il 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](#).

Non abilitare la memorizzazione nella cache dell'API Gateway

Non abilitate la memorizzazione nella cache per il metodo API Gateway quando lo utilizzate come provider di identità personalizzato per Transfer Family. La memorizzazione nella cache è inappropriata e non valida per le richieste di autenticazione perché:

- Ogni richiesta di autenticazione è unica e richiede una risposta in tempo reale, non una risposta memorizzata nella cache
- La memorizzazione nella cache non offre vantaggi poiché Transfer Family non invia mai richieste duplicate o ripetute all'API Gateway
- L'attivazione della memorizzazione nella cache farà sì che l'API Gateway risponda con dati non corrispondenti, con conseguenti risposte non valide alle richieste di autenticazione

Per utilizzare il metodo API Gateway per l'autenticazione personalizzata con Transfer Family

1. Crea uno CloudFormation stack. Per farlo:

 Note

I modelli di stack sono stati aggiornati per utilizzare BASE64-encoded le password: per i dettagli, vedere. [Miglioramenti ai modelli CloudFormation](#)

- a. Apri la CloudFormation console all'indirizzo. <https://console.aws.amazon.com/cloudformation>
- b. Segui le istruzioni per distribuire uno 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.

- [Gestione dei segreti AWS 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 Gestione dei segreti AWS](#).

- [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. Apri la console API Gateway all'indirizzo <https://console.aws.amazon.com/apigateway/>.
 - b. Scegli l'API del modello di base di Transfer Custom Identity Provider generata dal 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.

The screenshot displays the AWS API Gateway console interface for configuring a method request. On the left, a sidebar shows a resource tree with paths like `/servers`, `/users`, and `/config`. The main panel is titled 'Method request settings' and includes an 'Edit' button. The settings are organized into sections: 'Method request settings' (with fields for Authorization: AWS_IAM, Request validator: None, API key required: False, and SDK operation name: Generated based on method and path), 'Request paths (0)' (showing no request paths defined), 'URL query string parameters (2)' (listing protocol and sourceIp as optional and inactive), 'HTTP request headers (1)' (listing PasswordBase64 as optional and inactive), and 'Request body (0)' (showing no request body defined).

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.

The screenshot shows the AWS Transfer Family console interface. At the top, the breadcrumb navigation reads: API Gateway > APIs > Transfer Custom Identity Provider basic template API > Stages. The main heading is 'Stages'. On the left, a sidebar shows a list of stages with 'prod' selected. The main content area is divided into several sections:

- Stage details** (with an 'info' link and an 'Edit' button):
 - Stage name: prod
 - API cache: ☐ Inactive
 - Rate: 10000
 - Burst: 5000
 - Web ACL: -
 - Client certificate: -
 - Invoke URL**: <https://execute-api.us-east-1.amazonaws.com/prod> (This field is highlighted with a red rectangle in the original image).
 - Active deployment: t8aqrn on December 12, 2023, 10:49 (UTC-05:00)
- Logs and tracing** (with an 'info' link and an 'Edit' button):
 - CloudWatch logs: Error and info logs
 - Detailed metrics: ☐ Inactive
 - X-Ray tracing: ☐ Inactive
 - Custom access logging: ☐ Inactive
- Stage variables** (with tabs for Deployment history, Documentation history, Canary, and Tags):
 - Stage variables (0/0)
 - Search bar: Find resources
 - Table with columns: Name, Value
 - Message: No variables associated with the stage.
 - Button: Manage variables

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.

Choose an identity provider

Identity provider

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

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

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

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

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

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

Provide an Amazon API Gateway URL

Role
IAM role for the service to invoke your Amazon API Gateway URL

- b. 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 CloudFormation modello. Questo ruolo consente a Transfer Family di richiamare il metodo del gateway API.

Il ruolo di invocazione contiene il nome 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.

The screenshot displays the AWS API Gateway console interface for configuring a GET method. On the left, a sidebar shows the resource tree with the path `/servers/{serverId}/users/{username}/config` selected. The main area shows the 'Method request settings' for the GET method. The settings include: Authorization (AWS_IAM), API key required (False), Request validator (None), and SDK operation name (Generated based on method and path). Below this, the 'Request paths (0)' section indicates 'No request paths defined'. The 'URL query string parameters (2)' section lists two parameters: 'protocol' and 'sourceIp', both with 'Required' set to 'False' and 'Caching' set to 'Inactive'.

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, 0—9 A-Z, carattere di sottolineatura '_', trattino '-', punto '.' e nel segno '@'. Il nome utente non può iniziare con un trattino '-', punto '.' o dal segno '@'.

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 HTTP200. 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": "/amzn-s3-demo-bucket/path/to/home/directory"
}
```

Note

La policy viene salvata in formato JSON come stringa. Esempio:

```
"Policy":
"{
```

```

{"Version": "2012-10-17",
 "Statement":
  [
    {"Condition":
      {"StringLike":
        {"s3:prefix":
          ["user/*", "user/"]}},
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Sid": "ListHomeDir",
      {"Resource": "arn:aws:s3:::*",
        "Action": ["s3:PutObject",
          "s3:GetObject",
          "s3:DeleteObjectVersion",
          "s3:DeleteObject",
          "s3:GetObjectVersion",
          "s3:GetObjectACL",
          "s3:PutObjectACL"],
        "Effect": "Allow",
        "Sid": "HomeDirObjectAccess"]}
  ]
}

```

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\": \"/amzn-s3-demo-bucket1\"}]",
  "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, vedere [Gestione 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 il seguente esempio di funzioni Lambda 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 Entry/Target mappature desiderate, simili ai valori descritti nel [HomeDirectoryDetails](#) parametro per gli utenti gestiti dal servizio.

Le funzioni di esempio sono elencate in [Esempi di funzioni Lambda](#)

Funzione Lambda da utilizzare con Gestione dei segreti AWS

Per Gestione dei segreti AWS utilizzarla come provider di identità, puoi utilizzare la funzione Lambda nel modello di esempio 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 Gestione dei segreti AWS](#).

Per scaricare un CloudFormation modello di esempio che utilizza questa funzione Lambda, vai al bucket [Amazon S3 fornito](#) da AWS Transfer Family

Miglioramenti ai modelli CloudFormation

Sono stati apportati miglioramenti all'interfaccia API Gateway ai CloudFormation modelli pubblicati. I modelli ora utilizzano BASE64-encoded password con API Gateway. Le distribuzioni esistenti continuano a funzionare senza questo miglioramento, ma non consentono l'utilizzo di password con caratteri diversi dal set di caratteri di base. US-ASCII

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'PasswordBase64header` (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 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 CloudFormation stack, consulta [Modificare un modello di stack](#) nella Guida per l'AWS CloudFormation utente.

Utilizzo di più metodi di autenticazione

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 SSH/SFTP protocollo 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.

Per le opzioni personalizzate del provider di identità, puoi specificare una delle seguenti opzioni per 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.

Supporto IPv6 per provider di identità personalizzati

AWS Transfer Family i provider di identità personalizzati supportano completamente le connessioni IPv6. Quando si implementa un provider di identità personalizzato, la funzione Lambda può ricevere ed elaborare richieste di autenticazione da client IPv4 e IPv6 senza alcuna configurazione aggiuntiva. La funzione Lambda riceve l'indirizzo IP del client nel `sourceIp` campo della richiesta, che può essere un indirizzo IPv4 (ad esempio, `203.0.113.42`) o un indirizzo IPv6 (ad esempio, `2001:db8:85a3:8d3:1319:8a2e:370:7348`). L'implementazione del provider di identità personalizzato deve gestire entrambi i formati di indirizzi in modo appropriato.

Important

Se il tuo provider di identità personalizzato esegue la IP-based convalida o la registrazione, assicurati che l'implementazione gestisca correttamente i formati di indirizzi IPv6. Gli indirizzi IPv6 sono più lunghi degli indirizzi IPv4 e utilizzano un formato di notazione diverso.

Note

Quando gestisci gli indirizzi IPv6 nel tuo provider di identità personalizzato, assicurati di utilizzare le funzioni di analisi degli indirizzi IPv6 appropriate anziché semplici confronti di stringhe. Gli indirizzi IPv6 possono essere rappresentati in vari formati canonici (ad esempio `fd00:b600::ec2` o `fd00:b600:0:0:0:0:ec2`). Utilizza le librerie o le funzioni di indirizzi IPv6 appropriate nel tuo linguaggio di implementazione per convalidare e confrontare correttamente gli indirizzi IPv6.

Example Gestione degli indirizzi IPv4 e IPv6 in un provider di identità personalizzato

```
def lambda_handler(event, context):
```

```
# Extract the source IP address from the request
source_ip = event.get('sourceIp', '')

# Log the client IP address (works for both IPv4 and IPv6)
print(f"Authentication request from: {source_ip}")

# Example of IP-based validation that works with both IPv4 and IPv6
if is_ip_allowed(source_ip):
    # Continue with authentication
    # ...
else:
    # Reject the authentication request
    return {
        "Role": "",
        "HomeDirectory": "",
        "Status": "DENIED"
    }
```

Per ulteriori informazioni sull'implementazione di provider di identità personalizzati, consulta [Utilizzo AWS Lambda per integrare il tuo provider di identità](#)

Utilizzo di AWS Directory Service per Microsoft Active Directory

Puoi utilizzarlo AWS Transfer Family per autenticare gli utenti finali che effettuano il 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 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. Il blog AWS sullo storage contiene un post che descrive in dettaglio una soluzione per l'utilizzo di Active Directory with Transfer Family: [Simplify Active Directory authentication with a identity provider personalizzato per AWS Transfer Family](#).

 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 RADIUS-based MFA esistente.
- 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 Directory Service console.
2. Usa la console Transfer Family per creare un server che utilizzi AWS Managed Microsoft AD come provider di identità.
3. Configura AWS Directory utilizzando un connettore Active Directory.
4. Aggiungi l'accesso da uno o più dei tuoi Directory Service gruppi.
5. Sebbene non sia obbligatorio, ti consigliamo di testare e verificare l'accesso degli utenti.

Argomenti

- [Prima di iniziare a utilizzare AWS Directory Service for Microsoft Active Directory](#)
- [Utilizzo dei realm di Active Directory](#)
- [Scelta AWS Managed Microsoft AD come provider di identità](#)
- [Connessione a Microsoft Active Directory locale](#)
- [Concessione dell'accesso ai gruppi](#)
- [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

Note

AWS Transfer Family ha un limite predefinito di 100 gruppi di Active Directory per server. Se il tuo caso d'uso richiede più di 100 gruppi, prendi in considerazione l'utilizzo di una soluzione di provider di identità personalizzata, come descritto in [Semplificare l'autenticazione di Active Directory con un provider di identità personalizzato per AWS Transfer Family](#).

Fornisci un identificatore univoco per i tuoi gruppi AD

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`. AWS Transfer Family non accetta il valore specificato in `userPrincipalName`.

Aggiungi Directory Service autorizzazioni al tuo ruolo

Ti servono anche le autorizzazioni 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:UnauthorizeApplications` 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 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 user/group realm, viene visualizzato l'errore Nessun accesso associato trovato per i gruppi di utenti.

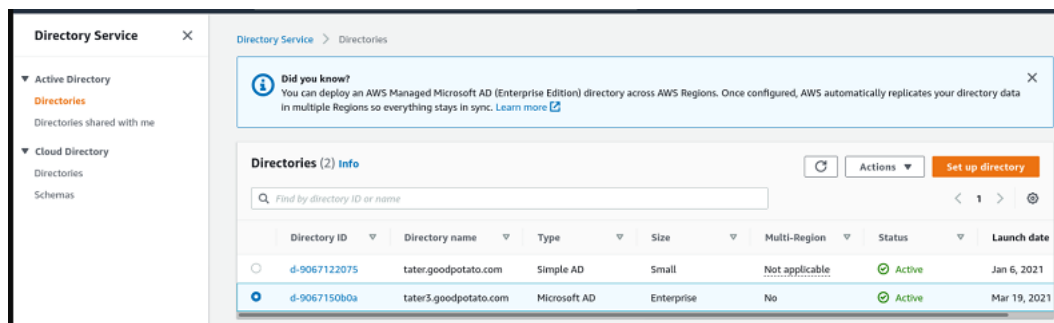
Scelta AWS Managed Microsoft AD come provider di identità

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 a Console di gestione AWS e apri la Directory Service console all'indirizzo <https://console.aws.amazon.com/directoryservicev2/>.

Usa la Directory Service console per configurare una o più directory gestite. Per ulteriori informazioni, consulta [AWS Managed Microsoft AD](#) nella Guida per gli amministratori 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.

Choose an identity provider

Identity provider

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

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

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

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

Directory
TATER3 ▼ 

[Cancel](#) [Previous](#) [Next](#)

5. L'elenco delle directory contiene tutte le directory gestite che hai configurato. Scegliete una directory dall'elenco e scegliete Avanti.

Note

- Cross-Account e Le directory condivise non sono supportate per AWS Managed Microsoft AD.
- Per configurare un server con Directory Service come provider di identità, è necessario aggiungere alcune 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 SFTP-enabled server](#)
- [Creare un FTPS-enabled server](#)

- [Crea un FTP-enabled server](#)

In queste procedure, continua con il passaggio successivo alla scelta di un provider di identità.

 Important

Non puoi eliminare una directory Microsoft AD Directory Service se l'hai usata in un server Transfer Family. È necessario prima eliminare il server, quindi è possibile eliminare la directory.

Connessione a Microsoft Active Directory locale

Questa sezione descrive come configurare una AWS directory utilizzando un AD Connector.

Per configurare la 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 utilizzando per Microsoft Active Directory.
 - Indirizzi IP DNS: inserisci gli indirizzi IP di Microsoft Active Directory.
 - Nome utente e password dell'account del server: inserisci i dettagli dell'account di servizio da utilizzare.
6. Completa le schermate per creare il servizio di directory.

Il passaggio successivo consiste nel creare un server Transfer Family con il protocollo SFTP e il tipo di provider di identità AWS Directory Service. Dall'elenco a discesa Directory, selezionate la directory aggiunta nella procedura precedente.

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

AWS Transfer Family ha un limite predefinito di 100 gruppi di Active Directory per server. Se il tuo caso d'uso richiede più di 100 gruppi, prendi in considerazione l'utilizzo di una soluzione di provider di identità personalizzata, come descritto in [Semplificare l'autenticazione di Active Directory con un provider di identità personalizzato per AWS Transfer Family](#).

Note

Gli utenti devono appartenere direttamente al gruppo a cui concedi 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 Amazon S3 che corrisponda alla home directory del gruppo.

 Note

Puoi limitare le porzioni del bucket visualizzate dagli utenti creando una policy 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, consulta [Creazione 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.

Endpoint configuration

Availability Zone	Subnet ID	Private IPv4 Address
us-east-1a	subnet-...	172.31.80.36

Accesses (1)

Actions Associate access

External Id	Home directory	Role
☒ S...	/padbucket3	ADGuy_S3_And_EFS

Additional details Edit

Logging role [Info](#)
Server activity not logged to Amazon CloudWatch

Server host key [Info](#)

Security Policy [Info](#)
TransferSecurityPolicy-2018-11

Domain
Amazon S3

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.

Identity provider testing

User configuration [Info](#)

Username:
Password:

Response

```
{
  "Response": {
    "homeDirectory": {"/padbucket3"},
    "homeDirectoryDetails": null,
    "homeDirectoryType": "PATH",
    "posixProfile": {
      "publicKeys": null,
      "role": "arn:aws:iam::195886157073:role/ADGuy_53_Aud_EFS",
      "policy": null,
      "userName": "transferuser1",
      "identityProviderType": null,
      "userConfigMessage": null
    },
    "StatusCode": 200,
    "Message": ""
  }
}
```

Cancel **Test**

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

Directory Service dispone delle seguenti opzioni per connettersi a un Active Directory autogestito:

- One-way forest trust (in uscita AWS Managed Microsoft AD e in entrata per Active Directory locale) funziona solo per il dominio radice.
- Per i domini figlio, 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`.

Utilizzo di AWS Directory Service per Entra ID Domain Services

Per i clienti che necessitano solo di SFTP Transfer e non desiderano gestire un dominio, è disponibile Simple Active Directory. In alternativa, i clienti che desiderano i vantaggi di Active Directory e l'elevata disponibilità in un servizio completamente gestito possono utilizzare AWS Managed Microsoft AD. Infine, per i clienti che desiderano sfruttare la foresta Active Directory esistente per il trasferimento SFTP, è disponibile Active Directory Connector.

Tenere presente quanto segue:

- Per sfruttare la foresta Active Directory esistente per le esigenze di trasferimento SFTP, è possibile utilizzare [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 di AWS Directory Service per Microsoft Active Directory](#).

Questo argomento descrive come usare un connettore Active Directory e i [servizi di dominio Entra ID \(precedentemente Azure AD\)](#) per autenticare gli utenti di SFTP Transfer con Entra ID.

Argomenti

- [Prima di iniziare a utilizzare AWS Directory Service per Entra ID Domain Services](#)
- [Fase 1: aggiunta dei servizi di dominio Entra ID](#)
- [Fase 2: Creazione di un account di servizio](#)
- [Fase 3: Configurazione della AWS directory tramite AD Connector](#)
- [Fase 4: Configurazione AWS Transfer Family del server](#)
- [Fase 5: Concessione dell'accesso ai gruppi](#)
- [Fase 6: Test degli utenti](#)

Prima di iniziare a utilizzare AWS Directory Service per Entra ID Domain Services

Note

AWS Transfer Family ha un limite predefinito di 100 gruppi Active Directory per server. Se il tuo caso d'uso richiede più di 100 gruppi, prendi in considerazione l'utilizzo di una soluzione

di provider di identità personalizzata, come descritto in [Semplificare l'autenticazione di Active Directory con un provider di identità personalizzato per AWS Transfer Family](#).

Perché AWS, hai bisogno di 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 VPN da sito a sito con Microsoft Entra

Per Microsoft Entra, è necessario quanto segue:

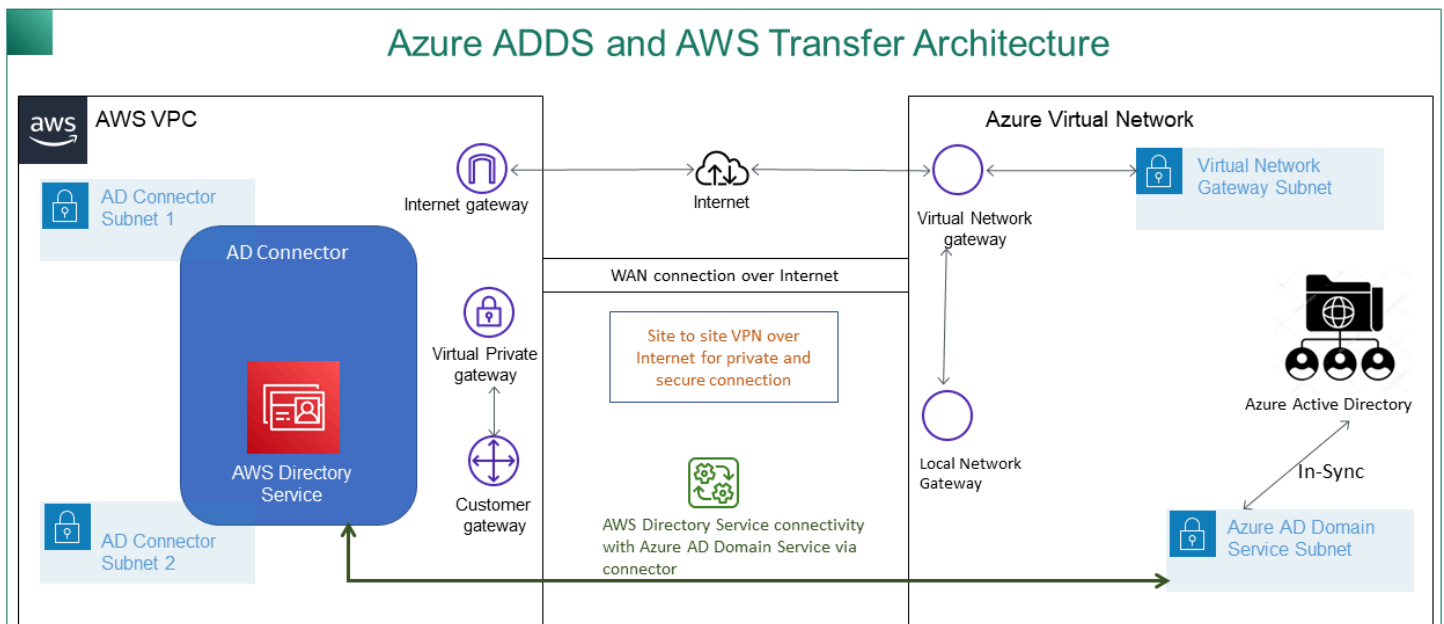
- Un ID Entra e un servizio di dominio Active Directory
- Un gruppo di risorse Entra
- Una rete virtuale Entra
- Connettività VPN tra Amazon VPC e il gruppo di risorse Entra

Note

Ciò può avvenire tramite tunnel IPSEC nativi o utilizzando dispositivi VPN. In questo argomento, utilizziamo i tunnel IPSEC tra un gateway di rete Entra Virtual e un gateway di rete locale. I tunnel devono essere configurati per consentire il traffico tra gli endpoint del servizio di dominio Entra e le sottoreti che ospitano il VPC. AWS

- Un gateway per i clienti e un gateway privato virtuale per la connessione VPN da sito a sito con Microsoft Entra

Il diagramma seguente mostra la configurazione necessaria prima di iniziare.



Fase 1: aggiunta dei servizi di dominio Entra ID

Per impostazione predefinita, Entra ID non supporta le istanze di aggiunta al dominio. Per eseguire azioni come Domain Join e utilizzare strumenti come Group Policy, gli amministratori devono abilitare Entra ID Domain Services. Se non hai già aggiunto Entra 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'attivazione di Entra ID Domain Services, vedere [Tutorial: Creare e configurare un dominio gestito di Microsoft Entra Domain Services](#).

Note

Quando abiliti Entra DS, assicurati che sia configurato per il gruppo di risorse e il dominio Entra a cui stai connettendo il tuo server di trasferimento SFTP.


bob.us

 Azure AD Domain Services

«
Refresh
Delete

Overview

 Activity log

 Access control (IAM)

 Tags

 Settings

 Properties


bob.us

Running

View health

Configuration issues for your managed domain were detected. Run configuration diagnostics

Fase 2: Creazione di un account di servizio

Entra deve disporre di un account di servizio che faccia parte di un gruppo di amministratori in Entra DS. Questo account viene utilizzato con il connettore AWS Active Directory. Assicurati che questo account sia sincronizzato con Entra DS.

[Home](#) > [Default Directory](#) > [Users](#) > [bobatusa](#)


bobatusa | Profile

 User

«
Edit
Reset password
Revoke sessions
Delete
Refresh
Got feedback?

Diagnose and solve problems

Manage

 Profile

 Assigned roles

 Administrative units

 Groups

 Applications

 Licenses

 Devices

 Azure role assignments

 Authentication methods

bobatusa

bobsmith@xyz.com



Creation time

 10/6/2021, 1:32:27 AM

Identity

Name	First name	Last name
bobatusa	Bob	Smith
User Principal Name	User type	
bobsmith@xyz.com	Member	

User Sign-ins

 30

 20

 10

 0

 Oct 10 Oct 17 Oct 24 Oct 31

Group memberships

 2

 1

 0

 Oct 10 Oct 17 Oct 24 Oct 31

Activity

 Sign-in logs

 Audit logs

Tip

Multi-factor l'autenticazione per Entra ID non è supportata per i server Transfer Family che utilizzano 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.

multi-factor authentication
users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)
Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users Multi-Factor Auth status: Any bulk update

☐	DISPLAY NAME ^	USER NAME	MULTI-FACTOR AUTH STATUS
☐	Christopher	admin@christopher.com	Disabled
☐	Robert	test@christopher.com	Disabled

Select a user

Fase 3: Configurazione della AWS directory tramite AD Connector

Dopo aver configurato Entra DS e creato un account di servizio con tunnel VPN IPSEC tra il tuo AWS VPC e la rete Entra Virtual, puoi testare la connettività eseguendo il ping dell'indirizzo IP DNS Entra DS da qualsiasi istanza EC2. AWS

Dopo aver verificato che la connessione sia attiva, puoi continuare qui sotto.

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 utilizzando per Entra DS.
 - Indirizzi IP DNS: inserisci i tuoi indirizzi IP Entra DS.

- Nome utente e password dell'account del server: inserisci i dettagli dell'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.

Directory Service > Directories

 **Did you know?**
You can deploy an AWS Managed Microsoft AD (Enterprise Edition) directory across AWS Regions. Once configured, AWS automatically replicates your directory data in multiple Regions so everything stays in sync. [Learn more](#)

Directories (1) [Info](#)



Actions ▾

Set up directory

< 1 > 

	Directory ID ▾	Directory name ▾	Type ▾	Size ▾	Multi-Region ▾	Status ▾	Launch date ▾
	d-906752c0d7		AD Connector	Small	Not applicable	 Active	Nov 3, 2021

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

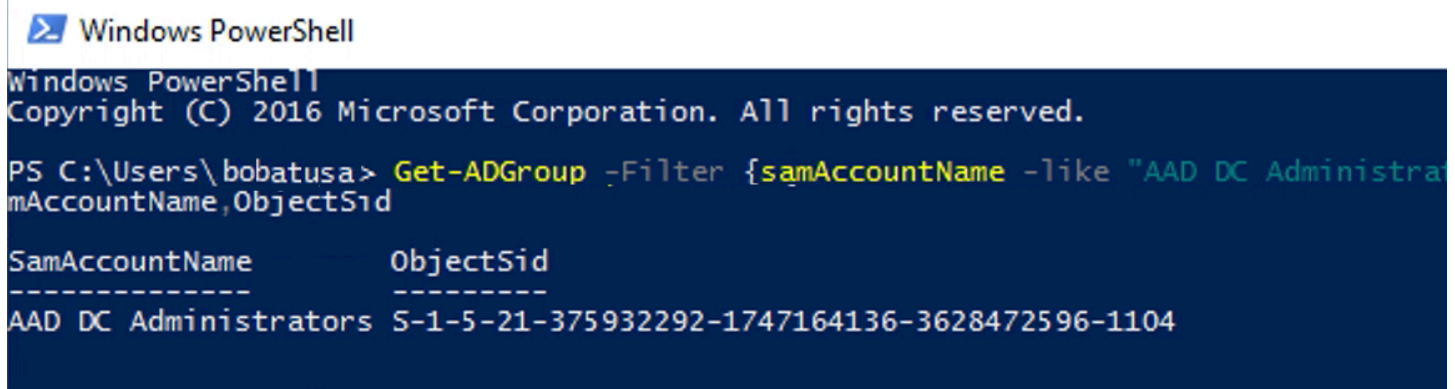
Gli utenti devono appartenere direttamente al gruppo a cui si concede l'accesso. Ad esempio, supponiamo che Bob sia un utente e appartenga al gruppo A e che lo stesso gruppo A sia incluso nel gruppo B.

- 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
```



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\bobatusa> Get-ADGroup -Filter {samAccountName -like "AAD DC Administrat
mAccountName,ObjectSid

SamAccountName      ObjectSid
-----
AAD DC Administrators S-1-5-21-375932292-1747164136-3628472596-1104
```

Concedi l'accesso ai gruppi

1. Aprire <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 che hai 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 directory Home, scegli un bucket Amazon 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:

Protocols Edit

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider Edit

Identity provider type
AWS Directory Service

Directory ID
d-123456789a

Accesses (1) Actions ▾ Add access

Search:

☐	External Id ▾	Home directory ▾	Role ▾
☐	S-1-5-21-375932292-1747164136-3628472596-1104	/sftp-home	sftp-user-role ↗

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.

Utilizzo di directory logiche per semplificare le strutture di directory Transfer Family

Le directory logiche semplificano la struttura delle directory del server. AWS Transfer Family Con le directory logiche, puoi creare una struttura di directory virtuale con nomi intuitivi che gli utenti utilizzano quando si connettono al tuo bucket Amazon S3 o al file system Amazon EFS. Ciò impedisce agli utenti di visualizzare i percorsi delle directory, i nomi dei bucket e i nomi dei file system effettivi.

Note

È necessario utilizzare i criteri di sessione in modo che gli utenti finali possano eseguire solo le operazioni che gli consentite 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.

Comprendere chroot e la struttura delle cartelle

Un'operazione chroot consente di impostare la directory principale di un utente in qualsiasi posizione nella gerarchia di archiviazione. Ciò limita gli utenti alla directory principale o principale configurata, impedendo l'accesso alle directory di livello superiore.

Prendi in considerazione un caso in cui un utente Amazon S3 è limitato a `amzn-s3-demo-bucket/home/${transfer:UserName}`. Senza chroot, alcuni client potrebbero consentire agli utenti di passare a `/amzn-s3-demo-bucket/home`, richiedendo un logout e un login per tornare alla directory corretta. L'esecuzione di un'operazione chroot previene questo problema.

È possibile creare strutture di directory personalizzate su più bucket e prefissi. Ciò è utile se il flusso di lavoro richiede un layout di directory specifico che i prefissi dei bucket da soli non sono in grado di fornire. 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.

Regole per l'utilizzo delle directory logiche

Questa sezione descrive alcune regole e altre considerazioni per l'utilizzo delle directory logiche.

Limiti di mappatura

- È consentita una sola mappatura quando lo Entry è `"/` (non sono consentiti percorsi sovrapposti).

- Le directory logiche supportano mappature fino a 2,1 MB per utenti IDP e AD personalizzati e 2.000 voci per utenti gestiti dal servizio. È possibile calcolare la dimensione delle mappature 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.

Requisiti del percorso di destinazione

- Usa la `${transfer:UserName}` variabile se il bucket o il percorso del file system sono stati parametrizzati in base al nome utente.
- Le destinazioni possono essere configurate in modo che puntino a diversi bucket o file system di Amazon S3, purché il ruolo IAM associato disponga delle autorizzazioni necessarie per accedere a tali posizioni di storage.
- Tutti gli obiettivi devono iniziare con una barra in avanti (/) ma non possono terminare con una. Ad esempio, `/amzn-s3-demo-bucket/images` è corretto, mentre non `amzn-s3-demo-bucket/images/` o `/amzn-s3-demo-bucket/images/` è.

Considerazioni sullo storage

- Amazon S3 è un archivio di oggetti in cui le cartelle esistono solo come concetto virtuale. Quando si utilizza lo storage Amazon S3, Transfer Family riporta i prefissi come directory nelle operazioni STAT, anche se non esiste un oggetto a zero byte con una barra finale. Un oggetto a zero byte appropriato con una barra finale viene inoltre riportato come directory nelle operazioni STAT. 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.
- Per le applicazioni che devono distinguere tra file e cartelle, usa Amazon Elastic File System (Amazon EFS) come opzione di storage Transfer Family.
- Se stai specificando i valori della directory logica per il tuo utente, il parametro che usi 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`

Valori delle directory utente

- Il parametro per specificare i valori delle directory logiche 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`
- Quando si utilizza `LOGICAL HomeDirectoryType`, è possibile specificare un `HomeDirectory` valore per gli utenti di `Service Managed`, l'accesso ad `Active Directory` e le implementazioni di `Custom Identity Provider`, laddove `HomeDirectoryDetails` forniti nella risposta. Se non specificato, il `HomeDirectory` valore predefinito è. /

Per informazioni dettagliate su come implementare le directory logiche, vedere. [Implementazione di directory logiche](#)

Implementazione di directory logiche

Important

Requisiti della directory principale

- Se non utilizzi le impostazioni di ottimizzazione delle prestazioni di Amazon S3, la directory principale deve esistere all'avvio.
- Per Amazon S3, ciò significa creare un oggetto a zero byte che termina con una barra (`.`). /
- Per evitare questo requisito, valuta la possibilità di abilitare l'ottimizzazione delle prestazioni di Amazon S3 quando crei o aggiorni il server.
- Quando si specifica un `HomeDirectory` con `LOGICAL HomeDirectoryType`, il valore deve essere mappato a una delle mappature delle directory logiche. Il servizio lo convalida sia durante la creazione degli utenti che durante gli aggiornamenti per evitare configurazioni che non funzionerebbero.

Configurazione logica della home directory

Quando si utilizza LOGICAL come impostazione HomeDirectoryType predefinita, tenere presente quanto segue:

- Il HomeDirectory valore deve corrispondere a una delle mappature di directory logiche esistenti.
- Il sistema lo convalida automaticamente durante la creazione e gli aggiornamenti degli utenti.
- Questa convalida impedisce configurazioni che potrebbero causare problemi di accesso.

Abilita le directory logiche

Per utilizzare le directory logiche per un utente, imposta il HomeDirectoryType parametro su LOGICAL. Esegui questa operazione quando crei un nuovo utente o aggiorni un utente esistente.

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

Abilita **chroot** per gli utenti

Perchroot, crea una struttura di directory composta da una singola Entry Target combinazione per ogni utente. La voce/rappresenta la cartella principale, mentre Target specifica la posizione effettiva nel bucket o nel file system.

Example for Amazon S3

```
[{"Entry": "/", "Target": "/amzn-s3-demo-bucket/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":
```

```
"/amzn-s3-demo-bucket/${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": "/amzn-s3-demo-bucket1/pics"},  
{"Entry": "/doc", "Target": "/amzn-s3-demo-bucket1/anotherpath/docs"},  
{"Entry": "/reporting", "Target": "/amzn-s3-demo-bucket2/Q1"},  
{"Entry": "/anotherpath/subpath/financials", "Target": "/amzn-s3-demo-bucket2/  
financials"}]
```

Note

Puoi caricare file solo nelle cartelle specifiche che mappi. Ciò significa che nell'esempio precedente non è possibile caricare /anotherpath solo anotherpath/subpath anotherpath/subpath/financials nelle nostre directory. 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": "/amzn-s3-demo-bucket/pics"
},
{
  "Entry": "/doc",
  "Target": "/amzn-s3-demo-bucket/mydocs"
},
{
  "Entry": "/temp",
  "Target": "/amzn-s3-demo-bucket2/temporary"
}
```

Puoi caricare file solo in quei bucket. La prima volta che ti connetti `ftp`, 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 qualsiasi `directory/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

Esempi di configurazioni di 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` ed `doc`.

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-
bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs
\"}]" \
  --ssh-public-key-body file:///~/.ssh/id_rsa.pub
```

Se **marymajor** è un utente esistente e il suo tipo di home directory è `PATH`, puoi cambiarlo `LOGICAL` con un comando simile a quello precedente.

```
aws transfer update-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-
bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs
\"}]"
```

Tenere presente quanto segue:

- Se le directory `/amzn-s3-demo-bucket1/pics` e `/amzn-s3-demo-bucket2/test/mydocs` io non esistono già, l'utente (o un amministratore) deve crearle.

Note

Queste directory vengono create automaticamente dal server Transfer Family se sono state configurate directory ottimizzate.

- Quando **marymajor** si connette al server ed esegue il `ls -l` comando, Mary 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 Mary aggiunge `pics` e che `doc` vengono aggiunti rispettivamente ai percorsi `/amzn-s3-demo-bucket1/pics` di Amazon S3. `/amzn-s3-demo-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.

Questo esempio fornisce una configurazione alternativa per un percorso home logico.

```
aws transfer create-user \  
  --user-name marymajor \  
  --server-id s-11112222333344445 \  
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \  
  --home-directory-type LOGICAL \  
  --home-directory /home/marymajor \  
  --home-directory-mappings "[{\"Entry\":\"/home/marymajor/pics\", \"Target\":\"/amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/home/marymajor/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs\"}]" \  
  --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Tenere presente quanto segue:

- Le mappature forniscono un percorso comune `/home/marymajor`, che è la prima parte dei due percorsi logici. I file possono quindi essere aggiunti alle cartelle `pics` e `doc`.
- Come nell'esempio precedente, la home directory `/home/marymajor`, è di sola lettura.

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. Esempio:

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{\"Entry\": \"/\", \"Target\": \"/amzn-s3-demo-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\\\": \\\"/amzn-s3-demo-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.

Accedi ai file system FSx for NetApp ONTAP con Transfer Family

Indice

- [Panoramica di](#)
- [Prerequisiti](#)
 - [Requisiti FSx for NetApp ONTAP](#)
 - [Autorizzazioni IAM richieste](#)
- [Come funziona lo storage FSx con Transfer Family](#)
 - [Identità dell'utente del file system](#)
- [Creazione di un punto di accesso S3 per FSx](#)
 - [Denominazione dei punti di accesso](#)
 - [Creazione di un punto di accesso per FSx for ONTAP NetApp](#)
 - [Configurazione delle autorizzazioni del file system](#)
- [Utilizzo degli alias dei punti di accesso S3 con FSx](#)
 - [Informazioni sugli alias dei punti di accesso](#)
 - [Individuazione dell'alias del punto di accesso](#)
- [Configurazione di Transfer Family per lo storage FSx](#)
 - [Creazione di un ruolo IAM](#)
- [Gestione degli utenti per lo storage FSx](#)
 - [Creazione di un utente](#)
 - [Configurazione di più mappature di directory](#)
- [Configurazione dei client per il trasferimento di file](#)
 - [Configurazione WinSCP](#)
 - [Altri client SFTP](#)
- [Risoluzione dei problemi di storage FSx](#)
 - [Problemi relativi al funzionamento dei file](#)

Panoramica di

Transfer Family supporta Amazon FSx for NetApp ONTAP tramite punti di accesso S3. Amazon FSx for NetApp ONTAP è un servizio completamente gestito che fornisce uno storage di file altamente affidabile, scalabile, ad alte prestazioni e ricco di funzionalità basato sul popolare file system ONTAP. NetApp Quando configuri Transfer Family con un file system FSx, gli utenti si connettono agli endpoint Transfer Family utilizzando client di trasferimento file standard. Transfer Family indirizza le

operazioni sui file tramite un punto di accesso S3 collegato al volume FSx, mentre i dati rimangono sul file system FSx. Per ulteriori informazioni su FSx for NetApp ONTAP, consulta [Cos'è Amazon FSx for ONTAP? NetApp](#)

Questa integrazione ti consente di:

- Trasferisci file utilizzando i protocolli SFTP, FTPS o FTP su uno storage di file di livello aziendale
- Accedi agli stessi dati tramite più protocolli (SFTP, NFS, SMB)
- Utilizza funzionalità FSx come istantanee, backup e tiering dei dati

Important

Alcune operazioni sui file non sono supportate quando si utilizzano i file system FSx con Transfer Family, incluse le operazioni di ridenominazione e aggiunta. Per le operazioni di caricamento, le dimensioni dei file sono limitate a 5 GB. Per un elenco completo delle limitazioni, consulta [Compatibilità con i punti di accesso](#).

Prerequisiti

Prima di configurare Transfer Family con Amazon FSx, devi soddisfare i seguenti requisiti.

Requisiti FSx for NetApp ONTAP

Per utilizzare FSx for NetApp ONTAP con Transfer Family, è necessario:

- Un file system FSx for NetApp ONTAP che esegue ONTAP versione 9.17.1 o successiva
- Il file system e il punto di accesso S3 nella stessa regione AWS
- Lo stesso AWS account che possiede sia il file system che il punto di accesso

Per ulteriori informazioni, consulta la pagina [Guida introduttiva ad Amazon FSx for NetApp ONTAP](#).

Autorizzazioni IAM richieste

Puoi configurare ogni punto di accesso S3 con autorizzazioni e controlli di rete distinti che S3 applica per qualsiasi richiesta effettuata utilizzando quel punto di accesso. I punti di accesso S3 supportano le policy delle risorse IAM che puoi utilizzare per controllare l'uso del punto di accesso in base alla

risorsa, all'utente o ad altre condizioni. Affinché un'applicazione o un utente possa accedere ai file tramite un punto di accesso, sia il punto di accesso che il volume sottostante devono consentire la richiesta. Per ulteriori informazioni, consulta le [politiche dei punti di accesso IAM](#).

Gli access point Amazon S3 per FSx utilizzano un modello di autorizzazione a doppio livello che combina le autorizzazioni IAM con le autorizzazioni a livello di file system. Questo approccio garantisce che le richieste di accesso ai dati siano autorizzate correttamente sia a livello di AWS servizio che a livello di file system sottostante.

Affinché un'applicazione o un utente possa accedere correttamente ai dati tramite un punto di accesso, sia la policy del punto di accesso S3 che il volume FSx sottostante devono consentire la richiesta.

Per creare e configurare questa integrazione, sono necessarie le seguenti autorizzazioni:

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`
- `s3:PutAccessPointPolicy`(se si crea una policy opzionale per i punti di accesso)

Come funziona lo storage FSx con Transfer Family

Quando si configura Transfer Family con un file system FSx, i seguenti componenti interagiscono per abilitare i trasferimenti di file:

1. Un utente si connette al server Transfer Family utilizzando un client SFTP, FTPS o FTP.
2. Transfer Family autentica l'utente utilizzando identità gestite dal servizio, un provider di identità personalizzato o AWS Directory Service for Microsoft Active Directory. Una volta autenticata, Transfer Family assume il ruolo IAM associato all'utente.
3. Per ogni operazione sui file, Transfer Family funge da client API S3 standard, inoltra richieste all'Access Point S3 utilizzando il ruolo IAM presunto dell'utente e verifica le autorizzazioni rispetto alla policy del punto di accesso S3.
4. Il file system FSx verifica che l'utente del file system associato al punto di accesso sia autorizzato a eseguire l'operazione richiesta. L'operazione sul file viene quindi eseguita sul volume FSx.

Affinché un'operazione sui file abbia esito positivo, entrambi i livelli di autorizzazione devono consentire la richiesta.

 Note

Il collegamento di un access point S3 a un volume FSx non modifica il comportamento del volume in caso di accesso diretto tramite NFS o SMB. L'accesso al protocollo di file esistente continua a funzionare invariato.

Identità dell'utente del file system

Ogni punto di accesso utilizza un'identità utente del file system specificata durante la creazione del punto di accesso. Questa identità autorizza tutte le richieste di accesso ai file effettuate tramite quel punto di accesso. L'utente del file system è un account utente sul file system Amazon FSx sottostante. Se l'utente del file system ha accesso in sola lettura, vengono autorizzate solo le richieste di lettura effettuate utilizzando il punto di accesso e le richieste di scrittura vengono bloccate. Se l'utente del file system dispone di accesso in lettura/scrittura, sono autorizzate sia le richieste di lettura che quelle di scrittura al volume allegato effettuate utilizzando il punto di accesso.

Creazione di un punto di accesso S3 per FSx

Prima di configurare Transfer Family, è necessario creare un punto di accesso S3 collegato al volume FSx. I punti di accesso S3 sono endpoint di rete denominati collegati a un'origine dati come un bucket o un volume Amazon FSx for ONTAP. Puoi creare e collegare un access point a un FSx for NetApp ONTAP utilizzando la console Amazon FSx, l'interfaccia a riga di AWS comando o l'API. Una volta collegato, si possono utilizzare le API degli oggetti S3 per accedere ai dati dei file. I dati continuano a risiedere nel file system Amazon FSx e continuano a essere direttamente accessibili per i carichi di lavoro esistenti. È possibile continuare a gestire lo storage utilizzando tutte le funzionalità di gestione dello storage FSx for NetApp ONTAP, tra cui backup, istantanee, quote di utenti e gruppi e compressione.

Per ulteriori informazioni, consulta [Creazione dei punti di accesso](#).

Denominazione dei punti di accesso

Quando assegnate un nome al punto di accesso, seguite queste linee guida:

- I nomi dei punti di accesso devono essere univoci all'interno del tuo AWS account e della tua regione.
- I nomi non possono terminare con `-ext-s3alias` (riservato agli alias).

- Evita di includere informazioni sensibili nei nomi perché sono pubblicati nel DNS.

Per un elenco completo delle regole di denominazione, consulta Regole, [restrizioni e limitazioni di denominazione dei punti di accesso](#).

Creazione di un punto di accesso per FSx for ONTAP NetApp

Utilizzare la procedura seguente per creare un punto di accesso S3 per un volume FSx NetApp for ONTAP.

Per creare un punto di accesso (console)

1. Apri la console Amazon FSx all'indirizzo. <https://console.aws.amazon.com/fsx/>
2. Nel riquadro di navigazione, scegli File system.
3. Scegliete il vostro file system FSx for NetApp ONTAP.
4. Scegliete la scheda Volumi.
5. Seleziona il volume che desideri allegare.
6. Per Azioni, scegli Crea punto di accesso S3.
7. Per il nome del punto di accesso, inserisci un nome descrittivo (ad esempio, transfer-family-ap).
8. Per Tipo di identità utente del file system, scegliete una delle seguenti opzioni:
 - Identità UNIX: per volumi con stile di sicurezza UNIX
 - Identità Windows: per volumi con stile di sicurezza NTFS
9. (Facoltativo) Per la policy dei punti di accesso, inserisci una policy IAM che definisca quali presidi IAM possono eseguire quali operazioni sugli oggetti a cui si accede tramite questo punto di accesso. Per ulteriori informazioni, consulta [Gestione dell'accesso ai punti di accesso](#).
10. Scegli Create (Crea).
11. Dopo la creazione, annota l'alias del punto di accesso da utilizzare nella configurazione Transfer Family.

Note

Quando AWS Transfer Family accede alle risorse S3 per conto dei tuoi SFTP/FTPS utenti connessi, le richieste provengono dall' AWS Transfer Family infrastruttura, non dal tuo VPC.

Per questo motivo, gli access point S3 configurati con un'origine di rete VPC negheranno queste richieste. Tuttavia, anche se si utilizza un Access Point configurato con un'origine di rete Internet, tutto il traffico tra Transfer Family e l'Access Point rimane privato e viaggia sulla rete AWS dorsale, senza attraversare la rete Internet pubblica.

Configurazione delle autorizzazioni del file system

L'utente del file system specificato determina le operazioni che gli utenti di Transfer Family possono eseguire. È necessario configurare le autorizzazioni appropriate sul volume FSx.

Esempio UNIX:

```
# Create a directory for Transfer Family users
mkdir -p /vol1/transfer-users

# Set ownership to match the access point user
chown 1001:1001 /vol1/transfer-users

# Set permissions
chmod 755 /vol1/transfer-users
```

Esempio di Windows:

```
# Create a directory for Transfer Family users
New-Item -Path "D:\vol1\transfer-users" -ItemType Directory

# Set permissions for the file system user associated with the access point
# Replace DOMAIN\TransferUser with your Windows user identity
icacls "D:\vol1\transfer-users" /grant "DOMAIN\TransferUser:(OI)(CI)M" /T

# Verify permissions
icacls "D:\vol1\transfer-users"
```

Utilizzo degli alias dei punti di accesso S3 con FSx

Quando si utilizzano i file system FSx con Transfer Family, è necessario utilizzare gli alias dei punti di accesso S3. Transfer Family non supporta l'utilizzo di access point ARN o altri metodi di riferimento per lo storage FSx.

 Important

AWS Transfer Family supporta gli alias dei punti di accesso S3 solo quando si utilizzano i file system FSx. Non è possibile utilizzare gli ARN dei punti di accesso o gli URI in stile ospitato virtualmente.

 Important

Il punto di accesso deve trovarsi nella stessa regione del volume.

Informazioni sugli alias dei punti di accesso

Quando crei un punto di accesso S3 collegato a un volume FSx, Amazon S3 genera automaticamente un alias del punto di accesso. Questo alias è un identificatore univoco che puoi usare ovunque utilizzi un nome di bucket S3.

Per i punti di accesso collegati ai volumi FSx, l'alias utilizza il seguente formato:

```
access-point-name-metadata-ext-s3alias
```

Alias di esempio:

```
my-fsx-ap-aqfqprinstn7aefdfbarligizwgyfouse1a-ext-s3alias
```

 Note

Il `-ext-s3alias` suffisso è riservato agli alias dei punti di accesso FSx. Non è possibile utilizzare questo suffisso nei nomi dei punti di accesso.

Individuazione dell'alias del punto di accesso

È possibile trovare l'alias del punto di accesso dopo averlo creato.

Per trovare l'alias del punto di accesso (console)

1. Apri la console Amazon FSx all'indirizzo. <https://console.aws.amazon.com/fsx/>

2. Nel riquadro di navigazione, scegli File system.
3. Scegli il tuo file system.
4. Scegli la scheda Volumi e seleziona il volume per cui hai creato il punto di accesso.
5. Vai alla colonna dei dettagli del punto di accesso S3.
6. L'alias viene visualizzato nella colonna Alias.

Per trovare l'alias del punto di accesso (CLI)

Utilizza il comando `describe-s3-access-point-attachments`.

```
aws fsx describe-s3-access-point-attachments \
  --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

La risposta include l'alias:

```
{
  "S3AccessPointAttachments": [
    {
      "S3AccessPoint": {
        "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-fsx-
ap",
        "Alias": "my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias"
      }
    }
  ]
}
```

Quando configuri gli utenti Transfer Family, usa l'alias del punto di accesso nelle mappature delle home directory.

Formato della home directory:

```
/access-point-alias/path/to/directory
```

Esempio:

```
/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/jsmith
```

Configurazione di Transfer Family per lo storage FSx

Dopo aver creato il punto di accesso S3, configura un server Transfer Family per utilizzarlo.

Creazione di un ruolo IAM

Devi creare un ruolo IAM che conceda a Transfer Family l'accesso al punto di accesso S3.

Important

Le policy IAM richiedono il formato Access Point ARN, non l'alias. Utilizza il formato `arn:aws:s3:region:account-id:accesspoint/access-point-name` nelle dichiarazioni relative alle risorse relative alla policy IAM. L'alias del punto di accesso (che termina con `-ext-s3alias`) viene utilizzato solo per le mappature delle home directory.

Per creare il ruolo IAM

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, scegli Ruoli, quindi scegli Crea ruolo.
3. Per Tipo di entità attendibile, scegli Servizio AWS .
4. Per Caso d'uso, scegli Trasferisci.
5. Scegli Next (Successivo).
6. Scegli Crea politica e inserisci la tua politica (vedi esempio di politica di seguito).
7. Allega la politica al ruolo e scegli Crea ruolo.

Esempio di policy IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFileOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
```

```

        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
    ],
    "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap/
object/*"
  },
  {
    "Sid": "AllowDirectoryOperations",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap"
  }
]
}

```

Gestione degli utenti per lo storage FSx

Crea utenti Transfer Family con mappature della home directory che utilizzano l'alias del punto di accesso S3.

Creazione di un utente

Quando crei un utente per lo storage FSx, usa l'alias del punto di accesso nelle mappature della home directory.

Per creare un utente Service Managed (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. Scegli il tuo server.
4. Nella sezione Utenti, scegli Aggiungi utente.
5. Per Nome utente, inserisci un nome utente.
6. Per Ruolo, scegli il ruolo IAM che hai creato.
7. Per Home directory, scegli Restricted.
8. Per i mapping della home directory, aggiungi una mappatura utilizzando l'alias del punto di accesso:

```
[{"Entry": "/", "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/jsmith"}]
```

Per creare un utente (CLI)

Utilizza il comando `create-user`. Sostituisci l'alias del punto di accesso con il tuo alias.

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings '[  
    {  
      "Entry": "/",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/  
jsmith"  
    }  
  ]'
```

Configurazione di più mappature di directory

È possibile mappare più directory virtuali su percorsi diversi sul volume FSx.

Esempio: directory separate di upload e download

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings '[  
    {  
      "Entry": "/inbox",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/  
jsmith/inbox"  
    },  
    {  
      "Entry": "/outbox",  
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/  
jsmith/outbox"  
    }  
  ]'
```

```
}  
]'
```

Configurazione dei client per il trasferimento di file

Quando si utilizzano i file system FSx con Transfer Family, è necessario configurare i client di trasferimento file per disabilitare le funzionalità non supportate.

Configurazione WinSCP

WinSCP utilizza per impostazione predefinita una funzionalità di ridenominazione temporanea che non è supportata con i punti di accesso S3 per FSx.

Warning

Se non si disattiva la funzionalità di ridenominazione temporanea in WinSCP, il caricamento dei file avrà esito negativo.

Per disabilitare la ridenominazione temporanea in WinSCP

1. Apri WinSCP.
2. Nella finestra di dialogo di accesso, scegli Modifica per modificare le impostazioni della sessione.
3. Scegli Avanzato.
4. Nella barra di navigazione a sinistra, in Trasferimento, scegli Resistenza.
5. Per Abilita il trasferimento resume/transfer al nome di file temporaneo, scegli Disabilita.
6. Scegliete OK per salvare le impostazioni.

In alternativa, puoi disabilitare questa impostazione per una sessione esistente:

1. Connect al server Transfer Family.
2. Scegli Opzioni, quindi Preferenze.
3. Scegli Trasferimento, quindi Resistenza.
4. Per Abilita il trasferimento resume/transfer al nome di file temporaneo, scegli Disabilita.
5. Scegli OK.

Altri client SFTP

Per altri client SFTP, disabilitate le seguenti funzionalità, se disponibili:

- Caricamenti temporanei di file (caricamento su file temporaneo, quindi ridenominazione)
- Riprendi i trasferimenti utilizzando file temporanei
- Caricamenti atomici utilizzando operazioni di ridenominazione
- Modalità di aggiunta per i caricamenti

Consultate la documentazione del cliente per i passaggi di configurazione specifici.

Risoluzione dei problemi di storage FSx

Questa sezione descrive come identificare e risolvere i problemi più comuni quando si utilizza Transfer Family con i file system FSx.

Problemi relativi al funzionamento dei file

Autorizzazione negata

Se ricevi errori relativi all'autorizzazione negata:

1. Verifica che il ruolo IAM disponga delle autorizzazioni corrette per l'alias del punto di accesso. Puoi farlo testando direttamente con le API S3.
2. Verifica che la policy del punto di accesso consenta il ruolo IAM.
3. Verifica che l'utente del file system disponga delle autorizzazioni sul percorso di destinazione.
4. Conferma che la mappatura della home directory utilizzi l'alias corretto del punto di accesso.

Il caricamento non riesce con WinSCP

Se il caricamento dei file fallisce con WinSCP, disabilita la ridenominazione temporanea:

1. In WinSCP, scegliete Opzioni, quindi Preferenze.
2. Scegli Transfer, quindi Endurance.
3. Per Abilita il trasferimento resume/transfer al nome di file temporaneo, scegli Disabilita.

Per ulteriori informazioni, consulta [the section called “Configurazione dei client per il trasferimento di file”](#).

Il caricamento del file non riesce

Se il caricamento dei file fallisce:

1. Verifica che la dimensione del file sia inferiore a 5 GB.
2. Verificare che il volume FSx disponga di spazio di archiviazione sufficiente.
3. Monitora le CloudWatch metriche relative alla limitazione.

App web Transfer Family

Puoi creare app Web per abilitare un'interfaccia semplice per il trasferimento di dati da e verso Amazon Simple Storage Service (S3) tramite un browser Web. Ciò non richiede la creazione o il provisioning AWS Transfer Family di server.

Prima dell'introduzione delle app web Transfer Family, gli utenti finali dovevano utilizzare una soluzione client, personalizzata o di terze parti per accedere ai propri dati in Amazon S3. Ciò era dovuto ai rigorosi requisiti di sicurezza per clienti e partner e al fatto che le app dei clienti sono difficili da utilizzare per gli utenti non tecnici.

Con il lancio delle app Web, ora puoi estendere un portale personalizzato, sicuro e ad alta disponibilità per consentire agli utenti finali di sfogliare, caricare e scaricare dati in Amazon S3. Le app Web sono integrate nativamente con AWS IAM Identity Center Amazon S3 Access Grants. Ciò significa che solo gli utenti autenticati possono visualizzare i dati a cui sono autorizzati ad accedere. Le app Web sono create utilizzando [Storage Browser per Amazon S3](#) e offrono le stesse funzionalità per l'utente finale in un'offerta completamente gestita senza dover scrivere codice o ospitare la propria applicazione.

Per ulteriori informazioni sull'altro Servizi AWS che usi con le app web Transfer Family, consulta la seguente documentazione:

- [Gestione dell'accesso con S3 Access Grants nella Guida per l'utente di Amazon Simple Storage Service](#)
- [AWS IAM Identity Center Guida per l'utente](#)
- [Workshop sulle sovvenzioni di accesso ad Amazon S3](#)
- [Annuncio di app AWS Transfer Family Web per trasferimenti di file Amazon S3 completamente gestiti](#)

Le seguenti risorse sono disponibili per aiutarti a iniziare a usare le app web Transfer Family.

- La guida per l'utente offre una procedura dettagliata e dettagliata per la configurazione di un'app web Transfer Family qui: [Tutorial: configurazione di un'app web Transfer Family di base](#)
- Il AWS Getting Started Resource Center offre un tutorial qui: Guida [introduttiva](#) all'app web. AWS Transfer Family
- Visualizza [Guida introduttiva all'app AWS Transfer Family Web](#).

Regioni AWS per le app web Transfer Family

AWS Transfer Family le app web sono disponibili in tutte le regioni supportate da Transfer Family, elencate [AWS nella Tabella](#) delle regioni, ad eccezione di Asia Pacifico (Nuova Zelanda) AWS European Sovereign Cloud e.

Gli endpoint VPC per app Web sono supportati Regioni AWS ovunque siano disponibili app Web.

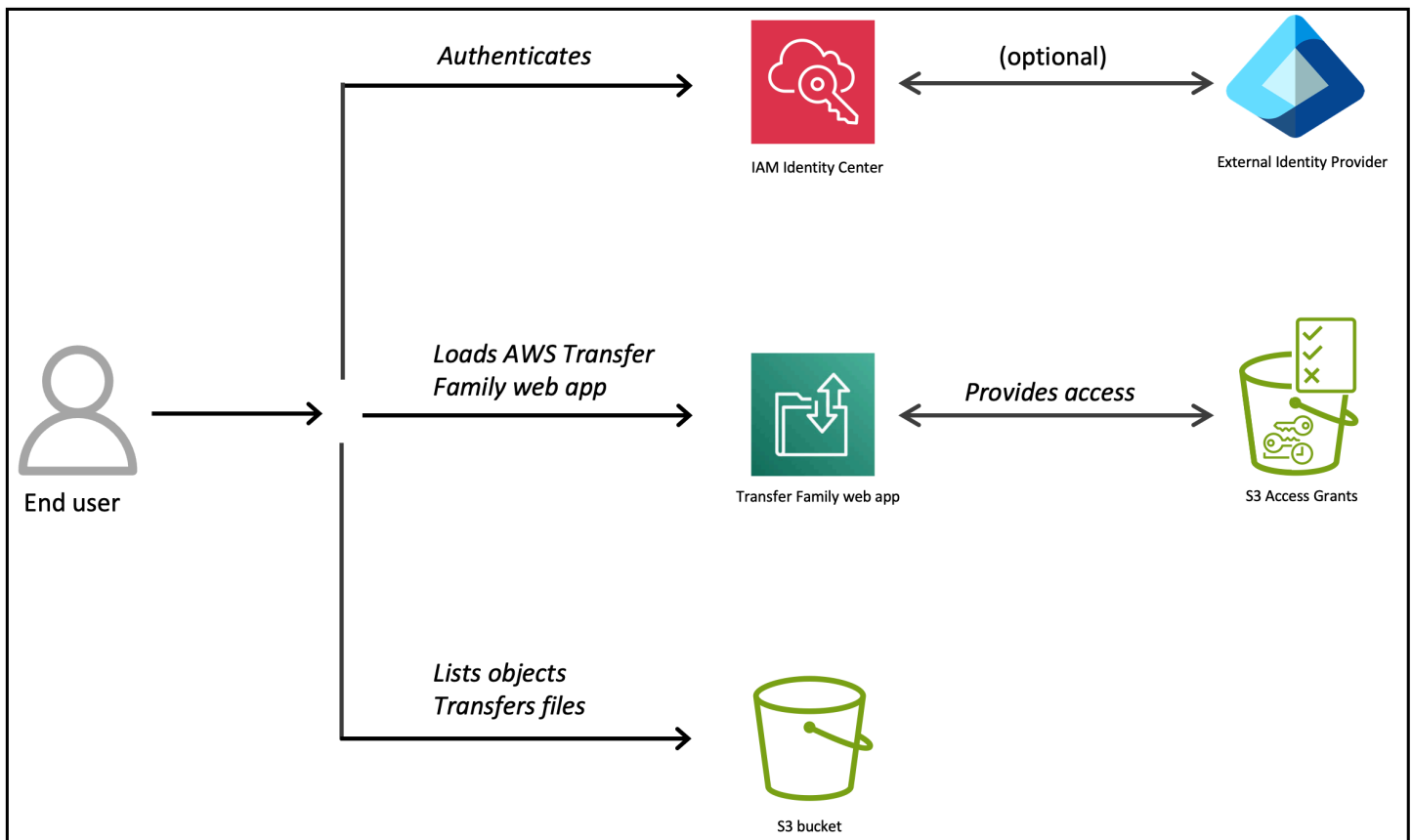
Compatibilità del browser per le app AWS Transfer Family Web

Le app web Transfer Family supportano i seguenti browser.

Browser	Versione	Compatibilità
Microsoft Edge	Ultime 3 versioni	Compatible
Mozilla Firefox	Ultime 3 versioni	Compatible
Google Chrome	Ultime 3 versioni	Compatible
Apple Safari	Ultime 3 versioni	Compatible

Come creare un'app web Transfer Family

Il diagramma seguente illustra l'architettura dell'app web Transfer Family.



In base al diagramma, puoi vedere che le app web Transfer Family interagiscono con quanto segue:

Servizi AWS

- Amazon S3 per lo storage e Amazon S3 Access Grants per l'acquisizione delle credenziali di sessione.
- AWS IAM Identity Center come provider di identità federate.
- Amazon CloudFront se configuri un URL personalizzato per la tua app web.

Tieni presente le seguenti limitazioni quando utilizzi app Web.

- Numero massimo di risultati di ricerca per query: 10.000
- I bucket Amazon S3 utilizzati dall'app web Transfer Family devono trovarsi nello stesso account dell'app Web stessa. Cross-account i bucket non sono attualmente supportati.
- Ampiezza massima di ricerca per query: 10.000 file ricercati
- Dimensione massima di caricamento per file: 160 GB (149 GiB)
- Dimensione massima del file per la copia: 5,36 GB (5 GiB)

- I nomi di cartella che iniziano o finiscono con punti (.) non sono supportati

Prerequisiti

In AWS Identity and Access Management, configura i ruoli necessari. Incolla i blocchi di codice che forniamo nelle istruzioni. Per informazioni sulla configurazione dei ruoli necessari, vedere [Configurazione dei ruoli IAM per le app web Transfer Family](#).

- Crea un ruolo di portatore di identità.
- Crea un ruolo IAM da utilizzare con S3 Access Grants. S3 Access Grants assume questo ruolo IAM per fornire credenziali temporanee al beneficiario per la sede Amazon S3 registrata.

Procedura per creare un'app web Transfer Family

Per creare la tua app web e rendere operativi gli utenti finali, esegui le seguenti attività:

1. Configura IAM Identity Center in modo che funga da provider di identità federato. Esegui le seguenti attività in IAM Identity Center. Per maggiori dettagli sulla configurazione di IAM Identity Center, consulta [Configura il tuo provider di identità per le app web Transfer Family](#).
 - a. Crea un'istanza IAM Identity Center, se non ne hai già una.
 - b. Determina la fonte della tua identità. Può essere la directory predefinita di IAM Identity Center o un provider di terze parti (ad esempio Okta).
 - c. Crea o identifica gli utenti o i gruppi che utilizzeranno la tua app web.
 - d. Se utilizzi la directory IAM Identity Center come fonte di identità, prendi nota degli ID utente o di gruppo che crei. Ne avrai bisogno in seguito quando crei una concessione di accesso utilizzando S3 Access Grants.
2. In Amazon S3, configura Amazon S3 Access Grants. Per ulteriori informazioni su S3 Access Grants, consulta [Configura Amazon S3 Access Grants per le app web Transfer Family](#).
 - Crea un'istanza S3 Access Grants se non ne hai già una. Regione AWS
 - Registra la tua posizione utilizzando il ruolo IAM.
 - Crea la concessione di accesso.
3. In Transfer Family, esegui le seguenti attività.
 - a. Crea l'app web Transfer Family. Per ulteriori informazioni su come creare l'app web Transfer Family, vedere [Configurare un'app web Transfer Family](#).

 Important

Configura la condivisione Cross-origin delle risorse (CORS) per tutti i bucket Amazon S3 utilizzati dalla tua app Web. Per informazioni sulla configurazione di CORS, consulta [Configura la condivisione Cross-origin delle risorse \(CORS\) per il tuo bucket](#)

- b. Assegnare utenti o gruppi all'app Web. Per ulteriori informazioni su come assegnare utenti e gruppi, vedere [Assegna o aggiungi utenti o gruppi a un'app web Transfer Family](#)
- c. (Facoltativo) Aggiorna l'endpoint di accesso per la tua app Web con un URL personalizzato. Per informazioni sulla creazione di un URL personalizzato, consulta [Aggiorna il tuo endpoint di accesso con un URL personalizzato](#).
- d. Fornisci agli utenti finali l'URL dell'endpoint di accesso in modo che possano accedere e interagire con la tua app web.

Configura il tuo provider di identità per le app web Transfer Family

La sezione seguente descrive come configurare il tuo provider di identità.

Per iniziare, è necessario disporre di una fonte di identità. Puoi utilizzare una directory IAM Identity Center o un provider di identità esterno. AWS Directory Service for Microsoft Active Directory Transfer Family utilizza IAM Identity Center come provider di identità federato, un sistema che archivia le credenziali degli utenti e autentica gli utenti di più organizzazioni.

Se non utilizzi una directory IAM Identity Center come fonte di identità, consulta i seguenti argomenti:

- [Gestisci un provider di identità esterno](#)
- [Connect a una directory di Microsoft AD](#)
- [Istanze di organizzazione e account di IAM Identity Center](#)
- [Tutorial sulle fonti di identità di IAM Identity Center](#)

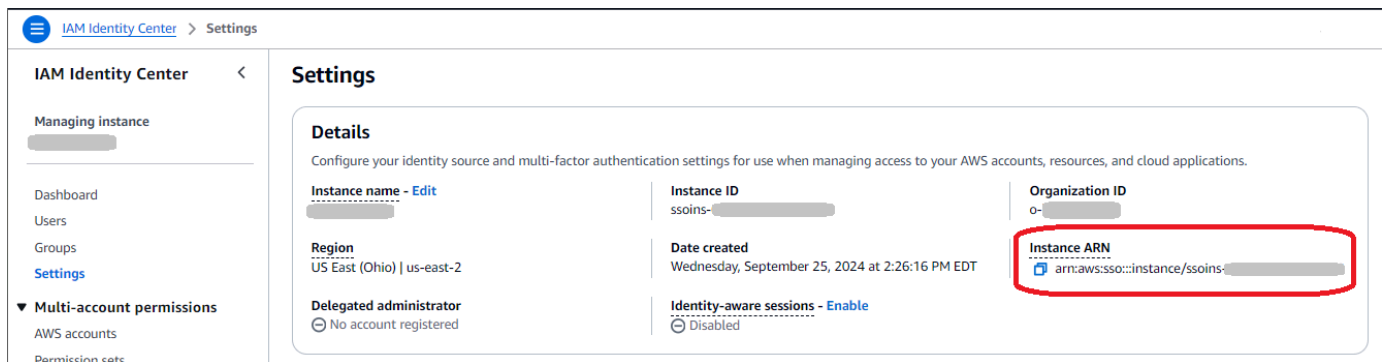
 Note

Puoi avere una sola fonte di identità in IAM Identity Center, per esempio, per. Regione AWS
Per i dettagli, consulta [Prerequisiti e considerazioni di IAM Identity Center](#).

Se prevedi di utilizzare la directory IAM Identity Center come fonte di identità e desideri una configurazione rapida, puoi saltare questo argomento e passare [Crea un'app web Transfer Family](#) alla creazione di un'istanza di IAM Identity Center dalla procedura guidata.

Per configurarlo AWS IAM Identity Center per l'uso con le app web Transfer Family

1. Accedi a Console di gestione AWS e apri la AWS IAM Identity Center console all'indirizzo <https://console.aws.amazon.com/singlesignon/>.
2. Puoi creare e utilizzare un'istanza di account o un'istanza dell'organizzazione di AWS IAM Identity Center.
 - Per informazioni dettagliate sulle istanze di account, consulta [Creare un'istanza di account di AWS IAM Identity Center](#). Con un'istanza di account di IAM Identity Center, puoi distribuire applicazioni AWS gestite supportate e applicazioni gestite dai clienti basate su OpenID Connect (OIDC). Le istanze di account supportano implementazioni isolate di applicazioni in un'unica soluzione Account AWS, sfruttando le funzionalità del portale di accesso e identità della forza lavoro di IAM Identity Center.
 - Per i dettagli sulle istanze organizzative, consulta [Organization instances of IAM Identity Center](#). Puoi gestire centralmente l'accesso di utenti e gruppi con una singola istanza organizzativa.
3. Nella pagina delle impostazioni di IAM Identity Center, annota l'ARN dell'istanza. Avrai bisogno di questo valore quando crei un'istanza Amazon S3 Access Grant.



4. Crea uno o più utenti e, facoltativamente, gruppi, da utilizzare con la tua app web Transfer Family. Se utilizzi una directory IAM Identity Center come provider di identità, puoi anche aggiungere utenti direttamente dall'app web stessa. Per ulteriori informazioni, consulta [Assegna o aggiungi utenti o gruppi a un'app web Transfer Family](#).

Configurazione dei ruoli IAM per le app web Transfer Family

Avrai bisogno di due ruoli: uno da usare come portatore di identità per la tua app web e un secondo da usare per configurare una concessione di accesso. Un ruolo di portatore di identità è un ruolo che include l'identità di un utente autenticato nelle sue sessioni. Viene utilizzato per effettuare richieste a S3 Access Grants per l'accesso ai dati per conto dell'utente.

Note

Puoi saltare la procedura per la creazione di un ruolo di portatore di identità. Per informazioni sulla creazione del ruolo di portatore di identità da parte del servizio Transfer Family, vedere [Crea un'app web Transfer Family](#).

Puoi saltare la procedura per la creazione di un ruolo di concessione di accesso. Nella procedura per la creazione di una concessione di accesso, nel passaggio in cui registri una sede S3, scegli Crea nuovo ruolo.

Crea un ruolo di portatore di identità

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Scegli Ruoli, quindi Crea ruolo.
3. Scegli Politica di fiducia personalizzata, quindi incolla il codice seguente.

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

4. Scegli Avanti, quindi salta Aggiungi autorizzazioni e seleziona nuovamente Avanti.
5. Inserisci un nome, ad esempio. `web-app-identity-bearer`
6. Scegli Crea ruolo per creare il ruolo di portatore di identità.
7. Scegli il ruolo che hai appena creato dall'elenco, quindi nel pannello Politiche di autorizzazione, scegli Aggiungi autorizzazioni > Crea politica in linea.
8. Nell'editor delle politiche, seleziona JSON e quindi incolla il seguente blocco di codice.

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

9. Per il nome della policy, inserisci `AllowS3AccessGrants`, quindi seleziona Crea policy.

Successivamente, crei il ruolo che S3 Access Grants assume per fornire credenziali temporanee all'assegnatario.

Note

Se consenti al servizio di creare per te il ruolo di portatore di identità, quel ruolo crea una confusa protezione sostitutiva. Pertanto, il suo codice è diverso da quello visualizzato qui.

Crea un ruolo per le concessioni di accesso

1. Accedi Console di gestione AWS e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Scegli Ruoli, quindi Crea ruolo. Questo ruolo dovrebbe avere l'autorizzazione ad accedere ai tuoi dati S3 in. Regione AWS

- Scegli Custom Trust Policy, quindi incolla il codice seguente.

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

- Scegli Avanti e aggiungi una politica minima come descritto in [Registrare una sede](#). Sebbene non sia consigliabile, puoi aggiungere la politica AmazonS3FullAccessgestita, che potrebbe essere troppo permissiva per le tue esigenze.
- Scegli Avanti e inserisci un nome (ad esempioaccess-grants-location).
- Scegli Crea ruolo per creare il ruolo.

Note

Se consenti al servizio di creare il ruolo Access Grants al posto tuo, quel ruolo creerà confusione nella protezione dei sostituti. Pertanto, il suo codice è diverso da quello visualizzato qui.

Configurare un'app web Transfer Family

Questa sezione descrive le procedure per creare un'app web Transfer Family. Per assegnare utenti e gruppi che possono utilizzarla, consulta [Assegna o aggiungi utenti o gruppi a un'app web Transfer Family](#).

 Note

Ripeti queste procedure per aggiungere altre app Web. Puoi riutilizzare i ruoli IAM che hai creato in precedenza. Assicurati di aggiungere gli endpoint di accesso per le nuove app Web alla policy di condivisione Cross-origin delle risorse (CORS) di ogni bucket.

Crea un'app web Transfer Family

 Note

Se non utilizzi la directory IAM Identity Center per il tuo provider di identità, non tentare di creare un'app web prima di aver già configurato IAM Identity Center e configurato un provider di identità di terze parti, come descritto in [Configura il tuo provider di identità per le app web Transfer Family](#).

Completa i seguenti passaggi per creare un'app web Transfer Family.

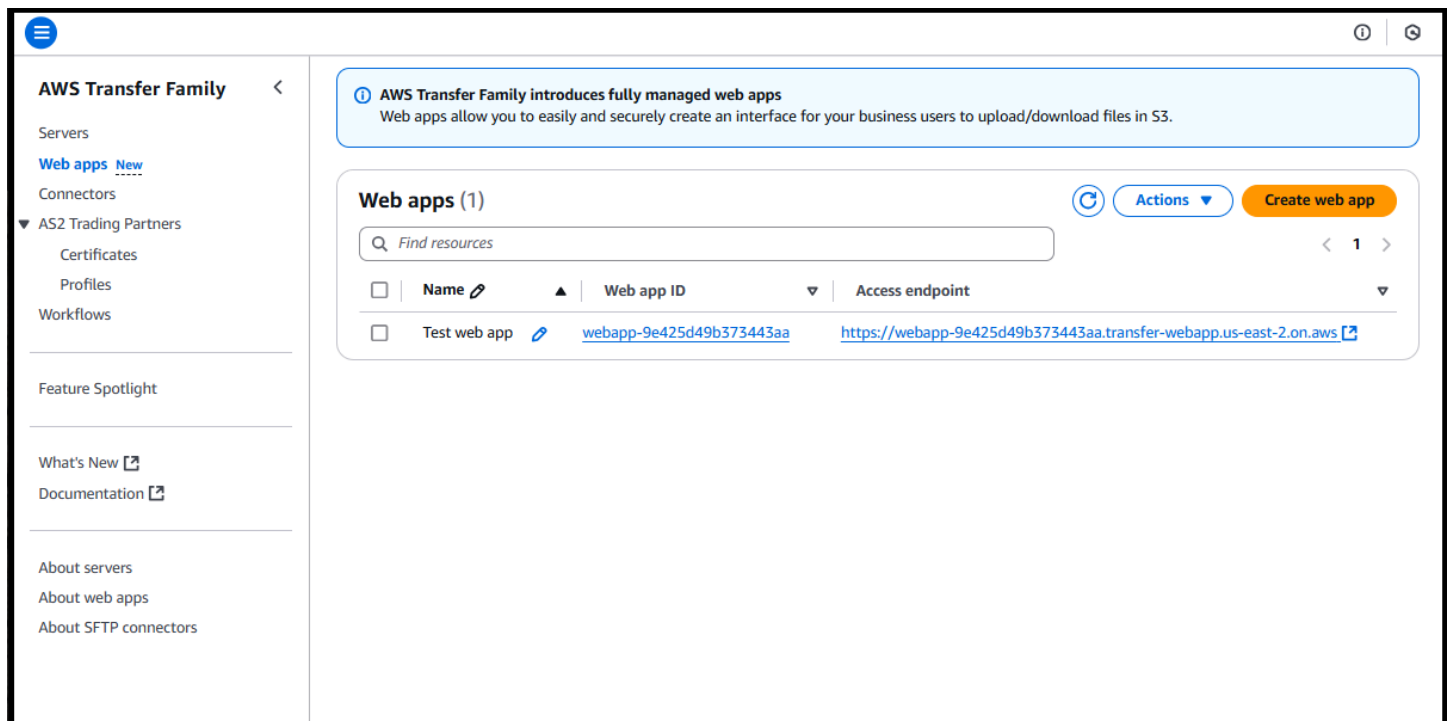
Per creare un'app web Transfer Family

1. Accedi a Console di gestione AWS e apri la AWS Transfer Family console all'indirizzo <https://console.aws.amazon.com/transfer/>.
2. Nel riquadro di navigazione a sinistra, scegli App Web.
3. Scegli Crea app web.

Per l'accesso tramite autenticazione, il riquadro viene compilato come segue.

- Se hai già creato un'organizzazione o un'istanza di account in AWS IAM Identity Center, vedrai questo messaggio: La tua AWS Transfer Family applicazione è connessa a un'istanza di account di IAM Identity Center.
 - Se disponi già di un'istanza di account e sei membro di un'istanza dell'organizzazione, hai la possibilità di scegliere a quale istanza connettere.
 - Se non disponi già di un'istanza di account o sei membro di un'istanza dell'organizzazione, ti vengono presentate le opzioni per creare un'istanza di account.
4. Per il tipo di endpoint, scegli il tipo di endpoint accessibile pubblicamente. Per un endpoint ospitato in un VPC, vedi. [Crea un'app web Transfer Family in un VPC](#)

5. Nel riquadro Tipo di autorizzazione, puoi utilizzare un ruolo creato in precedenza o fare in modo che il servizio ne crei uno automaticamente.
 - Se hai già creato un ruolo di portatore di identità, scegli Usa un ruolo esistente e scegli il tuo ruolo dal menu Seleziona un ruolo esistente.
 - Per fare in modo che il servizio crei un ruolo per te, scegli Crea e usa un nuovo ruolo di servizio.
6. Nel riquadro Unità dell'app Web, scegli un valore. Un'unità app Web consente l'attività dell'app Web da un massimo di 250 sessioni uniche. Quando si crea un'app Web, si effettua il provisioning di quante unità sono necessarie in base ai volumi di carico di lavoro di picco previsti. La modifica delle unità dell'app Web ha un impatto sulla fatturazione. Per informazioni sui prezzi, consulta [AWS Transfer Family Pricing](#).
7. Se utilizzi Transfer Family in un AWS GovCloud (US) Region, puoi selezionare la casella di controllo FIPS Enabled endpoint nel riquadro FIPS Enabled. Per tutti gli altri Regioni AWS, questa opzione non è disponibile.
8. (Facoltativo) Aggiungi un tag per aiutarti a organizzare le tue app Web. Ti suggeriamo di aggiungere un tag con Nome come chiave e un nome descrittivo come valore.
9. Scegli Next (Successivo). In questa schermata, puoi facoltativamente fornire un titolo per la tua app web. Se non fornite un titolo, viene fornito il titolo predefinito di Transfer Web App. Puoi anche caricare file di immagini per il tuo logo e la tua favicon.
10. Scegli Avanti, quindi scegli Crea app web.



Note

Assicurati di impostare una politica di condivisione Cross-origin delle risorse (CORS) per tutti i bucket a cui si accede dall'endpoint dell'app Web.

Assegnazione di indirizzi IP

Le app web Transfer Family utilizzano endpoint dual-stack, che supportano sia la connettività IPv4 che IPv6. Per l'autenticazione, vengono utilizzate app Web, che supportano anche IPv6 tramite endpoint AWS IAM Identity Center dual-stack.

Se al momento del lancio del supporto dual-stack per gli endpoint IAM Identity Center, nel tuo account erano presenti app Web in una regione, tutte le app Web di quell'account e di quella regione continuano a utilizzare l'endpoint IAM Identity Center per garantire la compatibilità con le versioni precedenti. IPv4-only Questo vale sia per le app web esistenti che per quelle appena create. Gli account che non disponevano di app Web al momento del lancio utilizzano l'endpoint dual-stack IAM Identity Center. Se devi modificare l'endpoint IAM Identity Center utilizzato dalla tua app web, contatta l'AWS assistenza.

 Note

Per determinare quale endpoint utilizza la tua app web, controlla l'URL quando vieni reindirizzato alla pagina di accesso di IAM Identity Center:

- IPv4-only: `[Region].signin.aws.amazon.com`
- Dual-stack: `[Region].sso.signin.aws`

Se la tua organizzazione utilizza firewall o gateway di rete, consenti sia gli endpoint IPv4 esistenti che i nuovi endpoint IAM Identity Center dual-stack per garantire un accesso ininterrotto indipendentemente dall'endpoint utilizzato dalle app web. Per l'elenco completo dei domini e degli endpoint URL da consentire, consulta [Aggiornare firewall e gateway per consentire l'accesso al portale di accesso nella Guida per l'utente di IAM Identity Center](#). AWS

Crea un'app web Transfer Family in un VPC

Questa sezione descrive le procedure per creare un'app web Transfer Family in un VPC. Puoi ospitare l'endpoint della tua app Web all'interno di un cloud privato virtuale (VPC) da utilizzare per il trasferimento di dati da e verso un bucket Amazon S3 senza passare dalla rete Internet pubblica. Per assegnare utenti e gruppi che possono utilizzare la tua app web, consulta [Assegna o aggiungi utenti o gruppi a un'app web Transfer Family](#)

 Note

Per garantire un flusso di dati end-to-end privato quando si utilizza un endpoint VPC dell'app Web Transfer Family, è necessario implementare tre componenti aggiuntivi. Innanzitutto, configura un PrivateLink endpoint per le operazioni dell'API Amazon S3 Control, necessario per le chiamate API Amazon S3 Access Grants. In secondo luogo, configura un endpoint per l'accesso ai dati di Amazon S3 utilizzando un endpoint Amazon PrivateLink S3 Gateway (per il traffico proveniente dal tuo VPC) o un endpoint Amazon S3 Interface (per il traffico proveniente da reti locali tramite VPN o Direct Connect). In terzo luogo, blocca l'accesso al bucket Amazon S3 aggiornando le policy del bucket per consentire solo il traffico proveniente da questi endpoint VPC. Questa combinazione garantisce che tutti i trasferimenti di dati rimangano all'interno dell'infrastruttura di rete privata e non attraversino mai la rete Internet pubblica.

Crea un'app web Transfer Family

Prerequisiti

- AWS IAM Identity Center configurato con un provider di identità configurato. Per informazioni, consulta [Configura il tuo provider di identità per le app web Transfer Family](#).
- Configurazione di VPC e componenti di rete. Vedi [Creare un VPC](#).
- Configurazione degli endpoint API per le operazioni di controllo di Amazon S3. Vedi [Accesso agli endpoint dell'interfaccia Amazon S3](#).
- Configurazione degli endpoint VPC per Amazon S3 (gateway o interfaccia). Vedi [Tipi di endpoint VPC per Amazon S3](#). Se utilizzi un endpoint di interfaccia, devi abilitare il DNS privato. Per un esempio, vedi [Introduzione al supporto DNS privato per Amazon AWS PrivateLink S3](#) con.

Note

AWS IAM Identity Center non supporta gli endpoint VPC; tutte le richieste di autenticazione transitano sulla rete Internet pubblica. Inoltre, le applicazioni web Transfer Family richiedono l'accesso a Internet per caricare contenuti statici (come JavaScript file CSS e HTML). I requisiti per l'accesso pubblico a Internet sono diversi dall'accesso ai dati. L'endpoint VPC garantisce che le connessioni vengano instradate attraverso l'infrastruttura VPC.

Per creare un'app web Transfer Family

1. Accedi a Console di gestione AWS e apri la AWS Transfer Family console all'indirizzo <https://console.aws.amazon.com/transfer/>.
2. Nel riquadro di navigazione a sinistra, scegli App Web.
3. Scegli Crea app web. Per l'accesso tramite autenticazione, il riquadro viene compilato come segue.
 - Se hai già creato un'organizzazione o un'istanza di account in AWS IAM Identity Center, vedrai questo messaggio: La tua AWS Transfer Family applicazione è connessa a un'istanza di account di IAM Identity Center.
 - Se disponi già di un'istanza di account e sei membro di un'istanza dell'organizzazione, hai la possibilità di scegliere a quale istanza connettere.

- Se non disponi già di un'istanza di account o sei membro di un'istanza dell'organizzazione, ti vengono presentate le opzioni per creare un'istanza di account.
4. Nella sezione Configurazione degli endpoint, scegli in che modo gli utenti accederanno alla tua app web:
- **Accessibile pubblicamente:** l'endpoint dell'app Web è accessibile al pubblico tramite HTTPS. Questa opzione non richiede alcuna configurazione VPC, il che la rende semplice da configurare e adatta ad applicazioni destinate a un ampio uso pubblico.
 - **Ospitato su VPC:** l'endpoint dell'app Web è ospitato all'interno del Virtual Private Cloud (VPC), che fornisce l'accesso alla rete privata tramite la rete VPC o le connessioni VPN. AWS Direct Connect Questa opzione offre una maggiore sicurezza grazie all'isolamento della rete ed è consigliata per le applicazioni interne.

Quando configuri un endpoint ospitato da un VPC, devi specificare:

- **VPC:** seleziona un VPC esistente o creane uno nuovo. È disponibile il pulsante Crea un VPC.
- **Zone di disponibilità:** scegli le zone di disponibilità in cui verrà distribuito l'endpoint.
- **Sottoreti:** seleziona le sottoreti all'interno di ciascuna zona di disponibilità scelta.
- **Gruppi di sicurezza:** seleziona o crea gruppi di sicurezza per controllare l'accesso in base agli indirizzi IP di origine. Se non specificato, viene utilizzato il gruppo di sicurezza predefinito del VPC. Gestisci i gruppi di sicurezza tramite la console VPC. Configura i gruppi di sicurezza VPC per consentire il traffico in entrata dalla rete tramite HTTPS sulla porta TCP 443. Ciò è necessario per l'autenticazione IAM Identity Center e il caricamento dei contenuti statici delle app Web.

Note

L'endpoint di accesso non può essere personalizzato per gli endpoint VPC. Per aggiungere un URL personalizzato, utilizza l'endpoint pubblico.

Post-creation passaggi

- Assicurati di impostare una politica di condivisione Cross-origin delle risorse (CORS) per tutti i bucket a cui si accede dall'endpoint dell'app Web. Per informazioni, consulta [Cross-origin politica di condivisione delle risorse \(CORS\)](#).

- Aggiorna la tua policy sui bucket per consentire solo il traffico proveniente dal tuo VPC attraverso l'endpoint VPC. Per informazioni, consulta [Limitazione dell'accesso a un endpoint VPC specifico](#).
- Assegna o aggiungi utenti o gruppi all'app web Transfer Family. Per informazioni, consulta [Assegna o aggiungi utenti o gruppi a un'app web Transfer Family](#).

Cross-origin politica di condivisione delle risorse (CORS)

È necessario configurare la condivisione delle risorse tra le origini (CORS) per tutti i bucket utilizzati dall'app Web. Per ulteriori informazioni sulla funzionalità CORS, consulta [Configura la condivisione Cross-origin delle risorse \(CORS\) per il tuo bucket](#).

Important

Prima di utilizzare la seguente politica di esempio, sostituisci Allowed Origin con il tuo endpoint di accesso. In caso contrario, gli utenti finali riceveranno un errore quando tentano di accedere a una posizione sulla tua app web.

Esempio di politica:

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://vpce-1234567-example.vpce-mq.transfer-webapp.us-east-1.on.aws"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
```

```

    "content-type",
    "x-amz-request-id",
    "x-amz-id-2",
    "date",
    "x-amz-cf-id",
    "x-amz-storage-class",
    "access-control-expose-headers"
  ],
  "MaxAgeSeconds": 3000
}
]
```

Limitazione dell'accesso a un endpoint VPC specifico

Di seguito è riportato un esempio di policy del bucket Amazon S3 che limita l'accesso a un bucket specifico, `amzn-s3-demo-bucket`, solo dall'endpoint VPC con l'ID `vpce-1a2b3c4d`. Se l'endpoint specificato non viene utilizzato, la policy nega l'accesso al bucket. La condizione `aws:SourceVpce` specifica l'endpoint. La condizione `aws:SourceVpce` non richiede un ARN per la risorsa dell'endpoint VPC, ma solo l'ID dell'endpoint VPC. Per ulteriori informazioni sull'aggiornamento della policy del bucket per consentire solo il traffico proveniente dal tuo VPC, consulta [Controllare l'accesso dagli endpoint VPC con le policy dei bucket](#). Per ulteriori informazioni sull'utilizzo delle condizioni in una policy, consulta [Esempi di policy Bucket](#) che utilizzano le chiavi di condizione. Come prerequisito per l'applicazione di questa policy, è necessario creare un endpoint VPC [Amazon S3](#).

Important

Prima di utilizzare la policy di esempio seguente, sostituire l'ID endpoint VPC con un valore appropriato per il caso d'uso. In caso contrario, non sarà possibile accedere al bucket.

```

{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket",
```



```
        "arn:aws:s3:::amzn-s3-demo-bucket/*"],
    "Condition": {
        "StringNotEquals": {
            "aws:SourceVpce": "vpce-1a2b3c4d"
        }
    }
}
```

Assegna o aggiungi utenti o gruppi a un'app web Transfer Family

Dopo aver creato un'app web Transfer Family, puoi assegnare utenti e gruppi che possono quindi accedere all'app web. Puoi recuperare gli utenti già creati e archiviati in IAM Identity Center oppure [aggiungere direttamente nuovi utenti](#) (se utilizzi una directory IAM Identity Center come provider di identità). Se aggiungi nuovi utenti, questi vengono aggiunti anche alla tua istanza IAM Identity Center.

Tenere presente quanto segue:

- Puoi aggiungere nuovi utenti solo se utilizzi la directory IAM Identity Center come fonte di identità e disponi delle autorizzazioni appropriate. Se sei membro di un'istanza dell'organizzazione, potresti non disporre delle autorizzazioni necessarie per aggiungere utenti.

Note

Se non assegni utenti o gruppi alla tua applicazione, gli utenti riceveranno un errore quando tentano di accedere alla tua app web.

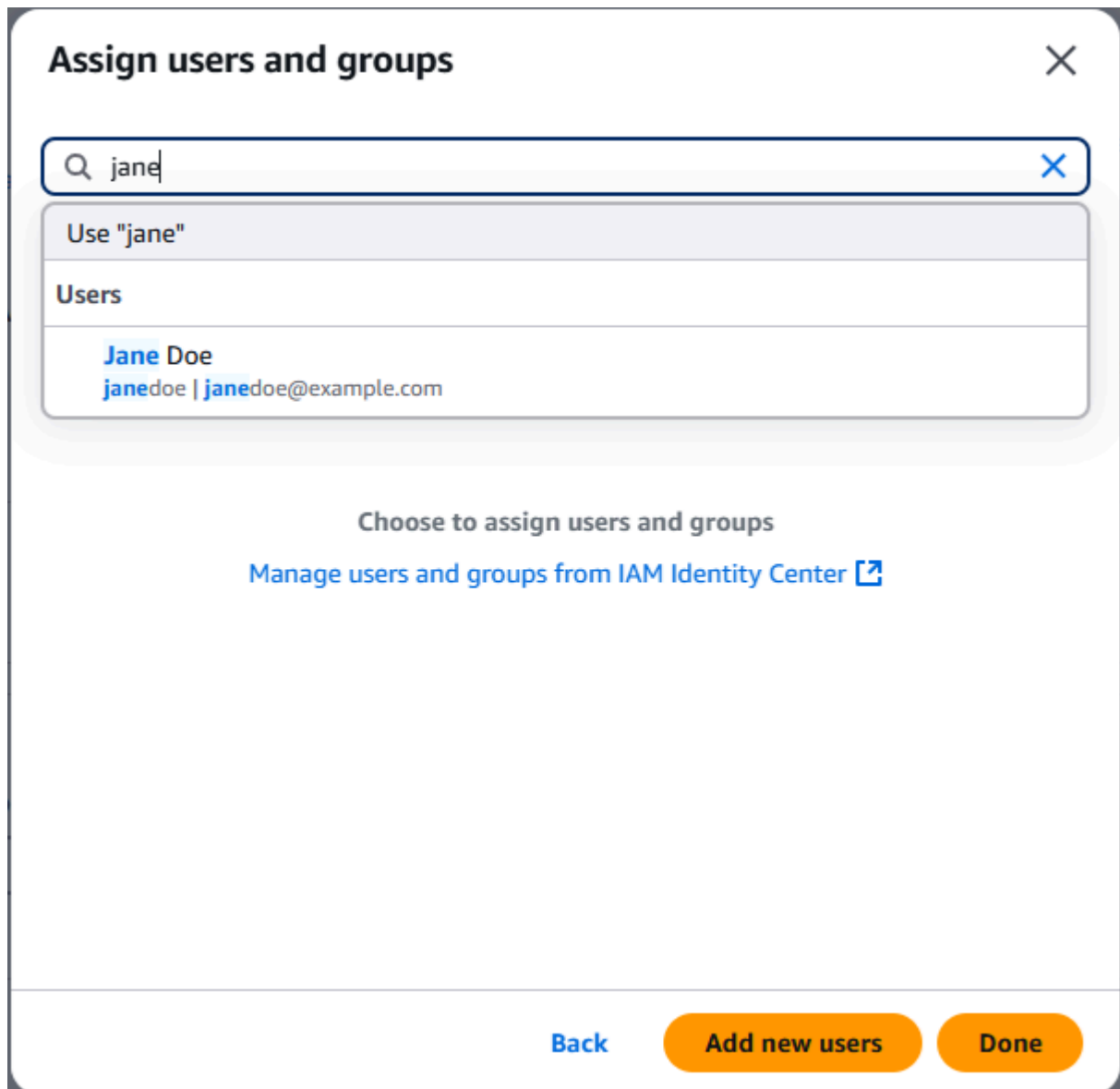
- Se crei un nuovo utente, devi anche creare una concessione di accesso S3 per questo utente in modo che possa accedere ai dati sulla tua app web.
- Dopo aver creato un nuovo utente, quell'utente riceve un'e-mail di onboarding da IAM Identity Center con le istruzioni su come procedere.

Per assegnare utenti a un'app web Transfer Family

1. Vai all'elenco delle tue app web e scegli quella che desideri modificare.
2. Seleziona Assegna utenti e gruppi.

The screenshot shows the AWS IAM console interface for a web application. At the top, there's a header with the web app name 'webapp-' and three buttons: 'Assign users and groups' (orange), 'Clear customization', and 'Delete'. Below this is the 'Web app details' section, which includes an 'Access endpoint' (a URL to the transfer-webapp.us-east-2.on.aws endpoint), a 'Web app endpoint' (a URL to the webapp.us-east-2.on.aws endpoint), and 'Web app units' (1). To the right of these details are the 'Identity provider' (AWS IAM Identity Center), 'IAM role', and 'Instance ARN'. Below the details section, there are two tabs: 'Users' (selected) and 'Groups'. The 'Users' tab shows a list of two users. Each user entry includes a checkbox, a 'Display name', a 'User ID', and a 'Username'. The first user has a display name of 'user1', a user ID of 'user1', and a username of 'user1'. The second user has a display name of 'user2', a user ID of 'user2', and a username of 'user2'. There is a search bar at the top of the user list with the placeholder text 'Find resources'. A 'Delete' button is visible in the top right corner of the user list section.

3. Per assegnare gli utenti che hai creato in precedenza in IAM Identity Center, seleziona Assegna utenti e gruppi esistenti. Per creare nuovi utenti, vai avanti al passaggio 4.
 - a. Viene visualizzata una schermata informativa. Scegli Get started (Nozioni di base) per continuare.
 - b. Cerca l'utente. Tieni presente che nessun utente viene visualizzato finché non inizi a inserire i criteri di ricerca. È necessario eseguire la ricerca in base al nome visualizzato, non al nome utente, se diverso. Vengono restituite solo le corrispondenze esatte. Se non riesci a trovare il tuo utente, accedi alla console di gestione IAM Identity Center, trova l'utente, quindi copia e incolla il nome visualizzato qui.



- c. Scegli gli utenti e i gruppi da aggiungere, quindi scegli Assegna.
4. Per creare un nuovo utente, seleziona Aggiungi e assegna nuovi utenti.
 - a. Viene visualizzata una schermata informativa. Scegli Get started (Nozioni di base) per continuare.
 - b. Scegli Add new users (Aggiungi nuovi utenti).
 - c. Immettete i seguenti dati utente nella finestra di dialogo: nome utente, nome e cognome e un indirizzo e-mail.

Add new users ✕

i Newly-created users are enabled by default. To grant them access to Add User Widget, you must set their password in the IAM Identity Center console. [Manage user passwords in the IAM Identity Center console](#) ↗ ✕

Username
A username is required for this person to sign in to the AWS access portal. You can't change the username later.

johnstiles

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: + = , . @ - _

First name **Last name**

John Stiles

Email address **Confirm email address**

johnstiles@example.com johnstiles@example.com

Display name
This is typically the full name of the user (first and last name) and appears in the users list.

John Stiles

Cancel Next

- d. Scegli Avanti, quindi scegli Aggiungi per aggiungere l'utente e chiudere la finestra di dialogo oppure Aggiungi nuovo utente per creare un altro utente.

Configura la condivisione Cross-origin delle risorse (CORS) per il tuo bucket

È necessario configurare la condivisione delle risorse tra le origini (CORS) per tutti i bucket utilizzati dall'app Web. Una configurazione CORS è un documento che definisce le regole che identificano le origini a cui consentirai l'accesso al tuo bucket. Per ulteriori informazioni su CORS, vedere [Configuring cross-origin resource sharing \(CORS\)](#).

 Important

Se non configurate CORS, gli utenti finali ricevono un errore quando tentano di accedere a una posizione sulla vostra app web.

Per configurare la condivisione Cross-origin delle risorse (CORS) per il tuo bucket Amazon S3

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Scegli Bucket dal pannello di navigazione a sinistra e cerca il tuo bucket nella finestra di dialogo di ricerca, quindi scegli la scheda Autorizzazioni.
3. Nella condivisione Cross-origin delle risorse (CORS), scegli Modifica e incolla il codice seguente. **WebAppEndpoint** Sostituiscilo con l'effettivo endpoint di accesso per la tua app web. Può trattarsi dell'endpoint ospitato in VPC o ad accesso pubblico creato al momento della creazione dell'app Web o di un endpoint di accesso personalizzato, se ne crei uno. Assicurati di non inserire barre finali, perché così facendo si generano errori quando gli utenti tentano di accedere alla tua app web.
 - Esempio errato: `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Esempi corretti:
 - `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`
 - `https://vpce-05668789767a-fh45z079.vpce-mq.transfer-webapp.us-east-1.on.aws`

Se stai riutilizzando un bucket per più app Web, aggiungi i relativi endpoint all'elenco.

AllowedOrigins

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
```

```
    "HEAD",
  ],
  "AllowedOrigins": [
    "https://WebAppEndpoint"
  ],
  "ExposeHeaders": [
    "last-modified",
    "content-length",
    "etag",
    "x-amz-version-id",
    "content-type",
    "x-amz-request-id",
    "x-amz-id-2",
    "date",
    "x-amz-cf-id",
    "x-amz-storage-class",
    "access-control-expose-headers"
  ],
  "MaxAgeSeconds": 3000
}
]
```

4. Scegliete Salva modifiche per aggiornare il CORS.

Per testare la configurazione CORS, consulta [Testare CORS](#).

Configura Amazon S3 Access Grants per le app web Transfer Family

Questo argomento descrive come aggiungere una concessione di accesso utilizzando Amazon S3 Access Grants. Questa concessione di accesso definisce l'accesso ai dati direttamente agli utenti e ai gruppi presenti nella directory aziendale e fornisce credenziali temporanee tempestive, con privilegi minimi e basate sulle concessioni. Una concessione individuale in un'istanza S3 Access Grants consente a un utente o gruppo specifico in una directory aziendale di ottenere l'accesso da una posizione registrata nella tua istanza S3 Access Grants. Per ulteriori dettagli, consulta i [concetti di S3 Access Grants](#) nella Amazon S3 User Guide.

 Note

Non puoi utilizzare la directory IAM Identity Center con S3 Access Grants se non con le app web Transfer Family.

È necessario specificare una concessione di accesso ad Amazon S3 per la propagazione delle identità. Una concessione di accesso ad Amazon S3 archivia i dati a cui gli utenti finali devono accedere. Quando i tuoi utenti finali accedono alla tua app web Transfer Family, S3 Access Grants trasmette l'identità dell'utente all'applicazione affidabile. Questa sezione descrive come aggiungere e configurare un'istanza di concessione di accesso Amazon S3 e quindi una concessione di accesso per un bucket Amazon S3.

 Note

Tieni a portata di mano l'[ARN e l'ID utente o di gruppo dell'istanza di IAM Identity Center](#), poiché ti servono per completare la configurazione della concessione di accesso.

Per creare una sovvenzione utilizzando Amazon S3 Access Grants

1. Accedi a Console di gestione AWS e apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Crea un bucket o prendi nota di un bucket esistente da utilizzare con la tua app web. Per informazioni sulla creazione di bucket, consulta la [Amazon S3](#) User Guide.
3. Dal riquadro di navigazione a sinistra, scegli Access Grants.
4. Scegli Crea un'istanza S3 Access Grants e fornisci le seguenti informazioni.
 - Seleziona Aggiungi istanza IAM Identity Center in **your-Region** cui si **your-Region** trova la tua. Regione AWS Tieni deselezionata questa casella se non utilizzi IAM Identity Center come provider di identità.
 - Incolla l'ARN dell'istanza di IAM Identity Center.

[Amazon S3](#) > [Access Grants](#) > Set up Access Grants Instance

- Step 1
☒ **Create S3 Access Grants instance**
- Step 2
☐ Register S3 Buckets or prefixes as locations
- Step 3
☐ Create grant
- Step 4
☐ Review and finish

Create S3 Access Grants instance [Info](#)

When you create your S3 Access Grants instance, you can use identities from your corporate directory or you can use IAM users and roles. This Access Grants instance serves as the container for your individual grants.

S3 Access Grants instance [Info](#)

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

☒ Add IAM Identity Center instance in US East (Ohio) us-east-2 - *optional*

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

IAM Identity Center instance ARN

You can find the IAM Identity Center instance ARN in the [IAM Identity Center console](#).

arn:aws:sso::instance/ssoin-

Format: arn:aws:sso::instance/<instanceIdentifier>

Seleziona Successivo per continuare.

- Registra i bucket o i prefissi S3 come posizioni. Ti consigliamo di registrare la posizione predefinita e di s3:// mapparla a un ruolo IAM. La posizione in questo percorso predefinito copre l'accesso a tutti i bucket Amazon S3 presenti nel Regione AWS tuo account. Quando crei una concessione di accesso, puoi restringere l'ambito a un bucket, un prefisso o un oggetto all'interno della posizione predefinita.

Inserisci le informazioni che seguono.

- Per l'ambito, cerca un bucket o inserisci il nome del tuo bucket e, facoltativamente, un prefisso.
- Per il ruolo IAM, scegli Crea nuovo ruolo per fare in modo che il servizio crei un ruolo.

In alternativa, puoi creare tu stesso il ruolo, come descritto in [Configurazione dei ruoli IAM per le app web Transfer Family](#), e quindi inserire il relativo ARN qui.

Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Register location

Register location [Info](#)

Registering a location for S3 your S3 Access Grants instance assigns an IAM role the permission to get temporary credentials to access resources within the specified scope.

Location [Info](#)

Location scope [Info](#)

You can't edit the location scope after registering the location.

Scope

[View](#) [Browse S3](#)

Format for all buckets: s3://
Format for bucket: s3://<bucket>
Format for prefix: s3://<bucket>/<prefix-with-path>

Permissions

This IAM role allows S3 Access Grants to access your specified location scope.

[To ensure the role has proper permissions to access the location scope, consult the \[list of permissions\]\(#\).](#)

IAM role [Info](#)

This IAM role allows S3 Access Grants to access your specified location scope.

☒ Create new role
☐ Choose from existing IAM roles
☐ Enter IAM role ARN

[Cancel](#) [Register location](#)

Seleziona Successivo per continuare.

6. Nella schermata Create Grant, fornisci i seguenti dettagli.

- Per Autorizzazioni, seleziona Lettura e scrittura. Le autorizzazioni di concessione di accesso possono essere di sola lettura o di lettura e scrittura, ma la sola scrittura non è supportata.
- Per il tipo di beneficiario, scegli Directory identity da IAM Identity Center.
- Per il tipo di identità Directory, seleziona Utente o Gruppo, a seconda del tipo che desideri registrare ora.
- In IAM Identity Center user/group ID, incolla l'ID del tuo utente o gruppo. Questo ID è disponibile nella console IAM Identity Center e nell'app web Transfer Family nella tabella utenti e gruppi.

Create Grant [Info](#)**Grant** [Info](#)

Grant a user or role a specific level of access to your S3 data.

Grant scope

The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location

s3://test

Location ID [Info](#)**IAM role** [Info](#)

[web-app-access-grants](#)

[Browse locations](#)

[Register location](#)

Subprefix - optional [Info](#)

Further scope the grant to a bucket, prefix, or an individual object.

*

Don't include any part of the grant already specified in the location.

Format for bucket: <bucket>/*

Format for prefix: <bucket>/<prefix-with-path>*

Format for object: <bucket>/<prefix-with-path>/<object>

Grant scope [Info](#)

s3://test/*

☐ The grant scope is an object

Permissions and access

Grant a user or role a specific level of access to your S3 data.

 The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions

☒ Read

☒ Write

Grantee type [Info](#)

☒ Directory identity from IAM Identity Center

☐ IAM principal

Directory identity type [Info](#)

☒ User

☐ Group

IAM Identity Center user ID [Info](#)

The user that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#)

Format: a1b2c3d4-5678-90ab-cdef-EXAMPLE1111

► **Application - optional**

Scegli Next (Successivo).

- Controlla le impostazioni sullo schermo. Se tutto è corretto, scegli Fine per creare la concessione di accesso. In alternativa, puoi scegliere Annulla o Precedente per apportare modifiche.

- Step 1
- Create S3 Access Grants instance
- Step 2
- Register S3 Buckets or prefixes as locations
- Step 3
- Create grant
- Step 4
- Review and finish

Review and finish

Step 1 - Create S3 Access Grants instance

S3 Access Grants instance

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

arn:aws:sso:::application/ssoins:/apl

Successfully created S3 Access Grants instance

Instance ARN: arn:aws:s3:us-east-2:::access-grants/default

You can grant other accounts access to this S3 Access Grants instance in the Resource Access Management console

Step 2 - Register S3 buckets or prefixes as locations

Location

Location scope

s3://

IAM role

web-app-beta-access-grants

Successfully registered location

Location ID:

Step 3 - Create grants

Grant

Grant a user or role a specific level of access to your S3 data.

Grant scope

s3:///*

IAM role

web-app-beta-access-grants

Location ID

Permissions and access

Access Type

READWRITE

Grantee type

Directory identity user

Grantee ID

Application - optional

Successfully created grant

Grant ARN: arn:aws:s3:us-east-2:::access-grants/default/grant/

Create another grant

Cancel

Previous

Finish

Configurazione delle concessioni di accesso ad Amazon S3

312

Amazon S3 > Access Grants > US East (Ohio) us-east-2: default

US East (Ohio) us-east-2: default

Share InstanceDelete Instance

S3 Access Grants provides scalable access control to data sets in your S3 buckets. To share an S3 Access Grants instance with external accounts by using the AWS Resource Access Manager console, choose Share instance. With S3 Access Grants, you can use identities from your corporate directory or from AWS Identity and Access Management (IAM) to control access. You can create one S3 Access Grants instance per AWS Region per account.

S3 Access Grants instance overview

Amazon Resource Name (ARN)

arn:aws:s3:us-east-2:access-grants/default

Creation date

October 25, 2024, 11:50:11 (UTC-04:00)

Account ID

IAM Identity Center

DeregisterAdd

IAM Identity Center instance ARN

arn:aws:sso:application/ssoins/apl-

GrantsLocations

Grants (1)

DeleteCreate Grant

Find by grant scope or grantee

Grant scope	Grant ID	Permission	Grantee type	Grantee ID	Creation date	Location ID	Application ARN
s3:///*		Read, Write	Directory identity user		October 25, 2024, 11:57:30 (UTC-04:00)		ALL

Questo completa la configurazione della tua app web. Gli utenti e i gruppi che hai configurato possono visitare l'app Web dal punto di accesso, accedere e caricare e scaricare file.

Aggiorna il tuo endpoint di accesso con un URL personalizzato

L'endpoint di accesso predefinito creato con la tua app web contiene identificatori generati dal servizio. Per offrire un'esperienza personalizzata, potresti voler fornire un URL personalizzato per consentire agli utenti di accedere alla tua app web Transfer Family. Questo argomento descrive come aggiornare l'endpoint di accesso con un URL personalizzato.

Note

L'endpoint di accesso non può essere personalizzato per gli endpoint VPC. Per aggiungere un URL personalizzato, utilizza l'endpoint pubblico.

Note

La procedura seguente si basa sull'utilizzo del modello di [CloudFormation stack](#) consigliato. Non è necessario utilizzare il modello: è possibile creare la distribuzione utilizzando direttamente la [CloudFront console](#).

Usa un URL personalizzato

313

Tuttavia, il modello fornito semplifica il processo e facilita l'eliminazione di errori di configurazione. Se non utilizzi il CloudFormation modello, assicurati di seguire queste linee guida:

- La [policy di richiesta Origin](#) dovrebbe inoltrare le stringhe di query e i cookie all'origine e non dovrebbe inoltrare l'Host intestazione all'origine.
- La [politica Cache](#) non deve includere l'Host intestazione nella chiave della cache.

Per personalizzare l'URL della tua app web

1. Crea una CloudFront distribuzione utilizzando il modello [CloudFormation stack AWS CloudFormation template](#) fornito da Transfer Family.
 - a. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
 - b. Scegli Crea pila e specifica quanto segue.
 - Nella sezione Prerequisito - Prepara modello, scegli Scegli un modello esistente.
 - Nella sezione Specify template (Specifica il modello) scegliere Upload a template file (Carica un file modello).
 - Salva il file del [modello CloudFormation dello stack](#), quindi caricalo qui.
 - c. Scegli Avanti e fornisci le seguenti informazioni.
 - WebAppEndpoint: copia il valore dalla tua app web
 - AccessEndpoint: fornisci il nome di dominio personalizzato che desideri utilizzare
 - AcmCertificateArn: fornisce l'ARN per un SSL/TLS certificato pubblico o privato archiviato in AWS Certificate Manager
 - d. Completa la CloudFormation procedura guidata fino alla creazione del nuovo stack.
2. Nella tua app web, modifica l'endpoint di Access, aggiornando l'URL personalizzato all'URL che desideri utilizzare.

Transfer Family > Web apps > webapp- > Edit web app details

Edit web app details

Authentication access [Info](#)

Connect or create an Identity Center instance

Instance ARN

Select your instance ARN

Permission type [Info](#)

Create and use a new service role

Create and use an IAM role to allow the service to access the AWS resource it needs to create your application

Use an existing role

Use an existing IAM role to allow the service to access the AWS resources it needs to create your application

By selecting use existing role, you need to manually create an IAM Role in order for the Transfer Family web application to access your AWS services data. Please select an existing IAM role below or [create a new role in IAM console](#)

Select an existing role

If your newly created role is not showing up in the dropdown list, please try the refresh button on the right

Find your IAM role

Make sure you have attached the trust policy and permission policy to the role you selected.

[learn more about required policies](#)

Access endpoint [Info](#)

Map your own fully qualified domain name to this web app so your end users can use your custom URL, not the service-provided URL to access your web app. Note- you can only complete this step in CloudFront after you have created the web app.

Custom URL

<https://my-custom-url>

[Create a new distribution](#)

3. Crea record DNS per indirizzare il traffico dal tuo nome di dominio personalizzato alla CloudFront distribuzione. Se utilizzi Route 53 per la zona, puoi creare un alias o un record CNAME per il nome della CloudFront distribuzione (ad esempio, xxxx.cloudfront.net). Per informazioni sull'utilizzo di Amazon Route 53 con CloudFront, consulta [Configurazione di Amazon Route 53 per instradare il traffico verso una CloudFront distribuzione](#).
4. Aggiorna la tua politica di condivisione delle risorse tra origini sostituendo l'endpoint di accesso predefinito con la seguente riga nel AllowedOrigins blocco di codice:

```
"https://custom-url"
```

Devi apportare questa modifica per ogni bucket utilizzato dalla tua app web.

Dopo aver effettuato l'aggiornamento, la AllowedOrigins sezione della politica CORS dovrebbe avere il seguente aspetto:

```
"AllowedOrigins": [
  "https://custom-url",
```

È necessario un solo AllowedOrigins ingresso per ogni app web Transfer Family.

Per ulteriori dettagli, consulta la procedura di [configurazione della condivisione Cross-origin delle risorse \(CORS\) per il bucket Amazon S3](#).

Ora puoi visitare il tuo endpoint di accesso personalizzato e condividere questo link con i tuoi utenti finali.

CloudTrail registrazione per le app web Transfer Family

CloudTrail è un file Servizio AWS che crea un registro delle azioni intraprese all'interno del tuo Account AWS. Monitora e registra continuamente le operazioni API per attività come AWS Command Line Interface accessi, comandi e operazioni alla console. 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' AWS ambiente.

Per le app web Transfer Family, puoi tenere traccia sia degli eventi di autenticazione che delle operazioni di accesso ai dati eseguite dai tuoi utenti. Per abilitare la registrazione completa, devi:

1. CloudTrail Configurare per registrare gli eventi di gestione per il monitoraggio delle attività di autenticazione.
2. Abilita gli eventi sui dati di Amazon S3 per tenere traccia delle operazioni sui file eseguite tramite la tua app web.

Consulta anche

- [CloudTrail casi d'uso per IAM Identity Center](#)
- [Comprensione degli eventi di accesso a IAM Identity Center](#)
- [CloudTrail elemento userIdentity](#)
- [Abilitazione della registrazione CloudTrail degli eventi per bucket e oggetti S3](#)
- [Eventi Amazon S3 CloudTrail](#)

Abilitazione degli eventi relativi ai dati di Amazon S3

Per tenere traccia delle operazioni sui file eseguite tramite le app web Transfer Family sui tuoi bucket Amazon S3, devi abilitare gli eventi relativi ai dati per tali bucket. Gli eventi relativi ai dati forniscono

attività API a livello di oggetto e sono particolarmente utili per tenere traccia dei caricamenti, dei download e di altre operazioni eseguite dagli utenti delle app Web.

Per abilitare gli eventi dati Amazon S3 per la tua app web Transfer Family:

1. Apri la CloudTrail console all'indirizzo <https://console.aws.amazon.com/cloudtrail/>.
2. Nel riquadro di navigazione, scegli Percorsi, quindi seleziona un percorso esistente o creane uno nuovo.
3. In Selettori di eventi avanzati, scegli Modifica.
4. Scegli Aggiungi selettore di eventi avanzato.
5. Per il primo selettore di campo:
 - Imposta campo su `eventCategory`
 - Imposta operatore su Uguale
 - Imposta valore su `Data`
6. Scegli Aggiungi campo e per il secondo selettore di campo:
 - Imposta campo su `resources.type`
 - Imposta operatore su Uguale
 - Imposta valore su `AWS::S3::Object`
7. (Facoltativo) Per registrare gli eventi solo per bucket specifici, scegli Aggiungi campo e aggiungi:
 - Imposta campo su `resources.ARN`
 - Imposta operatore con cui iniziare
 - Imposta valore su `arn:aws:s3:::your-bucket-name/`
8. Scegli Save changes (Salva modifiche).

In alternativa, puoi utilizzare la configurazione degli eventi relativi ai dati precedenti:

1. In Data events, scegli Modifica.
2. Per Tipo di evento Data, seleziona Bucket S3 e Object Events.
3. Scegli i bucket Amazon S3 per cui registrare gli eventi relativi ai dati. Puoi selezionare Tutti i bucket S3 attuali e futuri o specificare singoli bucket.
4. Scegli se registrare gli eventi di lettura, gli eventi di scrittura o entrambi.
5. Scegli Save changes (Salva modifiche).

Dopo aver abilitato gli eventi relativi ai dati, puoi accedere a questi log nel bucket Amazon S3 configurato per CloudTrail. I log includono dettagli come l'utente che ha eseguito l'azione, il timestamp dell'azione, l'oggetto specifico interessato e il `onBehalfOf` campo che aiuta a tracciare le azioni eseguite tramite le `userId` app web Transfer Family.

Individuazione e visualizzazione dei registri

Esistono diversi modi per trovare e visualizzare CloudTrail i registri della tua app web Transfer Family:

Utilizzo della console CloudTrail

Il modo più veloce per visualizzare gli eventi recenti:

1. Apri la CloudTrail console all'indirizzo <https://console.aws.amazon.com/cloudtrail/>.
2. Scegli Cronologia eventi.
3. Filtra gli eventi per:
 - Fonte dell'evento: `signin.amazonaws.com` per gli eventi delle app Web
 - Fonte dell'evento: `s3.amazonaws.com` per le operazioni sui file
4. Fai clic su un evento per visualizzare informazioni dettagliate.

Accesso ai log in Amazon S3

Per accedere ai file di log completi archiviati in Amazon S3:

1. Identifica il CloudTrail bucket Amazon S3 del tuo percorso:

```
aws cloudtrail describe-trails --query 'trailList[*].[Name,S3BucketName]' --output table
```

2. Accedi ai file di registro in Amazon S3:

```
aws s3 ls s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/
```

3. Scarica e cerca nei file di registro l'ID della tua app web:

```
aws s3 cp s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/ . --recursive
```

```
gunzip *.json.gz
grep -l "webapp-1a2b3c4d5e6f7g8h9" *.json
```

Utilizzo AWS CLI per cercare eventi

Cerca eventi specifici delle app Web utilizzando AWS CLI:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "webapp-1a2b3c4d5e6f7g8h9" \
  --start-time $(date -d "1 day ago" +%s)000
```

Oppure cerca eventi di autenticazione:

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "UserAuthentication" \
  --start-time $(date -d "1 day ago" +%s)000
```

Esempi di log di autenticazione

CloudTrail registra gli eventi di autenticazione per le app web Transfer Family, che possono aiutarti a tenere traccia dei tentativi di accesso riusciti e falliti. Questi registri sono particolarmente utili per il monitoraggio della sicurezza e la conformità.

Argomenti

- [Esempio di immissione di registro per la verifica delle credenziali](#)
- [Esempio di immissione di registro per l'autenticazione dell'accesso](#)
- [Esempio di registrazione per ListCallerAccessGrants](#)
- [Esempio di immissione nel registro di un evento GetDataAccess](#)

Esempio di immissione di registro per la verifica delle credenziali

L'esempio seguente mostra una voce di CloudTrail registro per un evento di verifica delle credenziali che si verifica durante il processo di autenticazione.

```
{
```

```

    "eventVersion": "1.09",
    "userIdentity": {
      "type": "Unknown",
      "principalId": "123456789012",
      "arn": "",
      "accountId": "123456789012",
      "accessKeyId": "",
      "userName": "demo-user-2",
      "onBehalfOf": {
        "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
        "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
      },
      "credentialId": "58138a11-87e5-401d-8f0b-7161c9389112"
    },
    "eventTime": "2025-08-08T15:29:30Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.224",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
      "AuthWorkflowID": "f304a48b-7b6d-41c8-b136-4f49c91c1f31",
      "CredentialType": "PASSWORD"
    },
    "requestID": "ff936828-4a81-453c-802d-81368b6bca1a",
    "eventID": "70cb7008-493d-42c2-a9eb-38bf168af6a8",
    "readOnly": false,
    "eventType": "AWS ServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
      "CredentialVerification": "Success"
    },
    "eventCategory": "Management"
  }
}

```

Questo evento fornisce ulteriori dettagli sulla fase di verifica delle credenziali nel processo di autenticazione, mostrando l'ID specifico della credenziale e l'ID del flusso di lavoro di autenticazione utilizzati.

Esempio di immissione di registro per l'autenticazione dell'accesso

L'esempio seguente mostra una voce di CloudTrail registro relativa a un evento di autenticazione utente riuscito durante l'accesso all'app Web utilizzando IAM Identity Center.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "b41f0a02-1635-4d07-a414-aecf9e14b906"
  },
  "eventTime": "2025-08-07T14:09:07Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.14",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "7a4ef12c-7c4b-4bc3-b5bd-c2469afcc795",
    "LoginTo": "https://example.awsapps.com/start/",
    "CredentialType": "PASSWORD"
  },
  "requestID": "fc91bcf0-ac53-4454-a1a0-fb911eacc095",
  "eventID": "18522007-1e60-4a71-b2b5-150baf504ab3",
  "readOnly": false,
  "eventType": "AWS ServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
    "UserAuthentication": "Success"
  }
}
```

```

    },
    "eventCategory": "Management"
  }

```

In questo esempio, nota i seguenti campi importanti:

- `eventSource`: Mostra «signin.amazonaws.com», a indicare che si tratta di un evento di autenticazione IAM Identity Center.
- `userIdentity.onBehalfOf`: contiene l'ID utente e l'ARN dell'archivio di identità per l'utente dell'app Web.
- `additionalEventData.LoginTo`: mostra l'URL dell'applicazione IAM Identity Center a cui si accede.
- `additionalEventData.CredentialType`: Indica il metodo di autenticazione utilizzato (PASSWORD).
- `serviceEventDetails`: mostra il risultato dell'autenticazione (operazione riuscita).

Esempio di registrazione per ListCallerAccessGrants

L'esempio seguente mostra una voce di CloudTrail registro per un ListCallerAccessGrants evento, che si verifica quando l'app web Transfer Family richiede le concessioni di accesso disponibili per un utente.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:aws-transfer",
    "arn": "arn:aws:sts::123456789012:assumed-role/AWS
TransferWebAppIdentityBearer-us-east-2/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/service-role/AWS
TransferWebAppIdentityBearer-us-east-2",
        "accountId": "123456789012",
        "userName": "AWS TransferWebAppIdentityBearer-us-east-2"
      },

```

```

      "attributes": {
        "creationDate": "2025-08-08T15:29:34Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "transfer.amazonaws.com",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    }
  },
  "eventTime": "2025-08-08T15:29:35Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "ListCallerAccessGrants",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "Host": "123456789012.s3-control.dualstack.us-east-2.amazonaws.com",
    "allowedByApplication": "true",
    "maxResults": "100"
  },
  "responseElements": null,
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "bytesTransferredIn": 0,
    "AuthenticationMethod": "AuthHeader",
    "x-amz-id-2": "1g34AaAELn/fntxwriFVsr41VDl8dp5ygWFasHJFNVq5FDCWYfX0ye7s4tWHEJC8ppI5lLePYLIcw3iTXAgn5Q==",
    "bytesTransferredOut": 462
  },
  "requestID": "48485MTZEDWT0ANT",
  "eventID": "3de5dd60-b7cf-474c-a1ab-631467c1a5c3",
  "readOnly": true,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS:S3::AccessGrantsInstance",
      "ARN": "arn:aws:s3:us-east-2:123456789012:access-grants/default"
    }
  ],
  "eventType": "AWS ApiCall",

```

```
"managementEvent": true,  
"recipientAccountId": "123456789012",  
"eventCategory": "Management"  
}
```

In questo esempio, nota i seguenti campi importanti:

- `eventName`: Indica che si tratta di un `ListCallerAccessGrants` evento che interroga le concessioni di accesso S3 disponibili.
- `requestParameters.allowedByApplication`: indica che la query è filtrata in base alle concessioni consentite dall'applicazione.
- `requestParameters.maxResults`: mostra il numero massimo di concessioni da restituire nella risposta.
- `userIdentity.onBehalfOf`: collega la richiesta all'utente specifico dell'app Web.

Questo evento aiuta a tenere traccia di quando l'app web Transfer Family chiede a quali risorse S3 ha accesso un utente, fornendo visibilità sulle operazioni di rilevamento delle concessioni di accesso.

Esempio di immissione nel registro di un evento GetDataAccess

L'esempio seguente mostra una voce di CloudTrail registro per un `GetDataAccess` evento, che si verifica quando l'app web Transfer Family richiede le autorizzazioni di accesso per le risorse S3 per conto di un utente.

```
{  
  "eventVersion": "1.11",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "AROASEQRAEABP7ADWEZA5:aws-transfer",  
    "arn": "arn:aws:sts::123456789012:assumed-role/AWSTransferWebAppIdentityBearer-  
ap-southeast-1/aws-transfer",  
    "accountId": "123456789012",  
    "accessKeyId": "ASIAEXAMPLEKEY",  
    "sessionContext": {  
      "sessionIssuer": {  
        "type": "Role",  
        "principalId": "AROASEQRAEABP7ADWEZA5",  
        "arn": "arn:aws:iam::123456789012:role/service-role/  
AWSTransferWebAppIdentityBearer-ap-southeast-1",  
        "accountId": "123456789012",
```

```

        "userName": "AWSTransferWebAppIdentityBearer-ap-southeast-1"
    },
    "attributes": {
        "creationDate": "2025-05-08T16:09:05Z",
        "mfaAuthenticated": "false"
    }
},
"invokedBy": "transfer.amazonaws.com",
"onBehalfOf": {
    "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9667b0da7a",
    "userId": "191a35ec-10a1-70c1-e4ab-e2802411e13e"
}
},
"eventTime": "2025-05-08T16:10:25Z",
"eventSource": "s3.amazonaws.com",
"eventName": "GetDataAccess",
"awsRegion": "ap-southeast-1",
"sourceIPAddress": "transfer.amazonaws.com",
"userAgent": "transfer.amazonaws.com",
"requestParameters": {
    "Host": "123456789012.s3-control.dualstack.ap-southeast-1.amazonaws.com",
    "durationSeconds": 900,
    "permission": "READWRITE",
    "target": "s3://amzn-s3-demo-bucket/users/john.doe/documents/*"
},
"responseElements": null,
"additionalEventData": {
    "AuthenticationMethod": "AuthHeader",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "SignatureVersion": "SigV4",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2244,
    "x-amz-id-2": "8ce8sZ0gNwsaj9w1mzagyA
+cs0NjYl8FgEw4FGpE8DARi90aNC0RFWlTYNEn7ChqE9RCJrTzMvS+ru7Vz2xXHrkQt/1uQ9exZTZdlhX+/fM="
},
"requestID": "BXGSKKQXCWS5RAHB",
"eventID": "c11db1d1-dfb8-431e-8625-48eba2ebadfe",
"readOnly": true,
"resources": [
    {
        "type": "AWS:S3::AccessGrantsInstance",
        "ARN": "arn:aws:s3:ap-southeast-1:123456789012:access-grants/default",
        "accountId": "123456789012"
    }
]

```



```
    }  
  ],  
  "eventType": "AwsApiCall",  
  "managementEvent": true,  
  "recipientAccountId": "123456789012",  
  "eventCategory": "Management"  
}
```

In questo esempio, nota i seguenti campi importanti:

- `eventName`: Indica che si tratta di un `GetDataAccess` evento che si verifica quando Transfer Family richiede le autorizzazioni di accesso per le risorse S3.
- `userIdentity.onBehalfOf`: contiene l'ARN e l'ID utente dell'archivio di identità, che collegano la richiesta di accesso all'utente specifico dell'app Web.
- `requestParameters.target`: mostra il modello di percorso S3 per il quale è stato richiesto l'accesso.
- `requestParameters.permission`: indica il tipo di accesso richiesto (READWRITE, READ o WRITE).
- `requestParameters.durationSeconds`: mostra per quanto tempo è valida la concessione di accesso (in genere 900 seconds/15 minuti).
- `sourceIPAdresseuserAgent`: entrambi mostrano «transfer.amazonaws.com», a indicare che si tratta di una richiesta di servizio interna.

`GetDataAccess` gli eventi sono particolarmente utili per tracciare quando agli utenti dell'app web Transfer Family viene concesso l'accesso a risorse S3 specifiche, aiutandoti a monitorare i modelli di accesso e a garantire l'autorizzazione corretta.

Visualizzazione delle voci di CloudTrail registro

Esistono diversi modi per visualizzare e analizzare le voci di CloudTrail registro per la tua app web Transfer Family:

Utilizzo della CloudTrail console

La CloudTrail console offre un'interfaccia intuitiva per la visualizzazione e il filtraggio delle voci di registro:

1. Apri la CloudTrail console all'indirizzo. <https://console.aws.amazon.com/cloudtrail/>

2. Nel riquadro di navigazione scegliere Event history (Cronologia eventi).
3. Usa le opzioni di filtro per restringere gli eventi:
 - Imposta l'origine dell'evento `transfer.amazonaws.com` su per visualizzare solo gli eventi Transfer Family.
 - Filtra per nome dell'evento per vedere operazioni specifiche come `UserAuthentication`.
 - Usa Time Range per concentrarti sugli eventi in un periodo specifico.
4. Fai clic su un evento per visualizzarne le informazioni dettagliate.

Accesso ai log in Amazon S3

Se hai configurato un CloudTrail percorso per inviare i log a un bucket Amazon S3, puoi accedere direttamente ai file di log non elaborati:

1. Apri la console Amazon S3 all'indirizzo. <https://console.aws.amazon.com/s3/>
2. Accedi al bucket e al prefisso in cui sono archiviati i CloudTrail log.
3. I log sono organizzati per anno, mese, giorno e regione. Accedere alla directory appropriata.
4. Scarica e apri i file di registro, che sono in formato JSON.

Risoluzione dei problemi relativi alle app Web

Note

Questi suggerimenti per la risoluzione dei problemi sono rivolti all'amministratore dell'app Web piuttosto che all'utente finale. Per gli utenti finali, in caso di problemi, contattate l'amministratore dell'app web. Tutte le tue istanze riportate nei paragrafi seguenti si riferiscono all'amministratore dell'app Web.

Risolvi gli errori di rete

Descrizione

L'utente finale visualizza un banner di rete (Network Error) al caricamento dell'endpoint dell'app Web.

Causa

I problemi più comuni sono i seguenti:

- L'amministratore non ha assegnato l'utente che sta tentando di accedere alla nuova applicazione.
- L'amministratore non ha aggiunto le azioni necessarie ai tuoi ruoli IAM.
- Viene visualizzato un elenco di S3 Access Grants assegnati al tuo utente, ma CORS non è configurato correttamente per il tuo bucket o i bucket Amazon S3.

Soluzione

- In IAM Identity Center, assicurati di assegnare l'utente all'applicazione corretta. Oppure, se ti è stato assegnato un gruppo, assicurati che l'utente che tenta di accedere appartenga al gruppo corretto. Questa procedura è descritta in [Assegna o aggiungi utenti o gruppi a un'app web Transfer Family](#).
- Verifica se i tuoi ruoli contengono le azioni necessarie nella politica di fiducia personalizzata per entrambe `sts:AssumeRole` e `sts:SetContext` azioni. Questa procedura è descritta in [Configurazione dei ruoli IAM per le app web Transfer Family](#).
- Controlla la policy CORS per tutti i bucket utilizzati dalla tua app web. Questo è descritto in [Configurazione della condivisione Cross-origin delle risorse \(CORS\) per il bucket Amazon S3](#).

Risolvi i problemi relativi alla mancata visualizzazione del bucket configurato

Descrizione

Sembra che tutto sia configurato correttamente, ma il bucket Amazon S3 non viene visualizzato nell'app Web.

Causa

Una possibile causa è che il bucket Amazon S3 non si trova nello stesso account dell'app Web.

Soluzione

Assicurati che il bucket Amazon S3 si trovi nello stesso account dell'app Web. Cross-account bucket non sono attualmente supportati.

Risolvi gli errori relativi agli URL personalizzati

Descrizione

Quando l'utente finale accede all'app Web, riceve il messaggio di errore Autorizzazione fallita: codice di autorizzazione mancante.

Causa

Se hai utilizzato CloudFront direttamente, anziché il CloudFormation modello fornito, probabilmente hai configurato erroneamente la policy di richiesta di origine per non inoltrare le stringhe di query.

Soluzione

Aggiorna la politica di richiesta di origine per inoltrare le stringhe di query e i cookie all'origine.

Descrizione

Quando l'utente finale tenta di accedere a un'app web Transfer Family, riceve una risposta 404.

Causa

Se hai utilizzato CloudFront direttamente, anziché il CloudFormation modello fornito, probabilmente hai configurato erroneamente la politica della cache per includere l'Hostintestazione nella chiave della cache o hai configurato erroneamente la politica di richiesta di origine per inoltrare l'intestazione. Host

Soluzione

- Assicurati che la tua politica sulla cache non includa l'Hostintestazione nella chiave della cache
- Assicurati che la tua policy di richiesta di origine non inoltri l'Hostintestazione.

Risolvi errori vari

Descrizione

L'utente finale non può accedere o non può visualizzare bucket o file oppure viene visualizzato un altro errore.

Causa

Una possibile causa è che l'ARN dell'istanza IAM Identity Center non corrisponde al valore dell'ARN delle sovvenzioni o dell'ARN dell'istanza IAM Identity Center dell'app Web IAM Identity Center.

Soluzione

Controlla i seguenti elementi per vedere se corrispondono.

- In IAM Identity Center, accedi a Impostazioni e visualizza l'ARN dell'istanza.

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

- In Amazon S3, accedi a Access Grants e visualizza l'ARN dell'istanza IAM Identity Center.

```
arn:aws:sso:::account-id:application/ssoins-instance-identifier/apl-1234567890abcdef0
```

- In Transfer Family, accedi alla pagina dei dettagli della tua app Web e visualizza l'ARN dell'istanza.

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

Il *instance-identifier* valore deve essere lo stesso in tutte e tre queste posizioni.

Bucket S3 duplicati visualizzati nell'app Web

Descrizione

Gli utenti vedono lo stesso bucket S3 elencato più volte nell'interfaccia dell'app web Transfer Family.

Causa

Ciò si verifica quando un utente fa parte di più gruppi di Active Directory con concessioni duplicate allo stesso bucket S3. L'app Web elenca tutte le sovvenzioni di primo livello associate all'utente (UID o GID) indipendentemente dal fatto che all'utente siano assegnate più sovvenzioni alla stessa posizione del bucket.

Soluzione

Per risolvere questo problema, gli amministratori devono deduplicare le concessioni in modo che ogni utente disponga di una sola concessione per ogni sede S3. Rivedi la configurazione di S3 Access Grants e consolida le concessioni duplicate per lo stesso bucket in diversi gruppi di Active Directory.

Istruzioni per l'utente finale per le app web Transfer Family

Note

In questo argomento, le informazioni sono destinate agli utenti finali che interagiscono con l'app web. Tutte le istanze dell'utente riportate in questo argomento si riferiscono agli utenti finali.

Questo argomento descrive come accedere a un'app AWS Transfer Family Web che sei autorizzato a utilizzare e descrive come interagire con essa.

Quote per le app Web

Tieni presente le seguenti limitazioni quando utilizzi app Web.

- Numero massimo di risultati di ricerca per query: 10.000
- I bucket Amazon S3 utilizzati dall'app web Transfer Family devono trovarsi nello stesso account dell'app Web stessa. Cross-account i bucket non sono attualmente supportati.
- Ampiezza massima di ricerca per query: 10.000 file ricercati
- Dimensione massima di caricamento per file: 160 GB (149 GiB)
- Dimensione massima del file per la copia: 5,36 GB (5 GiB)
- I nomi di cartella che iniziano o finiscono con punti (.) non sono supportati

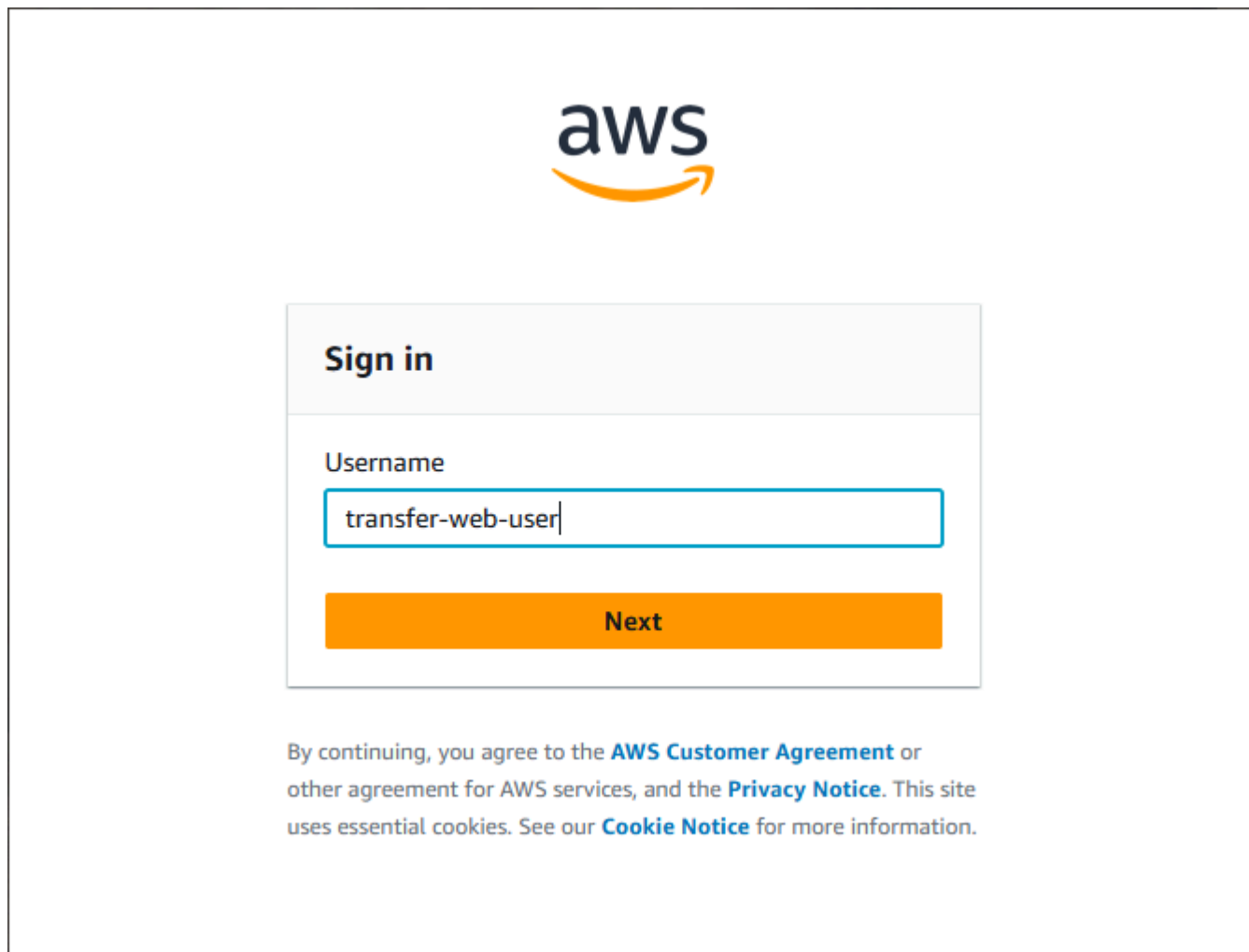
Esperienza utente per gli utenti di IAM Identity Center

Questa sezione descrive l'esperienza utente se l'organizzazione ha utilizzato IAM Identity Center per configurare i propri utenti.

Per accedere a un'app web Transfer Family

1. Dovresti ricevere un'email da `no-reply@login.awsapps.com` intitolata «Invito a partecipare» AWS IAM Identity Center. Accetta l'invito ad attivare il tuo account utente.
2. Nel messaggio, scegli l'URL sotto l'URL del tuo portale di AWS accesso.

Verrà visualizzata la schermata di AWS accesso.



aws

Sign in

Username

transfer-web-user

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

3. Inserisci le tue credenziali e scegli Accedi.

Si accede a Portale di accesso AWS, che mostra un elenco delle applicazioni disponibili.

4. Scegli l'applicazione per la tua app web Transfer Family.

Esperienza utente per utenti di provider di identità di terze parti

Se l'organizzazione non ha utilizzato la AWS IAM Identity Center funzione di configurazione degli utenti, l'esperienza di onboarding dipenderà dall'applicazione del provider di identità utilizzata per configurare gli utenti finali. Dopo l'autenticazione e l'accesso, l'interfaccia dell'app Web è la stessa descritta nella sezione successiva.

Note

Se un utente appartiene a più gruppi di Active Directory che dispongono di concessioni per lo stesso bucket Amazon S3, il bucket viene visualizzato più volte nell'interfaccia dell'app Web. Ciò si verifica perché l'app Web elenca tutte le sovvenzioni di primo livello associate all'UID o GID dell'utente, incluse le concessioni duplicate allo stesso bucket. Per evitare offerte duplicate, gli amministratori possono consolidare più concessioni in modo che ogni utente abbia una sola concessione per sede Amazon S3.

Interfaccia utente finale Transfer Family

Dopo esserti autenticato e aver effettuato l'accesso, puoi interagire con l'app web.

Esistono quattro viste principali.

- Home page: la tua home page elenca le sedi S3 a cui puoi accedere, oltre alle autorizzazioni per ciascuna di esse. Una posizione S3 è un bucket o prefisso S3, che puoi definire quando usi S3 Access Grants. Questa è la vista iniziale per gli utenti che mostra le risorse S3 di livello principale a cui gli utenti finali hanno accesso e le autorizzazioni per ogni posizione S3.

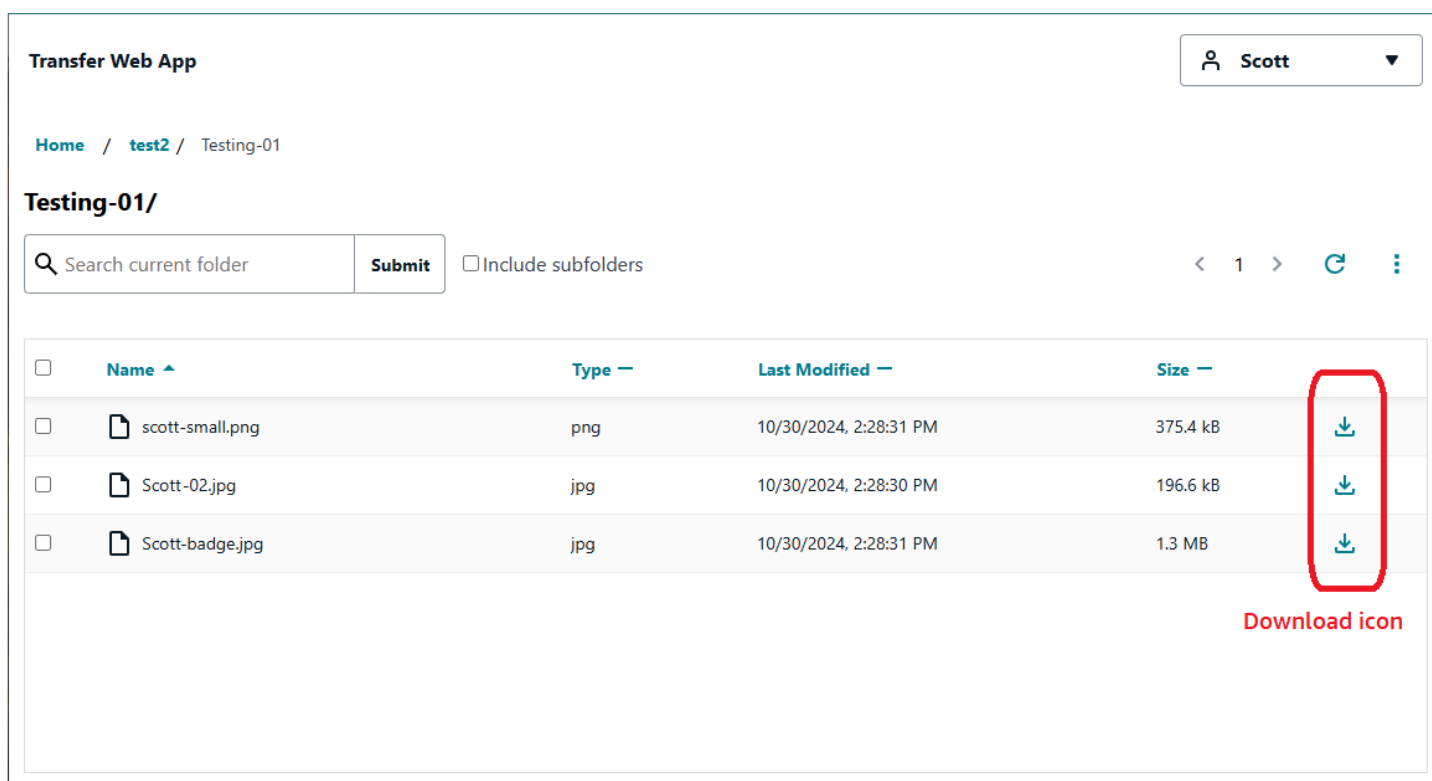
The screenshot displays the Amazon Transfer Family Home page. At the top left is the Amazon logo. On the right is a user profile dropdown menu. Below the logo is the heading 'Home'. A search bar with the placeholder 'Filter folders and files' and a 'Submit' button is present. To the right of the search bar are navigation controls: '< 1 >' and a refresh icon. Below these is a table with three columns: 'Folder', 'Bucket', and 'Permission'. The 'Folder' column has a dropdown arrow and contains the text 'test'. The 'Bucket' column has a dropdown arrow and contains the text 'test'. The 'Permission' column has a dropdown arrow and contains the text 'READWRITE'. A green box highlights the 'Bucket' column, and a red box highlights the 'Permission' column. Below the green box is the text 'Buckets the web app can access' in green. Below the red box is the text 'Permissions for the bucket' in red.

Folder	Bucket	Permission
test	test	READWRITE

- **Dettagli sulla posizione:** questa vista consente agli utenti di sfogliare i file e le cartelle in S3 e di caricare o scaricare i file
- **Azione sulla posizione:** dopo aver scelto un'azione (come Carica), si apre un'altra visualizzazione della posizione del file.
- **Puntini di sospensione verticali:** l'icona con i puntini di sospensione verticali apre il menu Azioni.

Operazioni disponibili

La maggior parte delle azioni è disponibile nel menu Azioni. Per l'altra azione principale, il download dei file, si utilizza l'icona di download dopo aver selezionato un file (attualmente è possibile scaricare solo un file alla volta).



The screenshot shows the AWS Transfer Web App interface. At the top, it says "Transfer Web App" and "Scott" is logged in. The breadcrumb path is "Home / test2 / Testing-01". Below this, the section "Testing-01/" is displayed. There is a search bar labeled "Search current folder" and a "Submit" button. A checkbox labeled "Include subfolders" is also present. To the right of the search bar are navigation icons: back, forward, refresh, and a vertical ellipsis (three dots). Below the search bar is a table with the following columns: "Name", "Type", "Last Modified", and "Size". The table contains three rows of files:

☐	Name	Type	Last Modified	Size	
☐	scott-small.png	png	10/30/2024, 2:28:31 PM	375.4 kB	Download icon
☐	Scott-02.jpg	jpg	10/30/2024, 2:28:30 PM	196.6 kB	Download icon
☐	Scott-badge.jpg	jpg	10/30/2024, 2:28:31 PM	1.3 MB	Download icon

The download icons (blue arrows pointing down) are highlighted with a red rectangle. Below the table, the text "Download icon" is written in red.

Da una cartella, utilizzate il menu Azioni per eseguire una delle seguenti attività:

- Copiare uno o più file in un'altra posizione.
- Creare una cartella.
- Eliminare uno o più file.
- Carica uno o più file.
- Carica un'intera cartella (comprese le sottocartelle, se presenti).

- Seleziona una cartella e accedi ad essa. È quindi possibile eseguire una qualsiasi delle azioni elencate in precedenza.
- Ordina per pagina.
- Filtra per nome del file o della cartella per cartella e sottocartelle.



  ▼

Home / test

test

☐ Include subfolders

< 1 >  

Name ▲	Type —	Last Modified —
 My First Folder/	Folder	
 My Second Folder/	Folder	
 Testing-01/	Folder	
 Testing-02/	Folder	

 Copy files
 Create folder
 Delete files
 Upload files
 Upload folder

AWS Transfer Family Connettori SFTP

Un connettore AWS Transfer Family SFTP stabilisce una connessione con un server SFTP remoto per trasferire file tra lo storage Amazon e un server remoto, utilizzando il protocollo SFTP. Puoi inviare file da Amazon S3 a un server SFTP esterno di proprietà di un partner, recuperare file dal server SFTP di un partner ad Amazon S3 o elencare, eliminare, rinominare o spostare file sul server remoto. I connettori SFTP supportano due tipi di uscita: servizio gestito (tramite infrastruttura AWS gestita) e VPC (routing attraverso il tuo VPC utilizzando Amazon VPC Lattice). Utilizzando i connettori SFTP, puoi creare flussi di lavoro di trasferimento di file automatizzati e basati sugli eventi. AWS

Visualizza i [connettori AWS Transfer Family SFTP](#) per una breve introduzione ai connettori SFTP Transfer Family.

Argomenti

- [Creazione di connettori SFTP](#)
- [Connettività VPC per connettori SFTP](#)
- [Utilizzo dei connettori SFTP](#)
- [Monitoraggio dei connettori SFTP](#)
- [Gestione dei connettori SFTP](#)
- [Scalabilità e quote per i connettori SFTP](#)
- [Architetture di riferimento che utilizzano connettori SFTP](#)

Creazione di connettori SFTP

Questo argomento descrive come creare connettori SFTP. Ogni connettore offre la possibilità di connettersi a un server SFTP remoto. Per configurare un connettore SFTP, si eseguono le seguenti attività di alto livello.

Note

Per i VPC-based connettori che indirizzano il traffico attraverso il tuo Virtual Private Cloud, vedi. [Crea un connettore SFTP con uscita VPC-based](#)

1. Memorizza le credenziali di autenticazione per il connettore in Gestione dei segreti AWS.

2. Crea il connettore, specificando l'ARN segreto, l'URL o l'ARN di configurazione delle risorse del server remoto, la politica di sicurezza contenente gli algoritmi che saranno supportati dal connettore e altre impostazioni di configurazione.
3. Dopo aver creato il connettore, potete testarlo per assicurarvi che possa stabilire connessioni con il server SFTP remoto.

Scelta del tipo di uscita del connettore SFTP

Quando crei un connettore SFTP, scegli il tipo di uscita tra «Service managed» e «VPC Lattice».

- Servizio gestito (impostazione predefinita): il connettore utilizza gateway NAT e indirizzi IP di proprietà di per AWS Transfer Family instradare le connessioni sulla rete Internet pubblica. Il servizio fornisce 3 indirizzi IP statici per i connettori che devono essere consentiti nell'elenco dei server remoti per stabilire connessioni.
- VPC Lattice: il connettore indirizza il traffico attraverso il tuo ambiente VPC utilizzando Amazon VPC Lattice. Utilizza la connettività VPC per i connettori SFTP in questi scenari:
 - Server SFTP privati: Connettiti a server SFTP accessibili solo dal tuo VPC
 - On-premises connettività: Connettiti ai server SFTP locali tramite AWS Direct Connect o connessioni AWS Virtual Private Network
 - Indirizzi IP personalizzati: presenta i tuoi gateway NAT e indirizzi IP elastici al server remoto
 - Controlli di sicurezza centralizzati: indirizzate i trasferimenti di file attraverso i controlli centrali della vostra organizzazione ingress/egress

La seguente matrice ti aiuta a scegliere il tipo di connettore giusto per i tuoi casi d'uso.

Matrice del tipo di uscita del connettore SFTP

Funzionalità	Tipo di uscita = Servizio gestito	Tipo di uscita = VPC Lattice
Connettività a server SFTP ospitati pubblicamente (accessibili da Internet)	Supportata	Supportato 1
Connettività a server SFTP ospitati privatamente (locali)	Non supportata	Supportato 2

Funzionalità	Tipo di uscita = Servizio gestito	Tipo di uscita = VPC Lattice
Connettività a server SFTP ospitati privatamente (in-VPC)	Non supportata	Supportata
Indirizzi IP statici presentati al server SFTP remoto	Supportato tramite indirizzi IP statici forniti dal servizio	Supportato tramite indirizzi IP statici di proprietà del cliente
Larghezza di banda disponibile	50 MBPS per account	Larghezza di banda più elevata, disponibile presso Resource Gateway e NAT Gateway di proprietà del cliente
Instradamento del traffico verso Internet tramite gateway NAT e firewall di rete di proprietà del cliente	Non supportato. I gateway NAT sono di proprietà e gestiti dal servizio Transfer Family.	Supportata

¹ Con Egress Type = VPC Lattice, la connettività ai server ospitati pubblicamente è supportata utilizzando la configurazione dell'infrastruttura di uscita (NAT Gateway) nei VPC in uscita.

² Con Egress Type = VPC Lattice, la connettività ai server ospitati privatamente è supportata utilizzando le reti esistenti nel tuo VPC, come o VPN. AWS Direct Connect

Scelta della modalità di indirizzamento IP

Quando si crea un connettore SFTP con uscita gestita dal servizio, è possibile scegliere tra due modalità di indirizzamento IP:

- Solo IPv4 (impostazione predefinita): il connettore utilizza gli indirizzi IPv4 esclusivamente per connettersi al server SFTP remoto. Questa è la modalità predefinita per la creazione di connettori tramite console, AWS CLI o API.
- Dual-stack: Il connettore supporta sia gli indirizzi IPv6 che IPv4. In modalità dual-stack, il connettore preferisce IPv6 quando la risoluzione DNS restituisce risultati IPv6 e utilizza IPv4 quando vengono restituiti solo risultati DNS IPv4.

 Note

La modalità di indirizzamento IP si applica solo ai connettori con tipo di uscita gestito dal servizio. I connettori che utilizzano l'uscita VPC Lattice non supportano questa impostazione.

Argomenti

- [Memorizza le credenziali di autenticazione per i connettori SFTP in Secrets Manager](#)
- [Crea un connettore SFTP con uscita gestita dal servizio](#)
- [Crea un connettore SFTP con uscita VPC-based](#)
- [Prova un connettore SFTP](#)

Memorizza le credenziali di autenticazione per i connettori SFTP in Secrets Manager

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 [Gestione dei segreti AWS Pricing](#).

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

1. Accedi a Console di gestione AWS e apri la Gestione dei segreti AWS 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. Fornisci le key/value informazioni relative al tuo segreto: devi fornire il nome utente e una chiave privata o una password.

- a. Nella sezione Key/value coppie, scegli la Key/valuescheda.
 - Chiave: Invio**Username**.
 - valore: immetti il nome dell'utente autorizzato a connettersi al server del partner.
- b. Se desideri fornire una coppia di chiavi, scegli Aggiungi riga e nella sezione Key/value coppie, scegli la Key/valuescheda.
 - Chiave: Invio**PrivateKey**.
 - valore: incolla la tua chiave privata.

Suggerimento: i dati della chiave privata che inserisci devono corrispondere alla chiave pubblica archiviata per questo utente sul server SFTP remoto.

 Note

Non è possibile utilizzare una chiave privata protetta da passphrase per l'autenticazione con un connettore SFTP. AWS Transfer Family

Per informazioni dettagliate su come generare una public/private key pair, vedere [Creazione di chiavi SSH su macOS, Linux o Unix](#).

- c. Se desideri fornire una password, scegli Aggiungi riga e nella sezione Key/value coppie, scegli la Key/valuescheda.
 - Chiave: Invio**Password**.
 - valore: immettere la password per l'utente.
6. Scegli Next (Successivo).
7. 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**.
8. Scegli Avanti, quindi accetta le impostazioni predefinite nella pagina Configura rotazione. Quindi scegli Successivo.
9. Nella pagina Revisione, scegli Store per creare e archiviare il segreto.

Crea un connettore SFTP con uscita gestita dal servizio

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 SFTP, quindi scegli Crea connettore SFTP.
3. Nella sezione Configurazione del connettore, per Tipo di uscita, scegli Servizio gestito. Questa opzione utilizza un'infrastruttura di uscita AWS Transfer Family gestita. Il servizio Transfer Family fornisce e gestisce indirizzi IP statici per ogni connettore SFTP.
4. Nella sezione Configurazione del connettore, fornisci le seguenti informazioni:

Connector configuration

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

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

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

URL of the remote (target) SFTP server

Access role Info
IAM Role for Amazon S3 access and AWS Secrets Manager access

Logging role - optional Info
IAM role for the connector to push events to your CloudWatch logs

- Per l'URL, immettete 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](#)

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

```

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

```

Note

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 Gestione dei segreti AWS segreti per gli utenti](#) di un altro account.

5. Completa la configurazione del connettore:

- (Facoltativo) Per il ruolo Logging, 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": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

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

SFTP configuration Info

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

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

① Connections to the remote server are established only if it's SSH fingerprint matches one of the provided trusted host key(s).

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

- Per le credenziali del connettore, dall'elenco a discesa, scegli il nome di un segreto Gestione dei segreti AWS che contiene la chiave privata o la password dell'utente SFTP.

È necessario creare un segreto e archivarlo in un modo specifico. Per informazioni dettagliate, vedi [Memorizza le credenziali di autenticazione per i connettori SFTP in Secrets Manager](#).

- (Facoltativo) È possibile creare il connettore lasciando il `TrustedHostKeys` parametro vuoto. Tuttavia, il connettore non sarà in grado di trasferire file con il server remoto finché non fornirai questo parametro nella configurazione del connettore. Puoi inserire le chiavi host affidabili al momento della creazione del connettore o aggiornare il connettore in un secondo momento utilizzando le informazioni sulla chiave host restituite dall'azione della `TestConnection` console o dal comando API. In altre parole, per la casella di testo `Trusted host keys`, puoi effettuare una delle seguenti operazioni:
 - Fornisci le chiavi `Trusted Host` al momento della creazione del connettore. 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](#).
 - Lascia vuota la casella di testo `Trusted Host Key (s)` quando crei il connettore e aggiorna il connettore in un secondo momento con queste informazioni. Se non disponi delle informazioni sulla chiave host al momento della creazione del connettore, puoi lasciare questo parametro vuoto per ora e procedere con la creazione del connettore. Dopo aver creato il connettore, utilizza l'ID del nuovo connettore per eseguire il `TestConnection` comando, nella AWS CLI o dalla pagina dei dettagli del connettore. In caso di successo, `TestConnection` restituirà le informazioni necessarie sulla chiave host. È quindi possibile modificare il connettore utilizzando la console (o eseguendo il `UpdateConnector` AWS CLI comando) e aggiungere le informazioni sulla chiave host restituite durante l'esecuzione `TestConnection`.

 Important

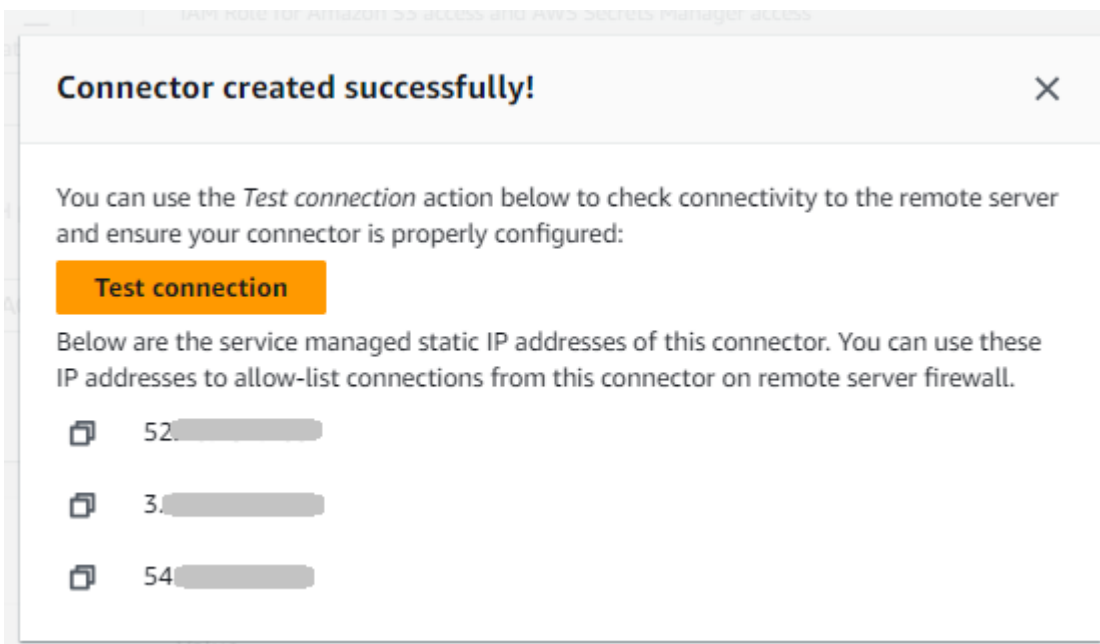
Se recuperi la chiave host del server remoto eseguendo `TestConnection`, assicurati di eseguire una convalida fuori banda sulla chiave restituita.

È necessario accettare la nuova chiave come attendibile o verificare l'impronta digitale presentata con un'impronta digitale precedentemente nota che avete ricevuto dal proprietario del server SFTP remoto a cui vi state connettendo.

- (Facoltativo) Per Numero massimo di connessioni simultanee, dall'elenco a discesa, scegliete il numero di connessioni simultanee che il connettore crea al server remoto. La selezione predefinita sulla console è 5.

Questa impostazione specifica il numero di connessioni attive che il connettore può stabilire contemporaneamente con il server remoto. La creazione di connessioni simultanee può migliorare le prestazioni dei connettori abilitando le operazioni parallele.

7. 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 di sicurezza per AWS Transfer Family i connettori SFTP](#)
8. (Facoltativo) Nella sezione Tag, per Chiave e Valore, inserite uno o più tag come coppie chiave-valore.
9. Dopo aver confermato tutte le impostazioni, scegli Crea connettore SFTP 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, consulta [Visualizza i dettagli del connettore SFTP](#).

CLI

Il [create-connector](#) comando 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](#)

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

```

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

```

Note

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 Gestione dei segreti AWS 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": "VisualEditor0",
      "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 Gestione dei segreti AWS 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

SecretIdPuò essere l'intero ARN o il nome del segreto (*example-username-key* nell'elenco precedente).

Quindi esegui il seguente comando 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 \
--maximum-concurrent-connections integer-from-1-to-5
```

Quando descrivi un connettore di tipo di uscita VPC, la risposta include i nuovi campi:

```
{
  "Connector": {
    "AccessRole": "arn:aws:iam::123456789012:role/connector-role",
    "Arn": "arn:aws:transfer:us-east-1:123456789012:connector/
c-1234567890abcdef0",
    "ConnectorId": "c-1234567890abcdef0",
    "Status": "ACTIVE",
    "EgressConfig": {
      "VpcLattice": {
        "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-12345678",
        "PortNumber": 22
      }
    },
    "EgressType": "VPC",
    "ServiceManagedEgressIpAddresses": null,
    "SftpConfig": {
```

```
    "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
    "UserSecretId": "aws/transfer/connector-secret"
  },
  "Url": "sftp://my.sftp.server.com:22"
}
```

Tieni presente che `ServiceManagedEgressIpAddresses` è nullo per i connettori di tipo VPC in uscita poiché il traffico viene indirizzato attraverso il tuo VPC anziché attraverso l'infrastruttura gestita. AWS

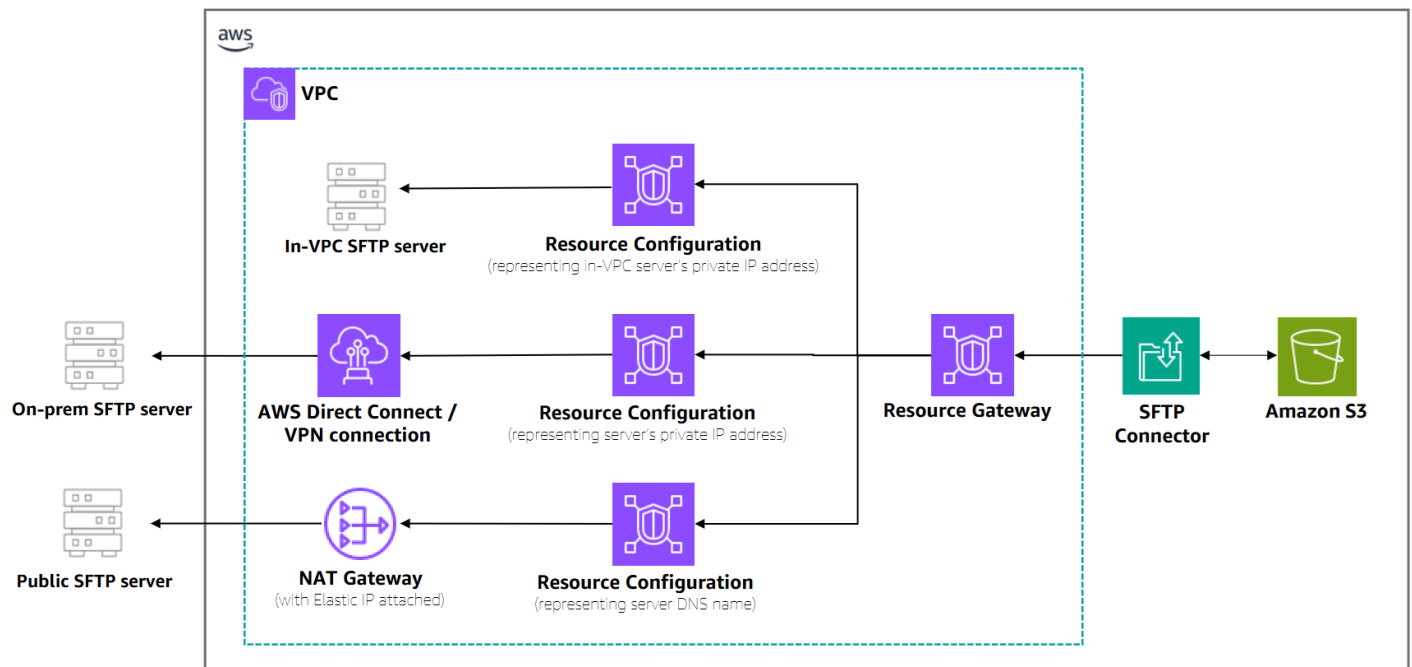
Crea un connettore SFTP con uscita VPC-based

Questo argomento fornisce istruzioni dettagliate per la creazione di connettori SFTP con connettività VPC. LATTICE-enabled I connettori VPC_ utilizzano Amazon VPC Lattice per indirizzare il traffico attraverso il tuo Virtual Private Cloud, abilitando connessioni sicure a endpoint privati o utilizzando i tuoi gateway NAT per l'accesso a Internet.

Quando utilizzare la connettività VPC

Utilizza la connettività VPC per i connettori SFTP in questi scenari:

- Server SFTP privati: Connettiti ai server SFTP accessibili solo dal tuo VPC.
- On-premises connettività: Connettiti ai server SFTP locali tramite AWS Direct Connect o connessioni AWS Site-to-Site VPN.
- Indirizzi IP personalizzati: utilizza i tuoi gateway NAT e indirizzi IP elastici, inclusi gli scenari BYOIP.
- Controlli di sicurezza centralizzati: indirizza i trasferimenti di file attraverso i controlli centrali dell'organizzazione. ingress/egress



Prerequisiti per i connettori VPC_ SFTP LATTICE-enabled

Prima di creare un connettore VPC_ LATTICE-enabled SFTP, è necessario completare i seguenti prerequisiti:

Come funziona la connettività VPC-based

VPC Lattice ti consente di condividere in modo sicuro le risorse VPC con altri servizi. AWS AWS Transfer Family utilizza una rete di servizi per semplificare il processo di condivisione delle risorse. I componenti principali sono:

- **Resource Gateway:** funge da punto di accesso al tuo VPC. Puoi crearlo nel tuo VPC con un minimo di due zone di disponibilità.
- **Configurazione delle risorse:** contiene l'indirizzo IP privato o il nome DNS pubblico del server SFTP a cui desideri connetterti.

Quando crei un LATTICE-enabled connettore VPC_, AWS Transfer Family utilizza Forward Access Session (FAS) per ottenere temporaneamente le tue credenziali e associare la tua Resource Configuration alla nostra rete di servizi.

Passaggi di configurazione richiesti

1. **Infrastruttura VPC:** assicurati di disporre di un VPC configurato correttamente con le sottoreti, le tabelle di routing e i gruppi di sicurezza necessari per i requisiti di connettività del server SFTP.
2. **Resource Gateway:** crea un Resource Gateway nel tuo VPC usando il comando VPC `create-resource-gateway`. Il Resource Gateway deve essere associato a sottoreti in almeno due zone di disponibilità. Per ulteriori informazioni, consulta [Resource gateway](#) nella Amazon VPC Lattice User Guide.
3. **Configurazione delle risorse:** crea una configurazione delle risorse che rappresenti il server SFTP di destinazione utilizzando il comando VPC `create-resource-configuration`. È possibile specificare:
 - Un indirizzo IP privato per endpoint privati
 - Un nome DNS pubblico per gli endpoint pubblici (gli indirizzi IP non sono supportati per gli endpoint pubblici)
4. **Credenziali di autenticazione:** memorizza le credenziali utente SFTP come descritto in. Gestione dei segreti AWS [Memorizza le credenziali di autenticazione per i connettori SFTP in Secrets Manager](#)

 Important

Resource Gateway e Resource Configuration devono essere creati nello stesso account. AWS Quando si crea una configurazione delle risorse, è necessario innanzitutto disporre di un Resource Gateway.

Per ulteriori informazioni sulle configurazioni delle risorse VPC, consulta Configurazioni delle [risorse nella](#) Amazon VPC Lattice User Guide.

 Note

La connettività VPC per i connettori SFTP è disponibile laddove sono disponibili Regioni AWS risorse Amazon VPC Lattice. Per ulteriori informazioni, consulta le domande frequenti su [VPC Lattice](#). Il supporto per le zone di disponibilità varia in base alla regione e i Resource Gateway richiedono un minimo di due zone di disponibilità.

Creare un connettore VPC_ SFTP LATTICE-enabled

Dopo aver completato i prerequisiti, puoi creare un connettore SFTP con connettività VPC utilizzando la console di AWS gestione o AWS CLI gli SDK. AWS

Console

Per creare un connettore VPC_ SFTP LATTICE-enabled

1. Apri la console all' AWS Transfer Family indirizzo. <https://console.aws.amazon.com/transfer/>
2. Nel riquadro di navigazione a sinistra, scegli Connettori SFTP, quindi scegli Crea connettore SFTP.
3. Nella sezione Configurazione del connettore, per il tipo di uscita, scegli VPC Lattice.

Questa opzione indirizza il traffico attraverso il tuo VPC utilizzando Amazon VPC Lattice per l'accesso alle risorse tra VPC. Puoi utilizzare questa opzione per connetterti a endpoint server ospitati privatamente, instradare il traffico attraverso i controlli di sicurezza del tuo VPC o utilizzare i tuoi gateway NAT e indirizzi IP elastici. L'indirizzo del server SFTP remoto è rappresentato come configurazione delle risorse nel tuo VPC. Per ulteriori informazioni sulle configurazioni delle risorse, consulta Configurazioni [delle risorse per le risorse VPC nella Amazon VPC](#) Lattice User Guide.

4. Completa la configurazione del connettore:
 - 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](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
  }
]
}

```

Note

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 più account, consulta [Autorizzazioni ai Gestione dei segreti AWS segreti per gli utenti](#) di un altro account.

- Per Resource Configuration ARN, inserisci l'ARN della VPC Lattice Resource Configuration che punta al tuo server SFTP:

```
arn:aws:vpc-lattice:region:account-id:resourceconfiguration/rcfg-12345678
```

- (Facoltativo) Per il ruolo Logging, scegli il ruolo IAM per il connettore da utilizzare per inviare eventi ai tuoi log. CloudWatch

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",

```

```

        "logs:CreateLogGroup",
        "logs:PutLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
}
]
}

```

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

- Per le credenziali del connettore, scegliete il nome di un segreto Gestione dei segreti AWS che contiene la chiave privata o la password dell'utente SFTP.
- Per le chiavi host affidabili, incollate la parte pubblica della chiave host utilizzata per identificare il server esterno oppure lasciatela vuota per configurarla in un secondo momento utilizzando il `TestConnection` comando.

Poiché questa chiave host è per un connettore VPC_LATTICE, rimuovi il nome host nella chiave

- (Facoltativo) Per il numero massimo di connessioni simultanee, scegliete il numero di connessioni simultanee che il connettore crea al server remoto (l'impostazione predefinita è 5).
6. Nella sezione Opzioni dell'algoritmo di crittografia, scegli una politica di sicurezza dall'elenco a discesa.
7. (Facoltativo) Nella sezione Tag, aggiungi i tag come coppie chiave-valore.
8. Scegli Crea connettore SFTP per creare il connettore LATTICE-enabled VPC_ SFTP.

Il connettore verrà creato con lo stato di PENDING durante il provisioning dell'associazione di risorse, operazione che in genere richiede diversi minuti. Una volta modificato lo stato ACTIVE, il connettore è pronto per l'uso.

CLI

Utilizzate il seguente comando per creare un connettore VPC_ LATTICE-enabled SFTP:

```

aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
  --sftp-config UserSecretId=my-secret-id,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \

```



```
--egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0} \  
--security-policy-name TransferSecurityPolicy-2024-01
```

Il parametro chiave per la connettività VPC è `--egress-config`, che specifica l'ARN di configurazione delle risorse che definisce la destinazione del server SFTP.

Monitoraggio dello stato del connettore VPC

I LATTICE-enabled connettori VPC_ hanno un processo di configurazione asincrono. Dopo la creazione, monitora lo stato del connettore:

- **IN SOSPESO:** è in corso il provisioning del connettore. Il provisioning della rete di assistenza è in corso e in genere richiede alcuni minuti.
- **ATTIVO:** Il connettore è pronto all'uso e può trasferire file.
- **ERRORE:** il provisioning del connettore non è riuscito. Controlla i dettagli dell'errore per informazioni sulla risoluzione dei problemi.

Controlla lo stato del connettore usando il `describe-connector` comando:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Durante lo stato **PENDING**, l'`test-connectionAPI` restituirà «Connettore non disponibile» fino al completamento del provisioning.

Considerazioni e limitazioni

- **Endpoint pubblici:** quando ti connetti a endpoint pubblici tramite VPC, devi fornire un nome DNS nella configurazione delle risorse. Gli indirizzi IP pubblici non sono supportati.
- **Disponibilità regionale:** la connettività VPC è disponibile in alcune versioni. Regioni AWS Cross-region la condivisione delle risorse non è supportata.
- **Requisiti della zona di disponibilità:** i Resource Gateway devono essere associati a sottoreti in almeno due zone di disponibilità. Non tutte le zone di disponibilità supportano VPC Lattice in tutte le regioni.
- **Limiti di connessione:** massimo 350 connessioni per risorsa con un timeout di inattività di 350 secondi per le connessioni TCP.

Considerazioni sui costi

Non sono previsti costi aggiuntivi oltre ai normali costi di AWS Transfer Family servizio. Tuttavia, i clienti potrebbero essere soggetti a costi aggiuntivi da parte di Amazon VPC Lattice associati alla condivisione delle proprie risorse Amazon Virtual Private Cloud e ai costi del gateway NAT se utilizzano i propri gateway NAT per l'accesso a Internet.

[Per informazioni complete AWS Transfer Family sui prezzi, consulta la pagina dei prezzi.AWS Transfer Family](#)

Esempi di connettività VPC per connettori SFTP

Questa sezione fornisce esempi di creazione di connettori SFTP con connettività VPC per vari scenari. Prima di utilizzare questi esempi, assicurati di aver completato la configurazione dell'infrastruttura VPC come descritto nella documentazione sulla connettività VPC.

Esempio: connessione endpoint privata

Questo esempio mostra come creare un connettore SFTP che si connette a un server SFTP privato accessibile solo dal tuo VPC.

Prerequisiti

1. Crea un Resource Gateway nel tuo VPC:

```
aws vpc-lattice create-resource-gateway \
  --name my-private-server-gateway \
  --vpc-identifier vpc-1234567890abcdef0 \
  --subnet-ids subnet-1234567890abcdef0 subnet-0987654321fedcba0
```

2. Crea una configurazione delle risorse per il tuo server SFTP privato:

```
aws vpc-lattice create-resource-configuration \
  --name my-private-server-config \
  --resource-gateway-identifier rgw-1234567890abcdef0 \
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"} \
  --port-ranges 22
```

Crea il connettore VPC_ LATTICE-enabled

1. Crea il connettore SFTP con connettività VPC:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-private-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

2. Monitora lo stato del connettore finché non diventa: ACTIVE

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Il server SFTP remoto vedrà le connessioni provenienti dall'indirizzo IP del Resource Gateway all'interno dell'intervallo CIDR VPC.

Esempio: endpoint pubblico tramite VPC

Questo esempio mostra come instradare le connessioni a un server SFTP pubblico tramite il VPC per sfruttare i controlli di sicurezza centralizzati e utilizzare i propri indirizzi IP del gateway NAT.

Prerequisiti

1. Crea un Resource Gateway nel tuo VPC (come nell'esempio di un endpoint privato).
2. Crea una configurazione delle risorse per il server SFTP pubblico usando il suo nome DNS:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"} \  
  --port-ranges 22
```

Note

Per gli endpoint pubblici, è necessario utilizzare un nome DNS, non un indirizzo IP.

Crea il connettore

- Crea il connettore SFTP:

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-public-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-0987654321fedcba0,PortNumber=22}
```

Il traffico fluirà dal connettore al Resource Gateway, quindi attraverso il gateway NAT per raggiungere il server SFTP pubblico. Il server remoto vedrà come origine l'indirizzo IP elastico del gateway NAT.

Esempio: Cross-account endpoint privato

Questo esempio mostra come connettersi a un server SFTP privato con un AWS account diverso utilizzando la condivisione delle risorse.

Note

Se hai già abilitato la condivisione delle risorse tra VPC tramite altri meccanismi, ad esempio AWS Transit Gateway, non è necessario configurare la condivisione delle risorse descritta qui. I meccanismi di routing esistenti, come le tabelle di routing Transit Gateway, vengono utilizzati automaticamente dai connettori SFTP. È sufficiente creare una configurazione delle risorse nello stesso account in cui si sta creando il connettore SFTP.

Account A (Resource Provider): condividi la configurazione delle risorse

1. Crea Resource Gateway e Resource Configuration nell'Account A (come negli esempi precedenti).
2. Condividi la configurazione delle risorse con l'account B utilizzando AWS Resource Access Manager:

```
aws ram create-resource-share \  
  --name cross-account-sftp-share \  
  --resource-arns arn:aws:vpc-lattice:us-  
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0 \  
  --principals 222222222222
```

Account B (Resource Consumer): accetta e utilizza la condivisione

1. Accetta l'invito alla condivisione delle risorse:

```
aws ram accept-resource-share-invitation \
  --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
  share-invitation/invitation-id
```

2. Crea il connettore SFTP nell'account B:

```
aws transfer create-connector \
  --access-role arn:aws:iam::222222222222:role/TransferConnectorRole \
  --sftp-config UserSecretId=cross-account-server-
  credentials,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-
  east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

Il connettore nell'account B può ora accedere al server SFTP privato nell'account A tramite la configurazione delle risorse condivisa.

Scenari per la risoluzione dei problemi comuni

Ecco le soluzioni per i problemi più comuni relativi alla creazione di connettori VPC_LATTICE-enabled :

- Connettore bloccato nello stato IN SOSPESO: verifica che il Resource Gateway sia ATTIVO e che le sottoreti siano presenti nelle zone di disponibilità supportate. Se il connettore è ancora bloccato con lo stato PENDING, chiama `UpdateConnector` utilizzando gli stessi parametri di configurazione utilizzati inizialmente. Ciò attiva un nuovo evento di stato che potrebbe risolvere il problema.
- Timeout di connessione: verifica che le regole del gruppo di sicurezza consentano il traffico sulla porta 22 e che il routing del VPC sia corretto.
- Problemi di risoluzione DNS: per gli endpoint pubblici, assicurati che il tuo VPC disponga di connettività Internet tramite un gateway NAT o un gateway Internet.
- Cross-account accesso negato: verifica che la condivisione delle risorse sia accettata e che l'ARN di configurazione delle risorse sia corretto. Se la politica di autorizzazione appropriata è allegata alla configurazione delle risorse quando l'account di origine crea la condivisione di risorse, sono necessarie le seguenti autorizzazioni: vpc -

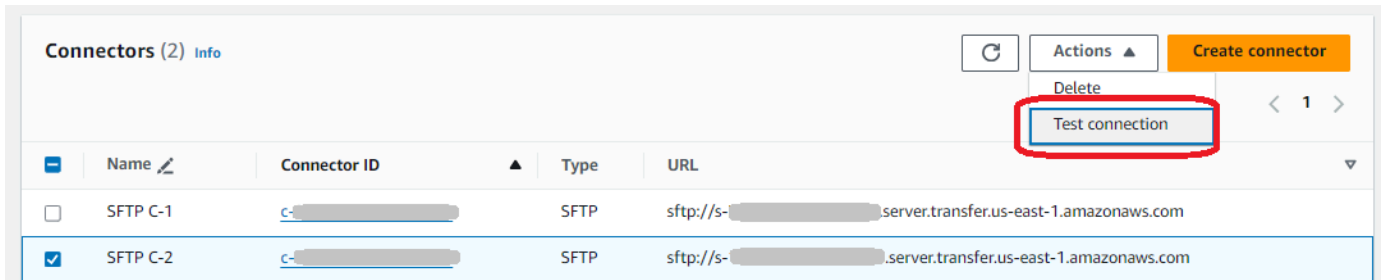
```
lattice:AssociateViaAWSService,,vpc-lattice:AssociateViaAWSService-  
EventsAndStates,vpc-lattice:CreateServiceNetworkResourceAssociation. vpc-  
lattice:GetResourceConfiguration
```

Prova un connettore SFTP

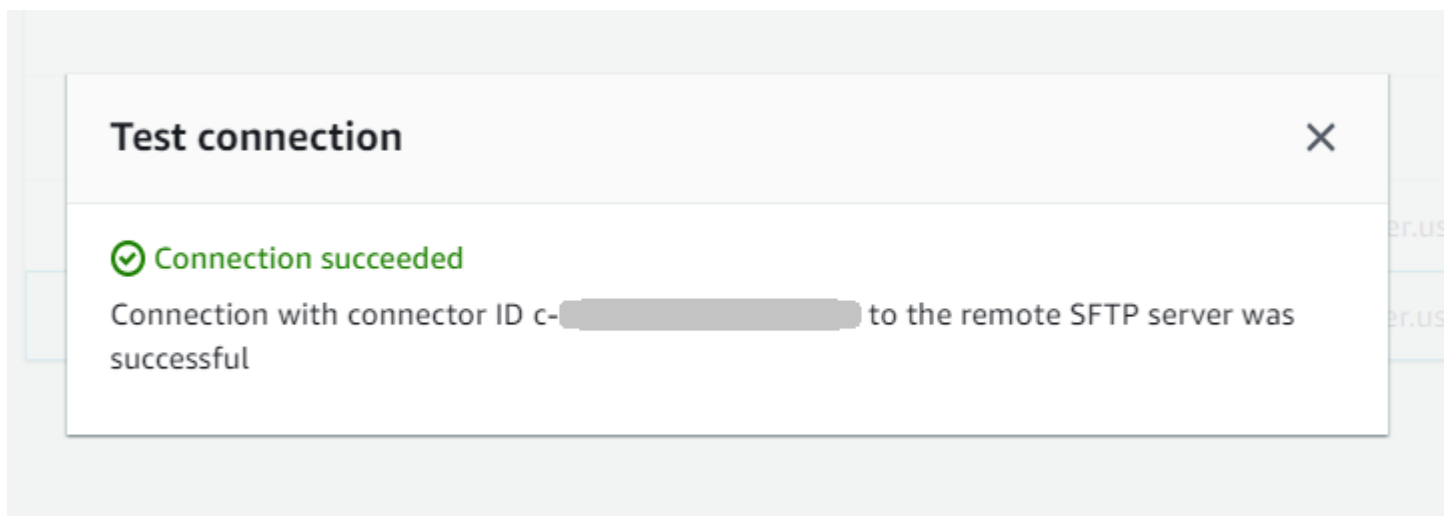
Dopo aver creato un connettore SFTP, si consiglia di testarlo prima di tentare di trasferire qualsiasi file utilizzando il nuovo connettore.

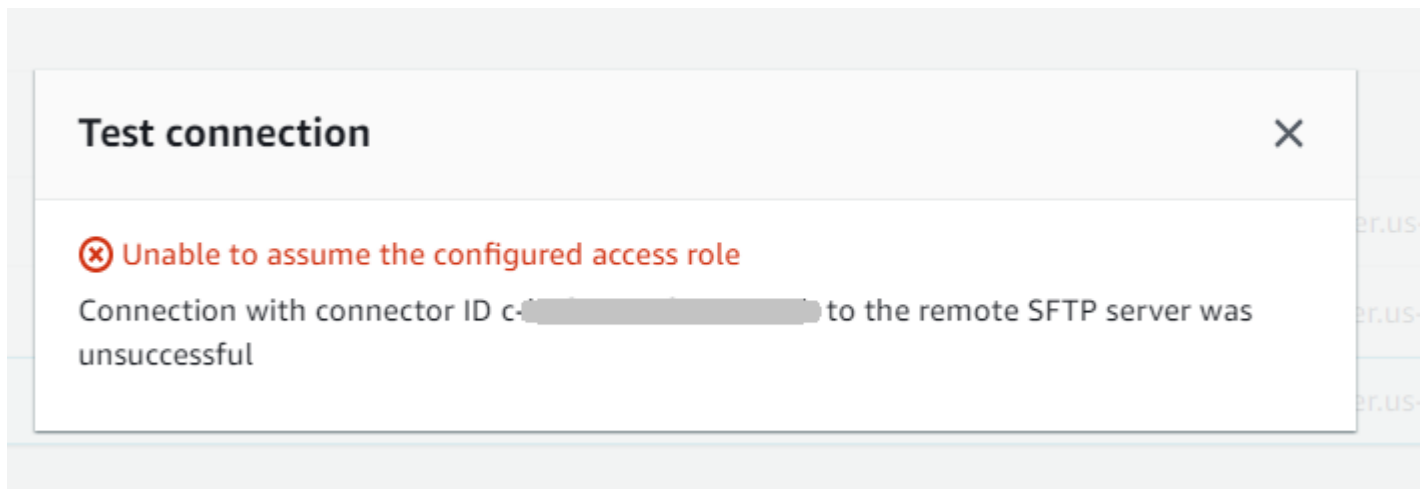
Per testare un connettore SFTP

1. Apri la AWS Transfer Family console all'indirizzo <https://console.aws.amazon.com/transfer/>.
2. Nel riquadro di navigazione a sinistra, scegli Connettori SFTP 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](#).

Connettività VPC per connettori SFTP

AWS Transfer Family I connettori SFTP supportano la connettività ai server SFTP remoti tramite i tuoi ambienti VPC utilizzando Amazon VPC Lattice. Ciò ti consente di connetterti a server SFTP ospitati privatamente o di indirizzare il traffico Internet attraverso i controlli di sicurezza del tuo VPC e utilizzare i tuoi gateway NAT e indirizzi IP elastici.

Tipi di uscita

I connettori SFTP possono utilizzare uno dei due tipi di uscita:

- Servizio gestito (impostazione predefinita): il connettore utilizza gateway NAT e indirizzi IP di proprietà di per AWS Transfer Family instradare le connessioni sulla rete Internet pubblica.
- VPC_LATTICE: il connettore indirizza il traffico attraverso l'ambiente VPC utilizzando Resource Access. Cross-VPC

Quando utilizzare la connettività VPC

Utilizza la connettività VPC per i connettori SFTP in questi scenari:

- Server SFTP privati: Connettiti ai server SFTP accessibili solo dal tuo VPC.

- On-premises connettività: Connettiti ai server SFTP locali tramite AWS Direct Connect o connessioni AWS Site-to-Site VPN.
- Indirizzi IP personalizzati: utilizza i tuoi gateway NAT e indirizzi IP elastici, inclusi gli scenari BYOIP.
- Controlli di sicurezza centralizzati: indirizza i trasferimenti di file attraverso i controlli centrali dell'organizzazione. ingress/egress

Requisiti

Prima di creare un connettore VPC_ LATTICE-enabled SFTP, è necessario:

- VPC e infrastruttura correlata (sottoreti, tabelle di routing, gruppi di sicurezza)
- Resource Gateway nel tuo VPC (minimo due zone di disponibilità)
- Configurazione delle risorse che specifica il server SFTP di destinazione

Per istruzioni di configurazione dettagliate, vedere. [Creare un connettore VPC_ SFTP LATTICE-enabled](#) E, per esempi, vedi [Esempi di connettività VPC per connettori SFTP](#).

Utilizzo dei connettori SFTP

Questo argomento descrive come eseguire le operazioni supportate sui file utilizzando il connettore SFTP. Puoi anche trovare esempi di comandi per eseguire queste operazioni selezionando i dettagli del connettore sulla AWS Transfer Family console all'indirizzo <https://console.aws.amazon.com/transfer/>.

Dopo aver creato un connettore SFTP, è possibile utilizzarlo per eseguire le seguenti operazioni sui file sul server SFTP remoto a cui è associato.

- Invia file da Amazon S3 al server SFTP remoto.
- Recupera i file dal server SFTP remoto su Amazon S3.
- Elenca file e sottocartelle da una directory sul server SFTP remoto.
- Eliminare, rinominare o spostare file e directory sul server SFTP remoto.

Per i dettagli sulla creazione di connettori, vedere. [Creazione di connettori SFTP](#)

Argomenti

- [Trasferimento dei file](#)
- [Elenca il contenuto di una directory remota](#)
- [Spostare, rinominare o eliminare file o directory sul server remoto](#)

Trasferimento dei file

Argomenti

- [Invia e recupera file utilizzando un connettore SFTP](#)

Invia e recupera file utilizzando un connettore SFTP

Per inviare e recuperare file utilizzando un connettore SFTP, si utilizza l'operazione [StartFileTransfer](#) API e si specificano i seguenti parametri, a seconda che si stiano inviando file (trasferimenti in uscita) o ricevendo file (trasferimenti in entrata). Tieni presente che ogni `StartFileTransfer` richiesta può contenere 10 percorsi distinti.

Note

Per impostazione predefinita, i connettori SFTP elaborano un file alla volta, trasferendo i file in sequenza. È possibile accelerare le prestazioni di trasferimento facendo in modo che i connettori creino sessioni simultanee con server remoti che supportano sessioni simultanee dello stesso utente ed elaborino fino a 5 file in parallelo.

Per abilitare le connessioni simultanee per qualsiasi connettore, è possibile modificare l'impostazione Numero massimo di connessioni connesse durante la creazione o l'aggiornamento di un connettore. Per informazioni dettagliate, vedi [Crea un connettore SFTP con uscita gestita dal servizio](#).

- 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 `/amzn-s3-demo-source-bucket/file1.txt` e `/amzn-s3-demo-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 *amzn-s3-demo-source-bucket* con il tuo bucket.

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt /amzn-s3-demo-source-bucket/file2.txt \
  --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

Per recuperare i file, specificate i parametri `retrieve-file-paths` and `local-directory-path`. L'esempio seguente recupera i file `/my/remote/file2.txt` sul server SFTP del partner / `my/remote/file1.txt` e li colloca nella posizione Amazon S3 `/amzn-s3-demo-bucket/`. *prefix*. 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 /amzn-s3-demo-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 `/amzn-s3-demo-source-bucket/file1.txt` `/users/marymajor/test-connectors/file1.txt`

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt \
  --remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --
region us-east-2
```

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 l'operazione 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 `/amzn-s3-demo-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 /amzn-s3-demo-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 omissso 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 omissso 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 200.000 articoli).

Di seguito è riportato un esempio del contenuto del file di output (`c-AAAA1111BBBBB2222C-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"
}
```

Spostare, rinominare o eliminare file o directory sul server remoto

Argomenti

- [Sposta o rinomina file o directory sul server SFTP remoto](#)
- [Eliminare file o directory sul server SFTP remoto](#)

Sposta o rinomina file o directory sul server SFTP remoto

È possibile utilizzare un connettore SFTP per spostare o rinominare file e directory su un server SFTP remoto. Si noti che il server remoto deve supportare queste operazioni per una corretta elaborazione tramite connettori.

Alcuni casi d'uso comuni sono i seguenti.

- Un server remoto genera o riceve un nuovo file ogni ora, con lo stesso nome di file ma un timestamp diverso. Per mantenere aggiornata la cartella principale (in modo che contenga solo il file più recente), puoi utilizzare un connettore per spostare i file più vecchi in una cartella archiviata.
- Utilizza un connettore per elencare tutti i file in una directory remota, quindi trasferisci tutti i file nell'archivio locale. È quindi possibile utilizzare un connettore per spostare i file in una cartella archiviata sul server remoto.

È necessario utilizzare una `StartRemoteMove` chiamata per ogni file o directory che si desidera elaborare, poiché il comando accetta come argomenti un unico file o directory di origine e destinazione. Tuttavia, è possibile accelerare le prestazioni facendo in modo che i connettori creino sessioni simultanee con server remoti che supportano sessioni simultanee dello stesso utente e move/rename fino a 5 file in parallelo.

L'esempio seguente sposta un file sul server SFTP remoto da `/source/folder/sourceFile` a `/destination/targetFile` e restituisce un identificatore univoco per l'operazione.

```
aws transfer --connector-id c-AAAA1111BBBB2222C start-remote-move \  
  --source-path /source/folder/sourceFile --target-path /destination/targetFile
```

Note

Per le move/rename operazioni, Transfer Family utilizza il SFTP `SSH_FXP_RENAME` comando standard per eseguire l' move/rename operazione.

Eliminare file o directory sul server SFTP remoto

È possibile utilizzare un connettore SFTP per eliminare file o directory su un server SFTP remoto. Si noti che il server remoto deve supportare queste operazioni per una corretta elaborazione tramite connettori.

 Note

Le operazioni di eliminazione per le directory remote sono supportate solo per le directory vuote.

Alcuni casi d'uso comuni sono i seguenti.

- Utilizzi un connettore per recuperare un file da un server SFTP remoto, archivarlo nel bucket Amazon S3 e quindi crittografarlo. Infine, puoi utilizzare un connettore per eliminare il file non crittografato sul server remoto.
- Utilizza un connettore per elencare tutti i file in una directory remota, quindi trasferisci tutti i file nell'archivio locale. È quindi possibile utilizzare un connettore per eliminare tutti i file trasferiti. Se preferisci, puoi anche eliminare la directory remota.

È necessario utilizzare una `StartRemoteDelete` chiamata per ogni file o directory che si desidera eliminare, poiché il comando accetta un singolo file o directory come argomento. Tuttavia, puoi accelerare le prestazioni facendo in modo che i connettori creino sessioni simultanee con server remoti che supportano sessioni simultanee dello stesso utente ed eliminino fino a 5 in files/directories parallelo.

L'esempio seguente elimina un file sul server SFTP remoto nel percorso `/delete/folder/deleteFile` e restituisce un identificatore univoco per l'operazione.

```
aws transfer start-remote-delete --connector-id c-AAAA1111BBBB2222C \  
--delete-path /delete/folder/deleteFile
```

 Note

Per l'operazione di eliminazione, Transfer Family utilizza il `SSH_FXP_REMOVE` comando standard per eliminare un file e `SSH_FXP_RMDIR` per eliminare una directory.

Monitoraggio dei connettori SFTP

È possibile monitorare lo stato delle operazioni del connettore utilizzando uno dei seguenti modi. Scegliete l'approccio più adatto alle vostre esigenze.

Utilizza l'API del connettore per interrogare lo stato delle richieste di trasferimento di file

Per tenere traccia dell'avanzamento di un'operazione di trasferimento di file, si utilizza l'operazione [ListFileTransferResults](#) API, che restituisce aggiornamenti in tempo reale e informazioni dettagliate sullo stato di ogni singolo file trasferito in una specifica operazione di trasferimento di file. È possibile specificare il trasferimento del file fornendo il relativo ID connettore e l'ID di trasferimento. L'esempio seguente restituisce un elenco di file per Connector ID a-11112222333344444 e aa1b2c3d4-5678-90ab-cdef-EXAMPLE11111 Transfer-ID.

```
aws transfer list-file-transfer-results --connector-id a-11112222333344444 --transfer-id aa1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Note

I risultati del trasferimento dei file sono disponibili fino a 7 giorni dopo la chiamata all'operazione `ListFileTransferResults` API.

È inoltre possibile visualizzare registri ed eventi per le richieste di trasferimento di file che utilizzano connettori SFTP. EventBridge Gli eventi Amazon per Transfer Family sono descritti in [Eventi del connettore SFTP](#). Per informazioni su come visualizzare le voci del CloudWatch registro Transfer Family, vedere [Visualizzazione dei flussi di log di Transfer Family](#).

Visualizza gli eventi del connettore SFTP in Amazon EventBridge

Per ogni operazione eseguita dai connettori SFTP, Transfer Family genera e invia automaticamente eventi al bus eventi predefinito nel tuo EventBridge account Amazon. Gli eventi contengono metadati dettagliati sull'operazione, incluso lo stato dell'operazione. È possibile sottoscrivere questi eventi in EventBridge, applicare filtri su criteri di eventi specifici, come lo stato dell'operazione, e attivare automaticamente azioni a valle in base allo stato. Per i dettagli sugli eventi generati dalle operazioni del connettore SFTP, vedere. [Eventi del connettore SFTP](#)

Visualizza i log dei connettori SFTP in Amazon CloudWatch

Tutte le operazioni del connettore SFTP generano log in dettagliati. CloudWatch Ad esempio, le voci di registro generate dai connettori SFTP, vedere. [Esempi di voci di registro per i connettori SFTP](#)

Monitoraggio dei connettori di tipo VPC in uscita

I connettori di tipo VPC in uscita offrono funzionalità e considerazioni di monitoraggio aggiuntive rispetto ai connettori standard gestiti dal servizio:

Monitoraggio dello stato del connettore

I connettori VPC_LATTICE includono informazioni aggiuntive per aiutarti a monitorare lo stato di approvvigionamento e operativo:

- **EgressType** campo: Mostra VPC i connettori di tipo di uscita VPC_LATTICE
- **EgressConfig** campo: Contiene l'ARN di configurazione delle risorse e le informazioni sulla porta

Monitora lo stato del connettore utilizzando l'`describe-connector` API:

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Monitoraggio dei costi di VPC Lattice

I connettori di tipo VPC in uscita comportano cariche VPC Lattice aggiuntive che è necessario monitorare:

- **Costi del fornitore di risorse:** ti verranno fatturati 0 USD. 006/GB per l'elaborazione dei dati in qualità di fornitore di risorse (fatturato direttamente da VPC Lattice)
- **Risorse a carico dei consumatori:** AWS Transfer Family assorbe 0\$. 01/GB costi legati al consumo di risorse (primo 1 PB)
- **Tariffe NAT Gateway:** per gli endpoint pubblici accessibili tramite VPC, potrebbero essere applicati costi aggiuntivi per NAT Gateway e trasferimento dati
- **Spese Transfer Family:** Standard \$0. 40/GB si applicano ancora le tariffe per l'elaborazione dei dati

Monitora l'utilizzo e i costi di VPC Lattice tramite la console AWS Cost and Billing, filtrando in base al servizio VPC Lattice.

Monitoraggio della rete per connettori VPC

Monitora l'attività e le prestazioni della rete per i connettori di tipo VPC in uscita:

- Registri di flusso VPC: abilita i log di flusso VPC per monitorare i modelli di traffico di rete tra Resource Gateway e server SFTP
- Registri di accesso VPC Lattice: VPC Lattice fornisce registri di accesso che source/destination mostrano indirizzi IP, tempi di connessione e volumi di trasferimento dati
- Monitoraggio dei gruppi di sicurezza: monitora le regole e i modelli di traffico dei gruppi di sicurezza per garantire controlli adeguati degli accessi alla rete
- Monitoraggio della risoluzione DNS: monitora i tempi e gli errori di risoluzione DNS per gli endpoint della rete di servizio

Esempio di registrazione del registro di accesso VPC Lattice:

```
{
  "eventTimestamp": "2025-01-16T20:59:08.531Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-1:123456789012:servicenetwork/sn-1234567890abcdef0",
  "sourceVpcArn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-12345678",
  "resourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-12345678",
  "protocol": "tcp",
  "sourceIpPort": "10.0.1.100:33760",
  "destinationIpPort": "10.0.2.200:22",
  "gatewayIpPort": "10.0.1.150:1769",
  "resourceIpPort": "10.0.2.200:22"
}
```

Risoluzione dei problemi tramite monitoraggio

Utilizza i dati di monitoraggio per risolvere i problemi più comuni del connettore VPC:

- Stato IN SOSPESO: monitora l'avanzamento della risoluzione DNS e attendi lo stato ATTIVO prima di tentare i trasferimenti
- Timeout di connessione: controlla i log di flusso VPC e le regole del gruppo di sicurezza per il traffico bloccato sulla porta 22
- Errori di trasferimento: esamina i CloudWatch log per messaggi di errore dettagliati e i log di accesso VPC Lattice per problemi a livello di rete
- Problemi di prestazioni: monitora i log di accesso a VPC Lattice per i tempi di connessione e le metriche di throughput

Gestione dei connettori SFTP

Questo argomento descrive come visualizzare e aggiornare 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. Questi indirizzi non sono dedicati esclusivamente al tuo account.

Se hai bisogno di indirizzi IP dedicati e prevedibili, configura i connettori con l'uscita VPC-based . Per ulteriori informazioni, consulta [the section called “Crea un connettore SFTP con uscita VPC-based”](#).

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
```

Aggiornamento delle impostazioni di connettività VPC

Puoi aggiornare le impostazioni di connettività VPC per i connettori esistenti, incluso il passaggio tra i tipi di uscita gestiti dal servizio e VPC o la modifica dell'ARN di configurazione delle risorse.

Per passare un connettore dall'uscita gestita dal servizio a quella in uscita VPC:

```
aws transfer update-connector \
  --connector-id connector-id \
  --egress-type VPC \
  --egress-config ResourceConfigurationArn=resource-configuration-arn
```

Per aggiornare l'ARN di configurazione delle risorse per un connettore VPC_: LATTICE-enabled

```
aws transfer update-connector \  
  --connector-id connector-id \  
  --egress-config ResourceConfigurationArn=new-resource-configuration-arn
```

Note

Quando si aggiornano le impostazioni di connettività VPC, lo stato del connettore cambierà PENDING durante il processo di riconfigurazione. Monitora lo stato del connettore utilizzando il `describe-connector` comando.

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.

Monitoraggio dello stato del connettore VPC

I LATTICE-enabled connettori VPC_ includono informazioni aggiuntive sullo stato per aiutarti a monitorare il processo di provisioning:

- Stato: mostra PENDING, o ACTIVE ERRORED
- EgressType: Spettacoli VPC o SERVICE_MANAGED
- EgressConfig: contiene l'ARN di configurazione delle risorse per i connettori VPC
- Errore: fornisce informazioni dettagliate sull'errore se il connettore è in uno stato ERRORED

Per i connettori VPC, il `ServiceManagedEgressIpAddresses` campo sarà nullo poiché il traffico utilizza invece i tuoi indirizzi IP VPC.

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 [DescribeConnector](#) all'API.

Scalabilità e quote per i connettori SFTP

Argomenti

- [Quote per i connettori SFTP](#)
- [Ridimensionamento dei connettori SFTP](#)

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

Nome	Predefinita	Adattabile
Dimensione massima della coda per i trasferimenti di file in sospeso	1000	No
Dimensione massima dei file	150 gibibyte (GiB)	No
Tempo massimo di trasferimento per file	12 ore	No
Tempo massimo di attesa della richiesta per file	12 ore	No
Larghezza di banda massima per i connettori per account (entrambi i connettori SFTP e AS2 contribuiscono a questo valore)	50 MBps	No
Numero massimo di elementi per le operazioni di elenco delle directory	200.000	No

Note

Per impostazione predefinita, i connettori SFTP elaborano un file alla volta, trasferendo i file in sequenza. È possibile accelerare le prestazioni di trasferimento facendo in modo che i connettori creino sessioni simultanee con server remoti che supportano sessioni simultanee dello stesso utente ed elaborino fino a 5 file in parallelo.

Per abilitare le connessioni simultanee per qualsiasi connettore, è possibile modificare l'impostazione Numero massimo di connessioni connesse durante la creazione o l'aggiornamento di un connettore. Per informazioni dettagliate, vedi [Crea un connettore SFTP con uscita gestita dal servizio](#).

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

Ridimensionamento dei connettori SFTP

Questa sezione descrive le considerazioni su come scalare i carichi di lavoro dei connettori AWS Transfer Family SFTP. È necessario tenere conto delle seguenti tre quote che si applicano quando si desidera scalare i carichi di lavoro con connettori SFTP.

- La dimensione massima della coda. Si riferisce al numero massimo di operazioni in sospeso nella coda di un connettore che sono state richieste. Un'operazione in sospeso si riferisce a qualsiasi richiesta di trasferimento inviata in precedenza che non è stata ancora completata, con successo o meno.

[La profondità massima di coda per le richieste in sospeso è attualmente fissata a 1.000 per connettore \(come definita nelle AWS Transfer Family quote di servizio\).](#) I tuoi carichi di lavoro possono superare questo limite di servizio quando richiedi migliaia di operazioni di trasferimento in un breve periodo e riceverai un messaggio `ThrottlingException` con il messaggio `Exceeded maximum pending requests`. Se i tuoi carichi di lavoro sono soggetti a questa quota, contatta il team di assistenza Transfer Family tramite Supporto AWS o il team del tuo account per discutere dei tuoi requisiti di scalabilità.

Puoi anche eseguire una o entrambe le seguenti azioni.

- Distribuisce i volumi di file su più connettori.
- Fai in modo che i tuoi connettori creino sessioni simultanee con il server remoto per elaborare più richieste dalla coda in parallelo.
- Il numero di sessioni simultanee. Per impostazione predefinita, un connettore SFTP trasferisce un file alla volta, trasferendo i file in sequenza dalla relativa coda.

È possibile accelerare le prestazioni di trasferimento facendo in modo che i connettori trasferiscano più file in parallelo. È possibile creare sessioni simultanee con server remoti che supportano

sessioni simultanee dello stesso utente ed elaborare fino a 5 file in parallelo. Quando crei un connettore SFTP, scegli un valore fino a 5 per l'impostazione Numero massimo di connessioni simultanee quando crei o aggiorni il connettore. Per informazioni dettagliate, vedi [Crea un connettore SFTP con uscita gestita dal servizio](#).

- La frequenza delle richieste. **StartFileTransfer** È possibile richiedere fino a 100 percorsi di file al secondo per il trasferimento con ogni connettore SFTP. I percorsi dei file richiesti vengono aggiunti alla coda dei connettori per l'elaborazione. È possibile utilizzare il `StartFileTransfer` comando in modo ricorsivo per richiedere fino a 100 percorsi di file al secondo per connettore, indipendentemente dal numero di file forniti in un singolo comando. `StartFileTransfer`

Architetture di riferimento che utilizzano connettori SFTP

Questa sezione elenca i materiali di riferimento disponibili per la configurazione di flussi di lavoro di trasferimento automatico dei file utilizzando connettori SFTP. Puoi progettare le tue architetture basate sugli eventi utilizzando gli eventi del connettore SFTP in Amazon EventBridge, per orchestrare tra l'azione di trasferimento dei file e le azioni di pre e post-elaborazione in AWS.

Post del blog

Il seguente post sul blog fornisce 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 AWS Transfer Family SFTP e crittografia PGP](#).

Workshop

- Il seguente workshop fornisce laboratori pratici per la configurazione dei connettori SFTP e l'utilizzo dei connettori per inviare o recuperare file da server SFTP remoti: [Transfer Family - workshop SFTP](#).
- [Il seguente workshop offre laboratori pratici per creare flussi di lavoro completamente automatizzati e basati sugli eventi che prevedono il trasferimento di file da o verso server SFTP esterni ad Amazon S3 e la comune pre- e post-elaborazione di tali file: workshop MFT. Event-driven](#)

Questo video fornisce una panoramica di questo workshop.

Soluzioni

AWS Transfer Family offre le seguenti soluzioni:

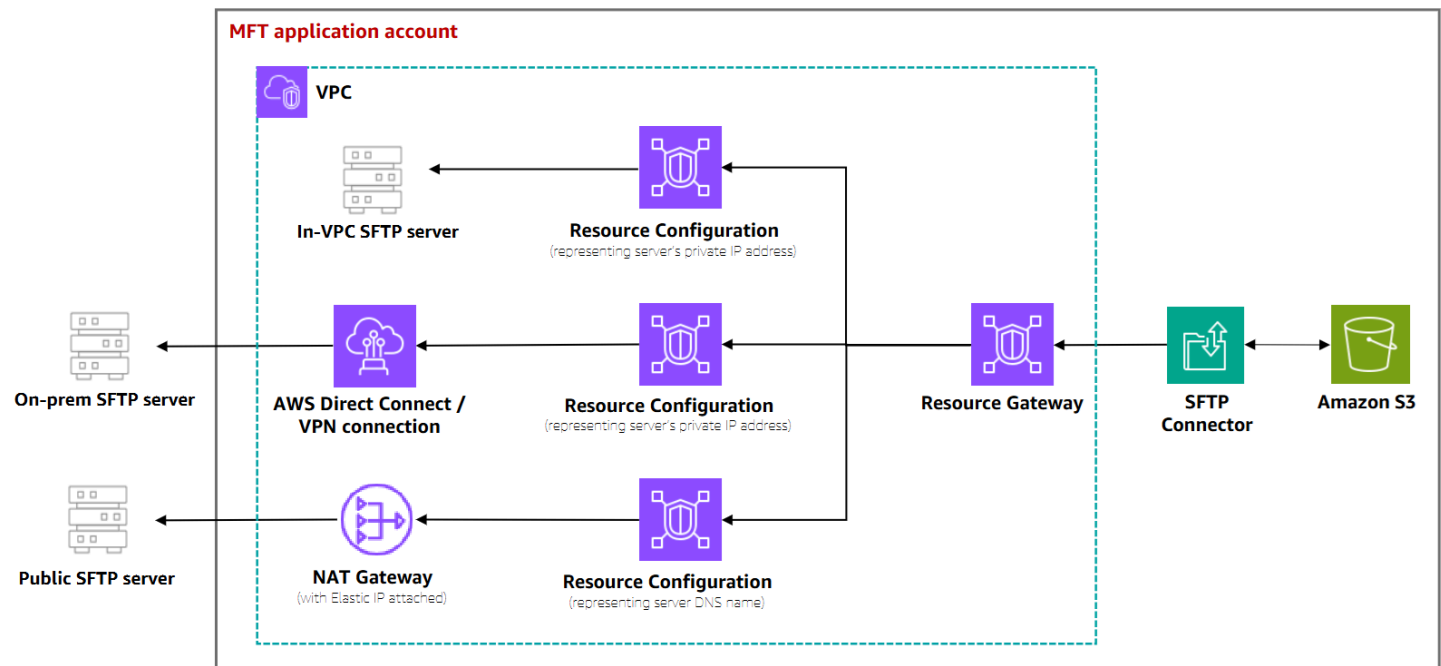
- La [soluzione di sincronizzazione del trasferimento di file](#) fornisce un'architettura di riferimento per automatizzare il processo di sincronizzazione delle directory SFTP remote, incluse intere strutture di cartelle, con i bucket Amazon S3 locali utilizzando un connettore SFTP. Orchestra il processo di elencazione delle directory remote, rilevamento delle modifiche e trasferimento di file nuovi o modificati.
- [Serverlessland - Trasferimento selettivo di file tra server SFTP remoto e S3; l'utilizzo AWS Transfer Family](#) fornisce un modello di esempio per elencare i file archiviati in posizioni SFTP remote e trasferire file selettivi su Amazon S3.

Architetture di riferimento VPC

Le seguenti architetture di riferimento mostrano modelli comuni per l'implementazione dei connettori VPC_ SFTP. LATTICE-enabled Questi esempi ti aiutano a capire dove è necessario creare le risorse VPC Lattice nella tua architettura generale. AWS

Account singolo con infrastruttura di uscita condivisa

In questa architettura, l'infrastruttura di uscita (NAT Gateway, tunnel VPN o Direct Connect) è configurata in un VPC all'interno dello stesso account dei connettori SFTP. Tutti i connettori possono condividere lo stesso Resource Gateway e NAT Gateway.

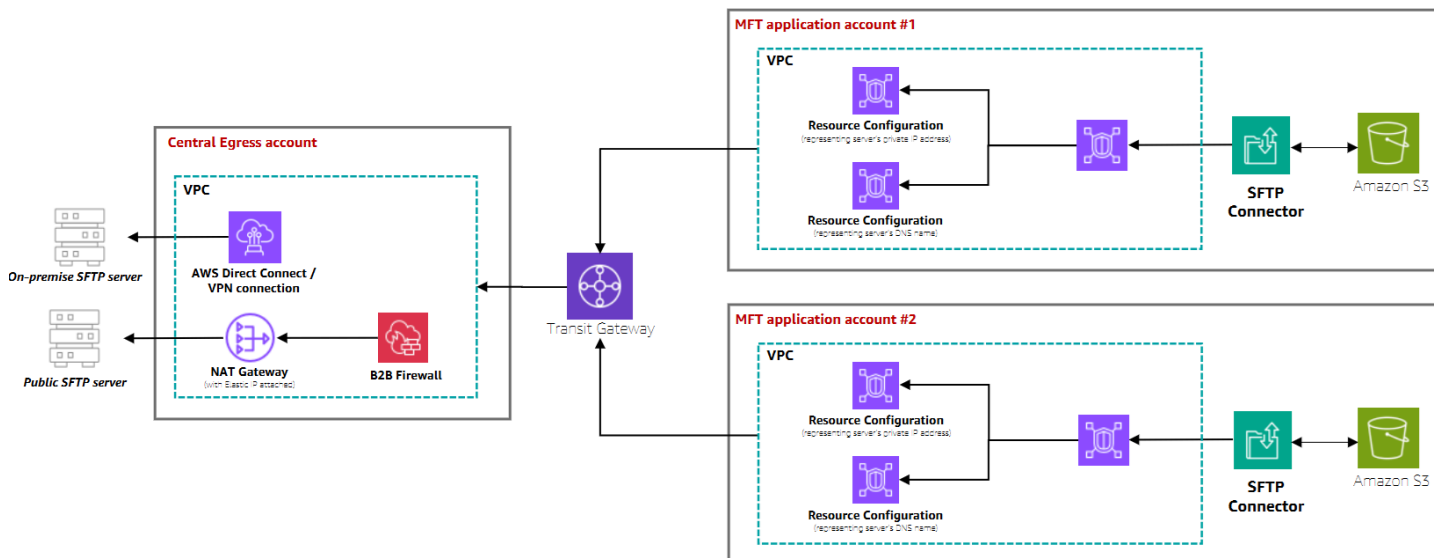


Questo modello è ideale quando:

- Tutti i connettori SFTP sono gestiti all'interno di un unico Account AWS
- L'infrastruttura di uscita è configurata in un VPC all'interno dello stesso account dei connettori SFTP

Cross-account con un'infrastruttura di uscita centralizzata

In questa architettura, l'infrastruttura in uscita (NAT Gateway, tunnel VPN, Direct Connect o firewall B2B) è configurata in un account Egress centrale gestito dal team di rete. I connettori SFTP vengono creati nell'account dell'applicazione MFT gestito dal team di amministrazione di MFT. Cross-account la rete viene stabilita utilizzando Transit Gateway per rispettare le regole di rete esistenti.



Questo schema è ideale quando:

- L'infrastruttura di rete è gestita da un team separato in un account dedicato
- Esistono percorsi esistenti (ad esempio AWS Transit Gateway) tra l'account in cui vengono creati i connettori SFTP e l'account in cui è configurata l'infrastruttura Egress. I connettori SFTP saranno in grado di sfruttare i percorsi esistenti che collegano i due account.
- Sono necessari controlli di sicurezza centralizzati e firewall B2B
- È necessario mantenere la separazione delle mansioni tra i team di rete e quelli addetti alle applicazioni

AWS Transfer Family per AS2

La Dichiarazione di applicabilità 2 (AS2) è una specifica per la RFC-defined trasmissione di file che include potenti meccanismi di protezione e verifica dei messaggi. La protezione di un payload AS2 in transito utilizza la Cryptographic Message Syntax (CMS) con crittografia e firme digitali 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 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. AWS Transfer Family Gli endpoint AS2 sono [certificati Drummond](#) e consentono ai clienti di settori quali vendita al dettaglio, scienze biologiche, produzione, servizi finanziari e servizi di pubblica utilità di effettuare transazioni in sicurezza con i propri partner commerciali.

Quando utilizzi AS2 con Transfer Family, i dati oggetto di transazione sono accessibili in modo nativo per: AWS

- Elaborazione, analisi e apprendimento automatico
- Integrazione con i sistemi di pianificazione delle risorse aziendali (ERP)
- Integrazione con i sistemi di gestione delle relazioni con i clienti (CRM)

Per scambiare file con un partner che dispone di un AS2-enabled server, è necessario:

- Genera una coppia di chiavi pubblica-privata per la crittografia
- Genera una coppia di chiavi pubblica-privata per la firma
- Scambia le chiavi pubbliche con il tuo partner

Important

Gli endpoint del server HTTPS AS2 non sono attualmente supportati. L'utente è responsabile della cessazione del TLS.

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.](#)

Per istruzioni dettagliate sulla configurazione di AS2 in Transfer Family, consulta quanto segue:

1. [Importa certificati AS2](#)
2. [Crea profili AS2](#)
3. [Creare un server AS2](#)
4. [Creare un accordo AS2](#)
5. [Configura i connettori AS2](#)

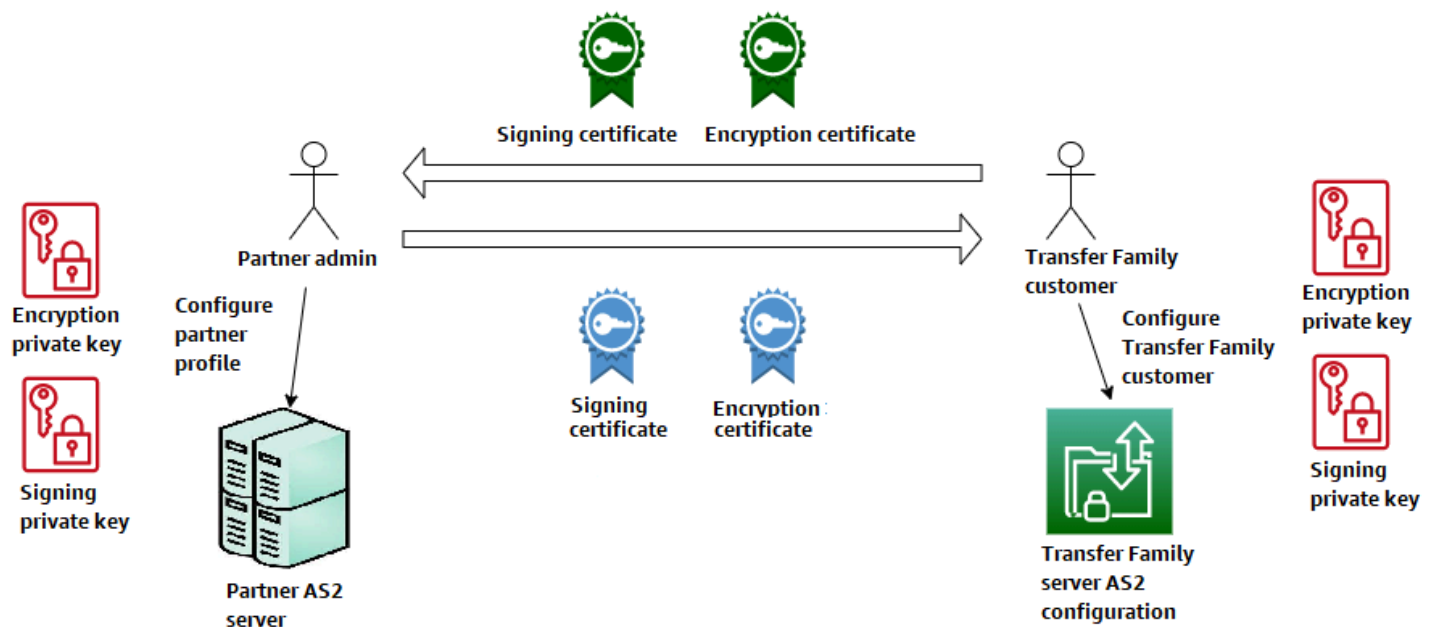
Per un esempio completo, vedi. [Configurazione di una configurazione AS2](#)

Note

Per mostrare il supporto per i modelli AS2 Terraform, aggiungi una reazione con il pollice in su (#) alla richiesta di funzionalità dei modelli [Transfer Family Terraform](#). Puoi anche aggiungere un commento che descriva il tuo caso d'uso.

Casi d'uso di AS2

Se sei un AWS Transfer Family cliente che desidera scambiare file con un partner che dispone di un AS2-enabled server, 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

Inbound-only casi d'uso

- 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 archivarli 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.

Outbound-only casi d'uso

- 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 scambiarsi 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.

Modelli AS2 CloudFormation

Questo argomento fornisce informazioni sui AWS CloudFormation modelli che è possibile utilizzare per distribuire rapidamente server e configurazioni AS2 per AWS Transfer Family. Questi modelli automatizzano il processo di configurazione e aiutano a implementare le migliori pratiche per i trasferimenti di file AS2.

- Il modello AS2 di base è descritto in [Usa un modello per creare uno stack demo Transfer Family AS2](#)
- Il modello AS2 per personalizzare le intestazioni HTTP è descritto in [Personalizza le intestazioni HTTP per i messaggi AS2](#)

Personalizzazione dei modelli AS2

Puoi personalizzare i modelli forniti per soddisfare le tue esigenze specifiche:

1. Scarica il modello dall'URL S3.
2. Modifica il codice YAML per regolare configurazioni come:
 - Impostazioni di sicurezza e configurazioni dei certificati
 - Architettura di rete e impostazioni VPC
 - Opzioni di archiviazione e gestione dei file
 - Preferenze di monitoraggio e notifica
3. Carica il modello modificato nel tuo bucket S3.
4. Implementa il modello personalizzato utilizzando la CloudFormation console o AWS CLI

Important

Quando personalizzi i modelli, assicurati di mantenere le dipendenze tra le risorse e di seguire le migliori pratiche di sicurezza.

Verifica della distribuzione AS2

Dopo aver distribuito un server AS2 utilizzando un modello, puoi testare la configurazione:

1. Controlla gli output dello CloudFormation stack per esempi di comandi e informazioni sugli endpoint.
2. Usa il AWS CLI per inviare un file di test:

```
aws s3api put-object --bucket your-bucket-name --key test.txt --body test.txt  
aws transfer start-file-transfer --connector-id your-connector-id --send-file-  
paths /your-bucket-name/test.txt
```

3. Verifica la consegna dei file nel bucket S3 di destinazione.
4. Controlla CloudWatch i log per verificare la corretta elaborazione e le risposte MDN.

Per test più completi, prendi in considerazione l'utilizzo di client AS2 di terze parti per inviare file al tuo server Transfer Family AS2.

Le migliori pratiche per la distribuzione dei modelli AS2

Segui queste best practice quando usi i modelli AS2: CloudFormation

Sicurezza

Usa certificati robusti e ruotali regolarmente.

Implementa politiche IAM con privilegi minimi.

Limita l'accesso alla rete utilizzando gruppi di sicurezza.

Affidabilità

Implementa su più zone di disponibilità.

Implementa il monitoraggio e la generazione di avvisi in caso di trasferimenti non riusciti.

Imposta nuovi tentativi automatici per i trasferimenti non riusciti.

Performance

Scegliete i tipi di istanza appropriati per il volume di trasferimento.

Implementa le politiche del ciclo di vita di S3 per una gestione efficiente dei file.

Monitora e ottimizza le configurazioni di rete.

Ottimizzazione dei costi

Usa l'auto-scaling per carichi di lavoro variabili.

Implementa le classi di storage S3 per i file più vecchi.

Monitora e regola le risorse in base all'utilizzo effettivo.

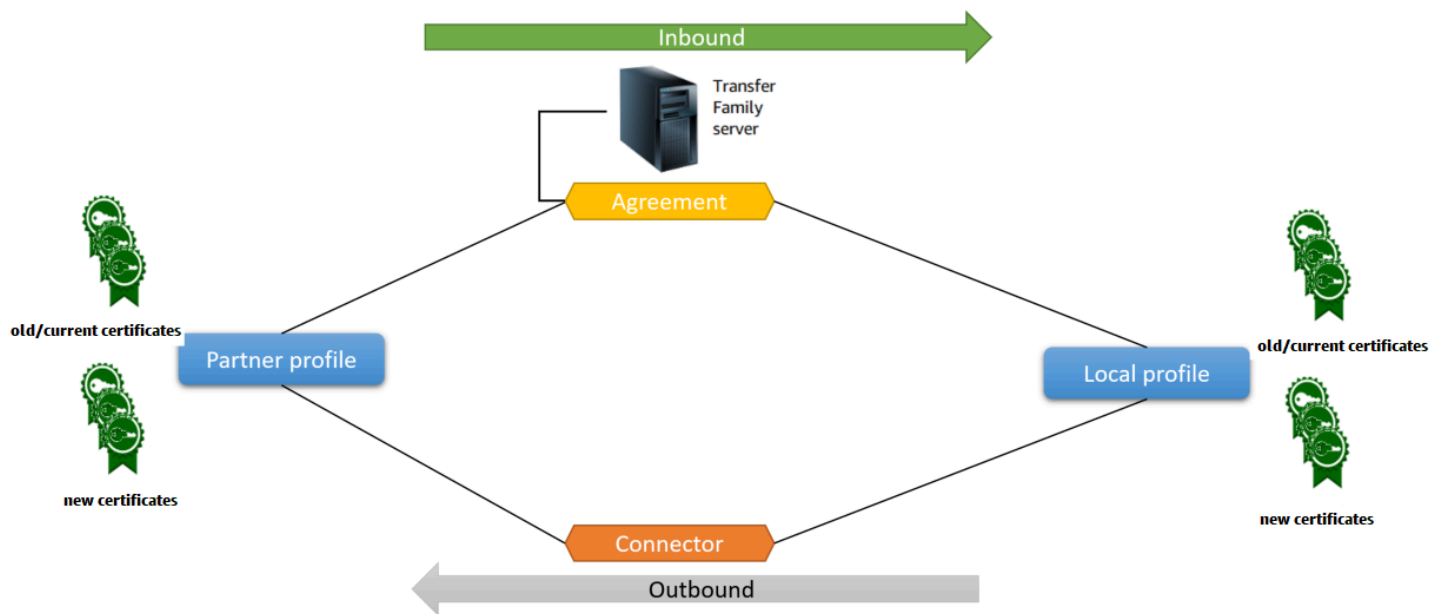
Configurazione di AS2

Per creare un AS2-enabled server, 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. Transfer Family AS2-inbound elabora gli accordi di utilizzo.
- **Certificati:** i certificati a chiave pubblica (X.509) vengono utilizzati nella comunicazione 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 AS2-enabled Transfer Family). Allo stesso modo, un profilo partner definisce l'organizzazione del partner remoto, esterna a Transfer Family.

Sebbene non sia necessario per tutti i AS2-enabled server, 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 esempio completo di configurazione AS2, vedere. [Configurazione di una configurazione AS2](#)

Argomenti

- [Configurazioni AS2](#)
- [Quote e limitazioni AS2](#)
- [Caratteristiche e funzionalità di AS2](#)

Configurazioni 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.

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 TLS-terminating proxy come un Application Load Balancer (ALB) e l'intestazione è presente. X-Forwarded-Proto: https

- Firma: facoltativa
- Compressione: facoltativa (l'unico algoritmo di compressione attualmente supportato è ZLIB)
- Message Disposition Notice (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: sincroni e asincroni
- 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 è necessario utilizzare HTTPS per i trasferimenti in entrata, è possibile terminare TLS su un Application Load Balancer o un Network Load Balancer. Questa procedura è descritta in [Ricevi messaggi AS2 tramite HTTPS](#).

- Trasferimenti in uscita: se fornisci un URL HTTP, devi 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 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	50 MB al secondo	No

Nome	Predefinita	Adattabile
richieste SFTP e AS2 in uscita contribuiscono entrambe a questo valore)		

Quote per la gestione dei segreti

AWS Transfer Family effettua chiamate per Gestione dei segreti AWS 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 [Gestione dei segreti AWS quote](#).

Secrets Manager **GetSecretValue**

Nome	Valore	Description
Frequenza combinata di richieste <code>GetSecretValue</code> API <code>DescribeSecret</code> e frequenza	Ogni regione supportata: 10.000 al secondo	Il numero massimo di transazioni al secondo <code>DescribeSecret</code> e le operazioni <code>GetSecretValue</code> 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 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 separatamente 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

- Server-side TCP keep-alive 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 processed/Warning: messaggio con 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. Self-signed i certificati 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 i server AWS Transfer Family](#)
- 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.
- È possibile collegare un flusso di lavoro di elaborazione file a un server Transfer Family che utilizza il protocollo AS2: tuttavia, i messaggi AS2 non eseguono flussi di lavoro collegati al server.

Caratteristiche e funzionalità di AS2

Le tabelle seguenti elencano le caratteristiche e le funzionalità disponibili per le risorse Transfer Family che utilizzano AS2.

Funzionalità 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
SHA-2 algoritmi crittografici	Sì
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
Non-TLS Trasporto (HTTP)	Sì	Sì ²

Funzionalità	In entrata: ricezione tramite server	In uscita: invio con connettore
MDN sincrono	Sì	Sì
Compressione dei messaggi	Sì	Sì
MDN asincrono	Sì	Sì
Indirizzo IP statico	Sì	Sì
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) o Application Load Balancer (ALB)
2. Trasporto non TLS in uscita disponibile solo quando la crittografia è abilitata

Gestisci i certificati AS2

Questo argomento illustra come importare e gestire i certificati AS2. L'importazione di certificati è il primo passo nel processo AS2 per Transfer Family.

1. Importazione di certificati
2. [Crea profili AS2](#)
3. [Creare un server AS2](#)
4. [Creare un accordo AS2](#)
5. [Configura i connettori 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, consulta [the section called “Fase 2: Importazione dei certificati come risorse di certificati Transfer Family”](#).

Per specificare un AS2-enabled certificato

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 Configurazione del certificato, per la 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 Utilizzo del certificato, scegli lo scopo di questo certificato. Può essere usato per la crittografia, la firma o entrambi.

Suggerimento: 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.

6. Nella sezione Contenuto del certificato, fornisci un certificato pubblico rilasciato da un partner commerciale o le chiavi pubbliche e private per un certificato locale.

Compila la sezione Contenuto del certificato con i dettagli appropriati.

- Se scegli il Self-signed certificato, non fornisci la catena di certificati.
 - Incolla il testo del certificato e la relativa catena nel campo Certificato e catena di certificati.
 - Se questo certificato è un certificato locale, incollane la chiave privata.
7. 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.

X.509 i certificati hanno `Not Before` e `Not After` date. Tuttavia, questi parametri potrebbero non fornire un controllo sufficiente per gli amministratori. Transfer Family fornisce `Active Date` e `Inactive Date` impostazioni per controllare quale certificato viene utilizzato per i payload in uscita e quale è accettato per i payload in entrata.

Monitoraggio della scadenza dei certificati

Transfer Family pubblica una CloudWatch metrica `Amazon DaysUntilExpiry` dopo l'importazione di un certificato. La metrica indica il numero di giorni tra la data corrente e la data specificata nel certificato. `InactiveDate` La metrica si trova nello spazio dei Transfer AWS nomi nella dashboard delle metriche. CloudWatch

Questa metrica avrà sempre una dimensione `metric` `CertificateId` facoltativamente includerà una dimensione `Descrizione`, se fornita dal cliente nel certificato. Per ulteriori informazioni sulle dimensioni CloudWatch metriche, consulta [Dimension](#) nel riferimento API. CloudWatch

Note

Può essere necessario fino a un giorno intero dopo l'importazione di un `Certificate` for Transfer Family per emettere questa metrica sull'account del cliente.

Puoi utilizzare questa metrica per creare CloudWatch allarmi che ti avvisano quando i certificati stanno per scadere.

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`

Esempio di rotazione dei certificati

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 (imposto da Transfer Family)	INACTIVE DATE (imposto da Transfer Family)	NOT AFTER (imposto 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

Tenere 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

Questo argomento descrive come creare profili da utilizzare nel processo AS2. Un profilo locale definisce l'organizzazione o il «partito» locale (AS2-enabledTransfer Family server). Allo stesso modo, un profilo partner definisce l'organizzazione del partner remoto, esterna a Transfer Family.

1. [Importa certificati AS2](#)
2. Crea profili AS2
3. [Creare un server AS2](#)
4. [Creare un accordo AS2](#)
5. [Configura i connettori 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, consulta [the section called “Fase 3: 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.

Suggerimento: 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, vedere [Importa 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.

Creare un server AS2

Questo argomento fornisce istruzioni per creare un server AS2-enabled Transfer Family, utilizzando la console o un CloudFormation modello. Per un esempio completo di configurazione AS2, vedi. [Configurazione di una configurazione AS2](#) Dopo aver creato un server AS2, puoi aggiungere un accordo al server.

1. [Importa certificati AS2](#)
2. [Crea profili AS2](#)
3. Crea un server AS2
4. [Creare un accordo AS2](#)
5. [Configura i connettori AS2](#)

Argomenti

- [Creare un server AS2 utilizzando la console Transfer Family](#)
- [Usa un modello per creare uno stack demo Transfer Family AS2](#)
- [Creare un accordo AS2](#)

Creare un server AS2 utilizzando la console Transfer Family

Questa procedura spiega come creare un AS2-enabled server utilizzando la console Transfer Family. Se AWS CLI invece desideri utilizzare il, consulta [the section called “Fase 4: Creare un server Transfer Family che utilizzi il protocollo AS2”](#).

Note

È possibile collegare un flusso di lavoro di elaborazione file a un server Transfer Family che utilizza il protocollo AS2: tuttavia, i messaggi AS2 non eseguono flussi di lavoro collegati al server.

Per creare un server AS2-enabled

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:

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID

Select a VPC ID ▼



Create a VPC 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

Cancel

Previous

Next

- a. Per il tipo di endpoint, scegli VPC ospitato per ospitare l'endpoint del tuo server. Per informazioni sulla configurazione dell' VPC-hosted endpoint, 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 del tuo VPC e dagli VPC-connected ambienti, come un data center locale tramite Direct Connect VPN.
 - Connessione Internet: scegli questa opzione per fornire l'accesso tramite Internet e dall'interno del tuo VPC e VPC-connected degli ambienti, ad esempio un data center locale o una VPN. 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

FIPS-enabled gli endpoint non sono supportati per il protocollo AS2.

- e. Scegli Next (Successivo).
6. Nella pagina Scegli un dominio, scegli Amazon S3 per archiviare e accedere ai tuoi file come oggetti utilizzando il protocollo selezionato.

Scegli Next (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 CloudFormation modello autonomo per creare rapidamente un server AS2-enabled Transfer Family. Il modello configura il server con un endpoint Amazon VPC pubblico, certificati, profili locali e partner, un accordo e un connettore.

Il modello di server AS2 di base crea le seguenti risorse:

- Un server AS2-enabled Transfer Family con un endpoint VPC
- Profili AS2 locali e partner con certificati
- Un accordo tra i profili
- Un bucket Amazon S3 per lo storage di file

- Ruoli e politiche IAM richiesti
- CloudWatch configurazione di registrazione

Prima di utilizzare questo modello, tenete 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 Gestione dei segreti AWS per archivarli 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 AS2-enabled Transfer Family da un CloudFormation modello

1. Apri la 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 Scegli un modello esistente.
5. Copia questo link, [modello demo AS2](#), e incollalo nel campo URL di Amazon S3.
6. Scegli Next (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-amzn-s3-demo-bucket`
8. Scegli Next (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 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 Output dello stack e copia il. `TransferExampleAs2Command` È quindi possibile eseguire il comando utilizzando. 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 amzn-s3-demo-bucket --key test.txt && aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId --send-file-paths /amzn-s3-demo-bucket/test.txt
```

 Note

La versione in uso di questo comando contiene i valori effettivi *TransferConnectorId* delle risorse *amzn-s3-demo-bucket* 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 amzn-s3-demo-bucket --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 /amzn-s3-demo-bucket/test.txt
```

Dopo aver eseguito il comando, puoi accedere al tuo bucket Amazon S3 (*amzn-s3-demo-bucket*) 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.

Creare un accordo 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, consulta [the 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.

In alternativa, purché disponga di almeno un server Transfer Family che utilizza il protocollo AS2, seleziona Agreements per ricevere messaggi dal menu AS2 Trading Partners. Quindi, nella schermata Crea accordo, seleziona il server AS2 a cui desideri associare questo accordo.

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. Inoltre, scegli se applicare o meno la firma dei messaggi.
 - Per impostazione predefinita, Enforce message signature è abilitata, il che significa che Transfer Family rifiuta i messaggi non firmati del tuo partner commerciale per questo contratto.
 - Deseleziona questa impostazione per consentire a Transfer Family di accettare messaggi non firmati dal tuo partner commerciale per questo contratto.
 - c. Nella sezione Configurazione della directory di posta in arrivo, fornisci le seguenti informazioni.

- Determina se selezionare o meno Specificare directory separate per archiviare i messaggi AS2, i file MDN e i file di stato JSON.
- Se si seleziona questa opzione, si specificano posizioni separate per i file di payload, i file non riusciti, i file MDN, i file di stato e i file temporanei.
- Se deseleziona questa opzione, tutti i file AS2 vanno nella posizione specificata per la directory di base.
- Per S3 Bucket, scegli un bucket Amazon S3.
- Per Prefix, puoi inserire un prefisso (cartella) da utilizzare per archiviare i file nel bucket.

Ad esempio, se inserisci **amzn-s3-demo-bucket** il tuo bucket e il tuo prefisso, **incoming** i tuoi file AS2 vengono salvati nella cartella. **/amzn-s3-demo-bucket/incoming**

- Per AWS IAM Role, scegli un ruolo che possa accedere al bucket specificato.
 - Per Preserve filename, scegli se conservare i nomi di file originali per i payload di messaggi AS2 in arrivo.
 - Se selezioni questa impostazione, il nome del file fornito dal tuo partner commerciale viene mantenuto quando il file viene salvato in Amazon S3.
 - Se si deseleziona questa impostazione, quando Transfer Family salva il file, il nome del file viene modificato, come descritto in. [Nomi e posizioni dei file](#)
- 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 Contratti della pagina dei dettagli del server.

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.

1. [Importa certificati AS2](#)
2. [Crea profili AS2](#)
3. [Creare un server AS2](#)
4. [Creare un accordo AS2](#)
5. Crea un connettore AS2

Crea un connettore AS2

Questa procedura spiega come creare connettori AS2 utilizzando la AWS Transfer Family console. Se AWS CLI invece desideri utilizzare il, consulta [the 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 per inviare messaggi, dal menu Partner commerciali AS2, quindi scegli Crea connettore AS2.
3. Nella sezione Configurazione del connettore, specifica le seguenti informazioni:
 - URL: immetti l'URL per le connessioni in uscita.
 - Modalità di indirizzamento IP: scegli solo IPv4 (impostazione predefinita) per utilizzare esclusivamente gli indirizzi IPv4 o Dual-stack per supportare sia IPv6 che IPv4. In modalità dual-stack, il connettore preferisce IPv6 quando la risoluzione DNS restituisce risultati IPv6 e utilizza IPv4 quando vengono restituiti solo risultati DNS IPv4.
 - 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 la Chiave gestita da AWS accesso Gestione dei segreti AWS, 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. Tenere presente quanto segue:
- Il Content-Type parametro Preserve S3 è abilitato per impostazione predefinita.
- Se impostato, Transfer Family utilizza Amazon S3 Content-Type associato agli oggetti in S3 anziché avere il tipo di contenuto mappato in base all'estensione del file. Deseleziona questa impostazione se desideri che il servizio mappi il tipo di contenuto dei tuoi messaggi AS2 in base all'estensione del file, anziché utilizzare il tipo di contenuto dell'oggetto S3.
- Per quanto riguarda l'algoritmo di crittografia, non scegliete DES_EDE3_CBC a meno che non dobbiate supportare un client legacy che lo richiede, poiché 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 Autenticazione di base, specificate 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, vedere [Abilita l'autenticazione di base per i connettori AS2](#).

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret

☒ Choose an existing secret

Choose a secret

aws/transfer/...
SFTP connector...

aws/transfer/sftp-connector1
Secret key ...

aws/transfer/c...

You must provide AWS Transfer Family with permission to use the secret key.

6. 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.
7. Dopo aver confermato tutte le impostazioni, scegli Crea connettore AS2 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.

Tipo	Algoritmo
Cifratura TLS	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Tipo	Algoritmo
	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

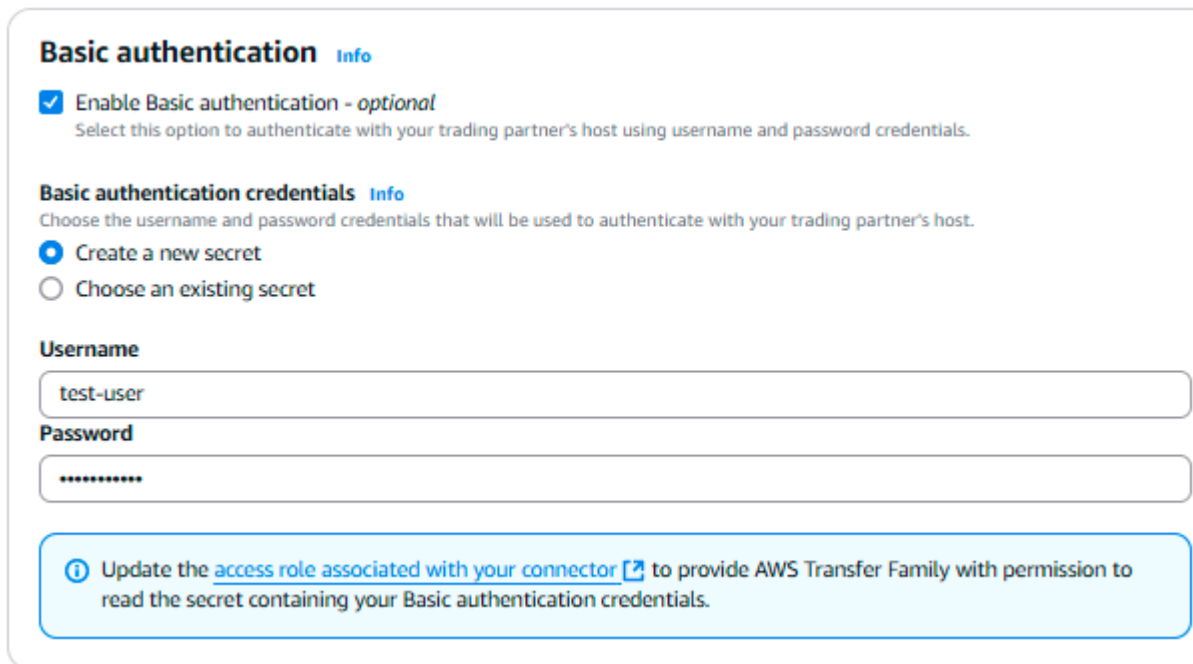
Quando crei o aggiorni un server Transfer Family che utilizza il protocollo AS2, puoi aggiungere l'autenticazione di base per i messaggi in uscita. A tale scopo, è necessario aggiungere informazioni di autenticazione a un connettore.

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.



Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

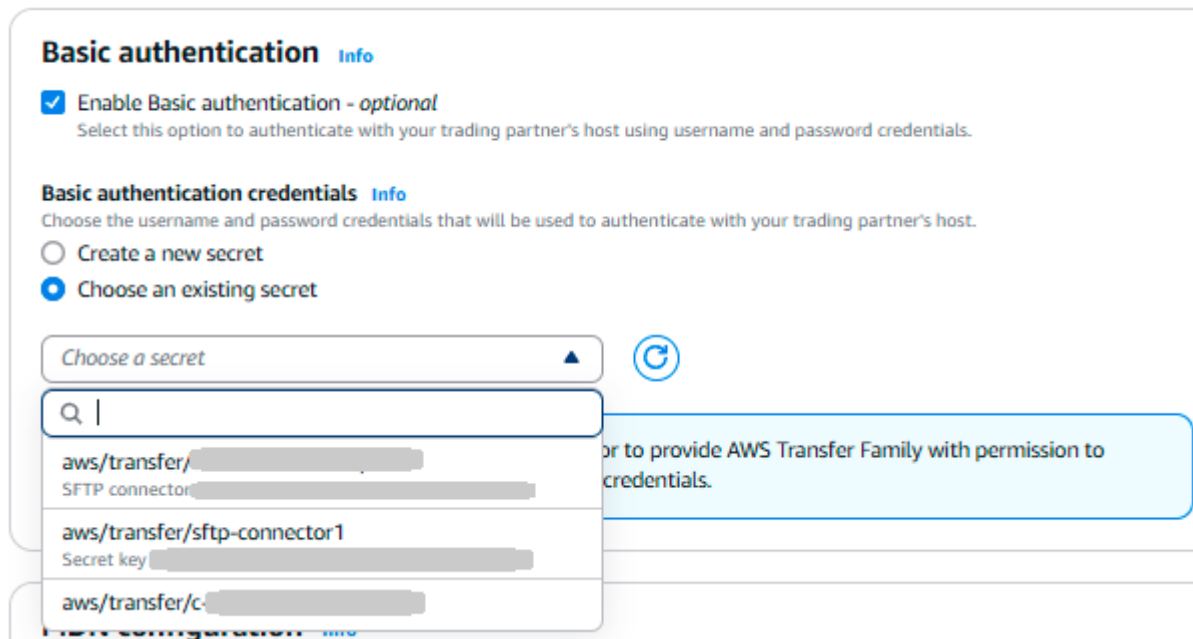
☒ **Create a new secret**
☐ Choose an existing secret

Username
test-user

Password
.....

Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

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](#).



Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☐ Create a new secret
☒ **Choose an existing secret**

Choose a secret

aws/transfer/SFTP connector1
Secret key

aws/transfer/c-

Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

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 Gestione dei segreti AWS. 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 Gestione dei segreti AWS](#)

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.

Basic authentication [Info](#)
☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.
☒ Create a new secret
☐ Choose an existing secret

Username

Password

[i](#) Update the [access role associated with your connector](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

[i](#) Note

Quando crei un nuovo segreto nella console, il nome del segreto segue questa convenzione di denominazione: **/aws/transfer/connector-id, connector-id** dov'è l'ID del

connettore che stai creando. Consideralo quando cerchi di individuare il segreto in Gestione dei segreti AWS.

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, vedere [Crea un segreto in Gestione dei segreti AWS](#).

Crea un segreto in Gestione dei segreti AWS

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. Accedi a Console di gestione AWS e apri la Gestione dei segreti AWS 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 Key/value coppie, scegli la Key/valuescheda.
 - 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 Key/value coppie, scegli la Key/valuescheda.

Scegli Aggiungi riga e, nella sezione Key/valuecoppie, scegli la Key/valuescheda.

- Chiave: Invio**Password**.
 - valore: immettere la password per l'utente.
7. Se desideri fornire una chiave privata, scegli Aggiungi riga e nella sezione Key/value coppie, scegli la Key/valuescheda.
 - 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. Scegli Next (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 (vedi [Configura 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

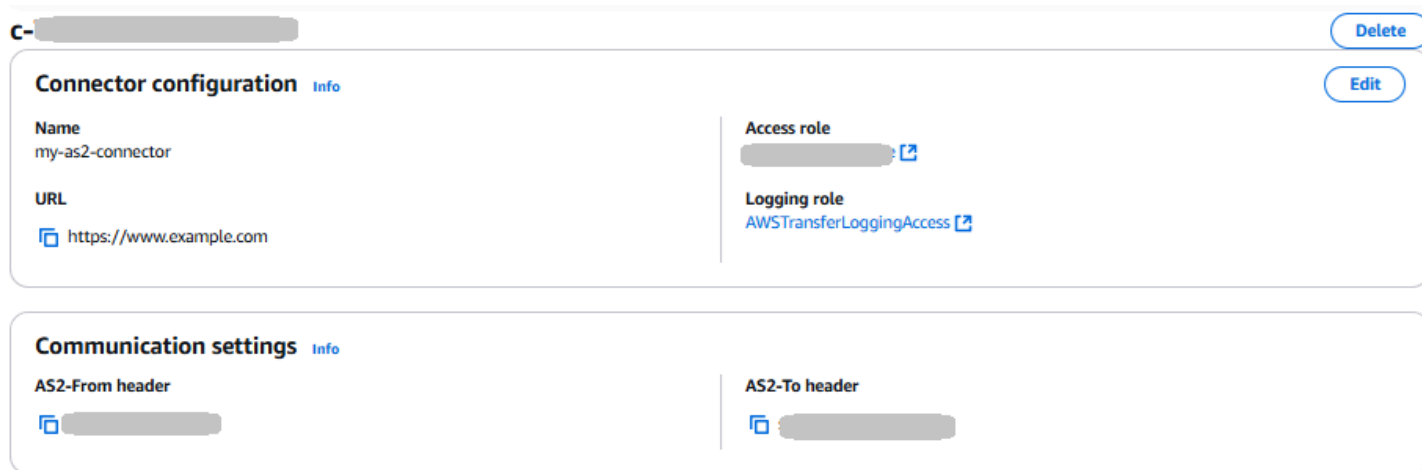
È possibile trovare un elenco di dettagli e proprietà di un AWS Transfer Family connettore AS2 nella AWS Transfer Family console. Le proprietà di un connettore AS2 includono l'URL, i ruoli, i profili, gli mDNS, i tag e le metriche di monitoraggio.

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.



Connector configuration [Info](#) [Delete](#) [Edit](#)

Name my-as2-connector	Access role [redacted] [icon]
URL [icon] https://www.example.com	Logging role AWSTransferLoggingAccess [icon]

Communication settings [Info](#)

AS2-From header [icon] [redacted]	AS2-To header [icon] [redacted]

AS2 configuration

Info

Edit

Local profile

Partner profile

Preserve S3 Content-Type

Compression

Message Subject

Encryption algorithm

Signing algorithm

Enabled

View

AES128_CBC

SHA384

MDN configuration

Info

Edit

Request MDN

Signed MDN

Synchronization

Enabled

Default to message signing algorithm: SHA384

Enabled

Basic authentication

Info

Edit

Basic authentication

Secret

Enabled

aws/transfer/c-

Egress IP details

Info

Service managed static IP addresses of this connector

23.23.130.9

44.196.109.11

3.219.16.7

Tags (1)

Manage tags

Use tags to organize, search, and filter your Connectors. We recommend adding a tag with 'Name' as the key and a unique string as the value to easily identify your Connector.

Find resources

< 1 >

Key

Value

Name

my-as2-connector

AS2 Monitoring

3h 1d 1w

UTC timezone

Refresh

OutboundMessage

OutboundMessage

OutboundFailedMessage

OutboundFailedMessage

No data available. Try adjusting the dashboard time range.

No data available. Try adjusting the dashboard time range.

No data available. Try adjusting the dashboard time range.

No data available. Try adjusting the dashboard time range.

OutboundMessage

OutboundFailedMessage

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 [DescribeConnector](#) all'API.

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

Algoritmo di crittografia	HTTP	HTTPS	Note
			possibile selezionare solo NONE se si utilizza un Application Load Balancer (ALB).

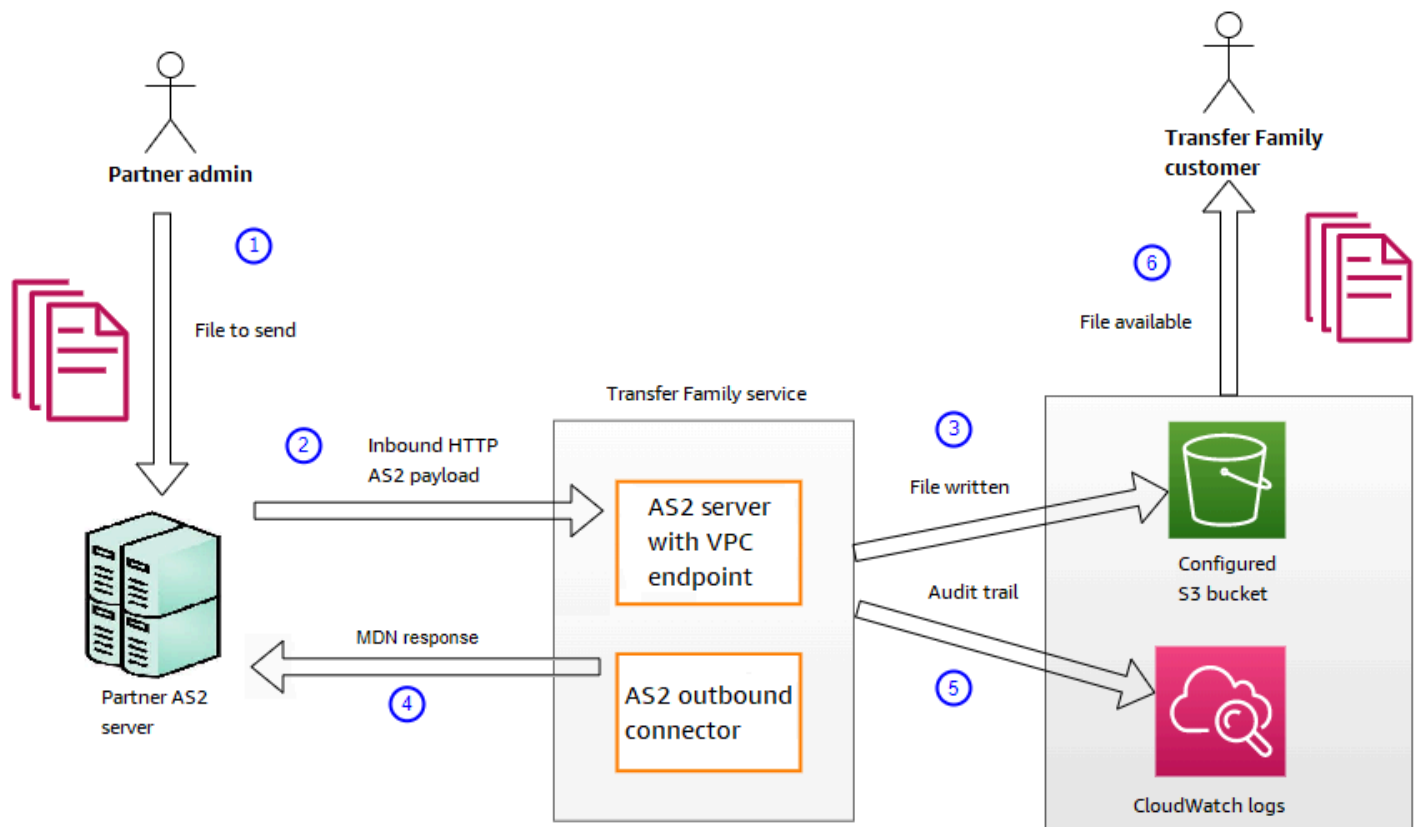
Argomenti

- [Processo di ricezione dei messaggi AS2](#)
- [Invio e ricezione di messaggi AS2 tramite HTTPS](#)
- [Trasferimento di file tramite un connettore AS2](#)
- [Nomi e posizioni dei file](#)
- [Codici di stato](#)
- [File JSON di esempio](#)

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' <code>X-Forwarded-Proto</code> intestazione richiesta per AS2 senza crittografia. Questa intestazione è descritta nel sito web X-Forwarded-Proto developer.mozilla.org.
TLS/SSL terminazione	Supporta la TLS/SSL terminazione	Supporta la TLS/SSL terminazione
TLS reciproco (mTLS)	Transfer Family attualmente non supporta l'utilizzo di un NLB per MTL	Supporto 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, scegli. 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, consulta [Per 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 SSL/TLS Certificato 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 (ALB) 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 SSL/TLS certificato all'ascoltatore.
 - b. In Gestione dei certificati del 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 di integrità per il gruppo target in modo che utilizzi il protocollo HTTP 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 SSL/TLS certificato.

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, la selezione dipende dal fatto che si stia utilizzando un ALB o un NLB.
 - Per un Network Load Balancer (NLB), scegli TCP
 - Per un Application Load Balancer (ALB), scegli HTTP
 - Per Port (Porta), immettere **5080**.
 - Per il tipo di indirizzo IP, scegliete IPv4.
 - Per VPC, scegli il VPC che hai creato per il tuo server Transfer Family AS2.
3. Nella sezione Controlli sanitari, scegli il protocollo Health check.
 - Per un ALB, scegli HTTP
 - Per un NLB, scegli TCP
4. Scegli Next (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 i trasferimenti 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 "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-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.

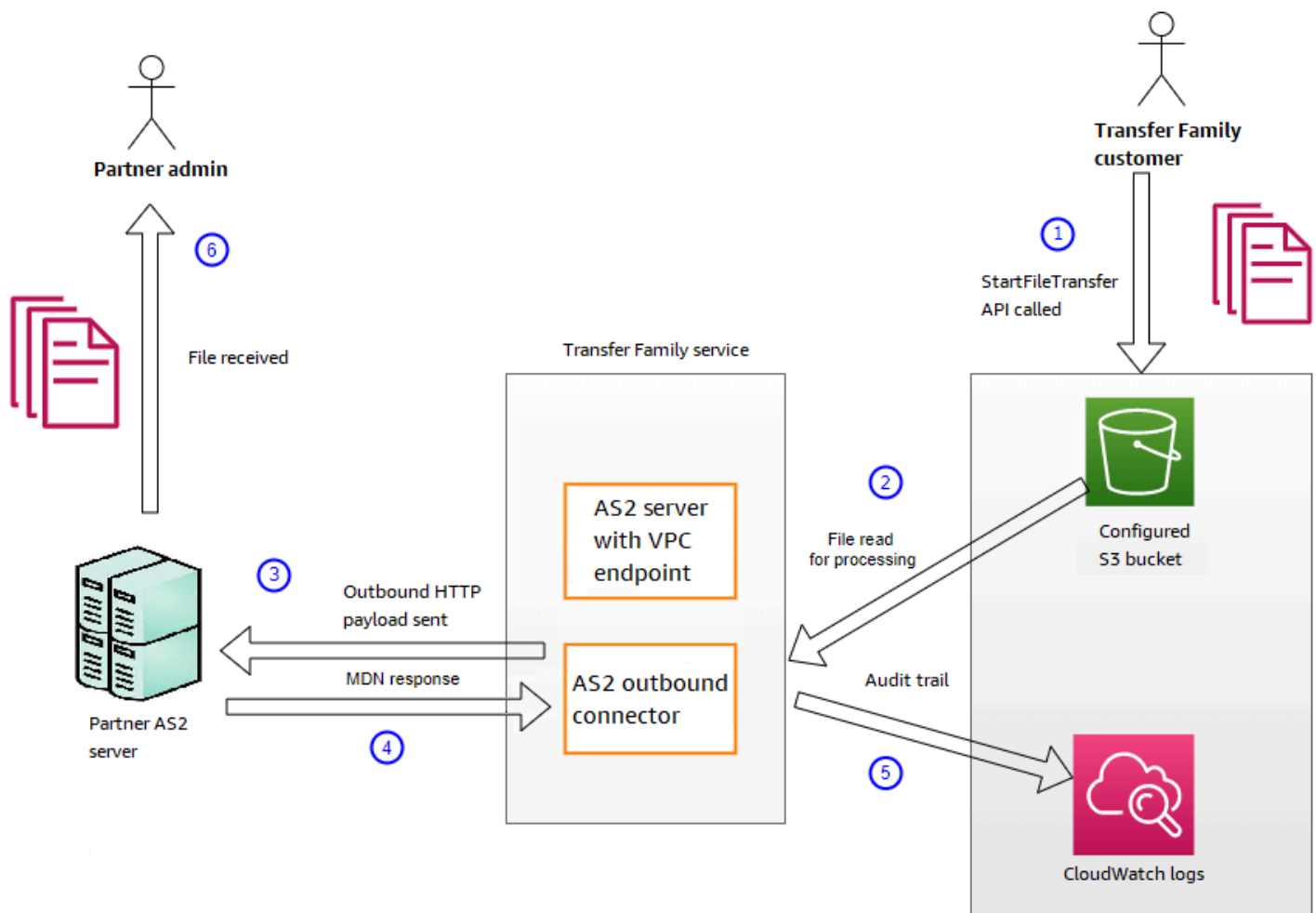
È possibile confermare che il partner ha ricevuto correttamente i file visualizzando i file JSON e MDN. Questi file sono denominati in base alle convenzioni descritte in [Nomi e posizioni dei file](#). Se hai configurato un ruolo di registrazione quando hai creato il connettore, puoi anche controllare 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](#).

Per inviare un messaggio AS2 in uscita

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 sincrona o asincrona).
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 dei server esistenti. AS2-enabled Per i dettagli sulle configurazioni supportate, vedere. [Configurazioni 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, `/amzn-s3-demo-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, `/amzn-s3-demo-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, `/amzn-s3-demo-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. Esempio:

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-bucket/AS2-folder/  
file-to-send.txt
```

Se si esegue questo comando, i file MDN e JSON vengono salvati in `/amzn-s3-demo-bucket/AS2-folder/processed` (per trasferimenti riusciti) o `/amzn-s3-demo-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.json`

- 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	Description	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

Codice	Description	Elaborazione completata?
NON RIUSCITO	L'elaborazione dei messaggi non è riuscita. Per un elenco dei codici di errore, vedere Codici di errore AS2 .	Sì

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",
  "message-subject": "File xyzTest from MyCompany_OID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_OID",
  "connector-id": "c-c21c63ceaaf34d99b",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 3198,
  "mdn-message-id": "OPENAS2-11072022063009+0000-df865189-1450-435b-9b8d-d8bc0cee97fd@PartnerA_OID_MyCompany_OID",
  "mdn-subject": "Message be18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa has been accepted",
  "as2-to": "PartnerA_OID",
  "transfer-id": "dedf4601-4e90-4043-b16b-579af35e0d83",
  "file-path": "/amzn-s3-demo-bucket/as2testcell10000/openAs2/TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa",
  "timestamp": "2022-07-11T06:30:10.791274Z"
}
```

Esempio di file in uscita che non è stato trasferito correttamente:

```
{
  "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-5ed8b90775fff@718de4cec1374598",
"failure-message": "http://Test123456789.us-east-1.elb.amazonaws.com:10080 returned
status 500 for message with ID 9a9cc9ab-7893-4cb6-992a-5ed8b90775fff@718de4cec1374598",
"transfer-id": "07bd3e07-a652-4cc6-9412-73ffdb97ab92",
"connector-id": "c-056e15cc851f4b2e9",
"file-path": "/amzn-s3-demo-bucket-4c1tq6ohjt9y/as2IntegCell10002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
"timestamp": "2022-07-11T21:17:24.802378Z"
}

```

Esempio di file in entrata trasferito correttamente:

```

{
  "requester-content-type": "application/EDI-X12",
  "subject": "File openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat sent from MyCompany
to PartnerA",
  "client-ip": "10.0.109.105",
  "requester-file-name": "openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat",
  "as2-from": "MyCompany_0ID",
  "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_0ID_PartnerA_0ID",
  "as2-to": "PartnerA_0ID",
  "agreement-id": "a-f5c5cbea5f7741988",
  "file-path": "processed/openAs2TestInboundAsyncMdn-
necco-5Ab6bTfC0.OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_0ID_PartnerA_0ID.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"
}
```

Personalizza le intestazioni HTTP per i messaggi AS2

Quando si inviano messaggi AS2 a partner commerciali, potrebbe essere necessario personalizzare le intestazioni HTTP per soddisfare requisiti specifici o migliorare la compatibilità con la configurazione del server AS2 del partner. Questo CloudFormation modello crea un'infrastruttura per abilitare intestazioni HTTP personalizzate per i messaggi AS2 inviati. AWS Transfer Family Configura un Amazon API Gateway e una funzione Lambda che fungono da proxy, permettendo la modifica dinamica delle intestazioni richieste dai server AS2 dei partner commerciali.

Usa questo modello per effettuare le seguenti operazioni:

- Aggiungi intestazioni HTTP personalizzate ai messaggi AS2 in uscita
- Sostituisci i valori di intestazione predefiniti con valori personalizzati

Important

Fai attenzione quando sovrascrivi i valori di intestazione predefiniti, poiché ciò può causare errori di invio: alcune intestazioni AS2 sono necessarie.

- Garantisci la compatibilità con i partner commerciali che hanno requisiti di intestazione specifici

Panoramica del modello

Il modello crea i seguenti componenti principali:

- Una funzione Lambda che elabora e inoltra messaggi AS2
- Un Amazon API Gateway per esporre la funzione Lambda
- Ruoli e autorizzazioni IAM per la funzione Lambda
- Risorse condizionali per il supporto HTTPS

Il file modello è disponibile qui: Modello di [intestazioni HTTP dinamiche](#).

Come funziona

1. Amazon API Gateway riceve messaggi AS2 in entrata da AWS Transfer Family
2. La richiesta viene inoltrata alla funzione Lambda.
3. La funzione Lambda elabora la richiesta, aggiungendo o modificando le intestazioni secondo necessità.
4. La richiesta modificata viene quindi inoltrata al server AS2 del partner.
5. La risposta dal server del partner viene restituita tramite Lambda e Amazon API Gateway a AWS Transfer Family

Caratteristiche chiave

- Modifica dinamica dell'intestazione: consente la personalizzazione dell'intestazione dell'oggetto e l'aggiunta di altre intestazioni richieste.
- Protocol Support: funziona con entrambi i protocolli HTTP e HTTPS.
- Configurazione flessibile: consente di specificare l'host, la porta e il percorso del partner.

Dettagli di implementazione

Il modello implementa i seguenti componenti chiave:

Funzione Lambda

Il cuore della soluzione è una funzione Node.js Lambda che:

- Riceve richieste da Amazon API Gateway
- Modifica le intestazioni in base alla configurazione e ai dati delle richieste in entrata

- Inoltra la richiesta modificata al server AS2 del partner
- Gestisce entrambi i protocolli HTTP e HTTPS
- Include la gestione e la registrazione degli errori

Gateway Amazon API

Un'API HTTP è configurata per:

- Ricevere messaggi AS2 in arrivo
- Indirizza le richieste alla funzione Lambda
- Restituisci le risposte a AWS Transfer Family

Parametri del modello

Immettete le informazioni per i parametri del modello come segue. Notate che tutti questi parametri sono stringhe.

- **Environment**: questo parametro viene utilizzato per denominare le risorse create dal modello, indipendentemente dal fatto che siano destinate a un ambiente di sviluppo o di produzione. I valori validi sono dev e prod.
- **PartnerHost**: l'indirizzo IP o il nome host del server partner AS2.
- **PartnerPort**: il numero di porta per il server partner AS2. Se non specificato, il valore predefinito è 80 per HTTP e 443 per HTTPS.
- **PartnerPath**: il percorso dell'endpoint AS2 sul server partner
- **ProtocolType**: il protocollo da utilizzare per la comunicazione AS2: i valori validi sono HTTP e HTTPS.

Risorse condizionali

Per il supporto HTTPS, il modello crea in modo condizionale:

- Un livello Lambda per i certificati CA
- HTTPS-specific configurazione nella funzione Lambda

Distribuzione e utilizzo

Per personalizzare le intestazioni HTTP AS2 utilizzando un modello CloudFormation

1. Apri la 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 Scegli un modello esistente.
5. Copia questo link, [modello di intestazioni HTTP dinamiche](#), e incollalo nel campo URL di Amazon S3.
6. Scegli Next (Successivo).
7. Inserisci i dettagli del parametro con le tue informazioni. Questi sono dettagliati in [Parametri del modello](#).
8. Scegli Next (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 CloudFormation potrebbe creare risorse AWS Identity and Access Management (IAM).

Dopo aver distribuito questo CloudFormation stack:

1. Prendi nota dell'URL dell'endpoint Amazon API Gateway fornito negli output dello stack.
2. Aggiorna il tuo AWS Transfer Family connettore esistente per utilizzare questo nuovo endpoint Amazon API Gateway.
3. La soluzione ora gestirà i messaggi AS2, aggiungendo o modificando le intestazioni in base alla configurazione.

Warning

Modifica l'intestazione Subject o aggiungi solo le intestazioni che il tuo partner si aspetta esplicitamente. La modifica di altre intestazioni può causare errori di trasferimento.

Monitoraggio dell'utilizzo di AS2

Puoi monitorare l'attività di AS2 utilizzando Amazon CloudWatch e AWS CloudTrail. Per visualizzare altre metriche del server Transfer Family, consulta [CloudWatch Registrazione Amazon per server AWS Transfer Family](#)

Metriche AS2

Metrica	Description
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
OutboundMessage	Il numero totale di messaggi AS2 inviati con successo dal server Transfer Family a un partner commerciale. Unità: numero Durata: 5 minuti
OutboundFailedMessage	Il numero totale di messaggi AS2 che sono stati inviati senza successo a un partner commerciale. Cioè, sono stati inviati dal server Transfer Family, ma non sono stati ricevuti con successo dal partner commerciale.

Metrica	Description
	Unità: numero
	Periodo: 5 minuti
DaysUntilExpiry	Il numero di giorni che mancano alla scadenza di un certificato è determinato da quanto <code>InactiveDate</code> indicato sul certificato al momento dell'importazione. Unità: numero Dimensioni: <code>CertificateId</code> , <code>Description</code> (se fornite) Periodo: 1 giorno Per ulteriori informazioni, consulta Rotazione dei certificati AS2.

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	Description	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

Codice	Description	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, vedere Codici 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 <i>send-file-path</i>	Si verifica quando si gestisce una <code>StartFileTransfer</code> richiesta in cui nessuna delle <code>SendFilePaths</code> due non è valida o non è valida. Cioè, nel percorso manca il nome

Codice	Errore	Descrizione e risoluzione
	Impossibile ottenere le credenziali con: ErrorCode <i>error-code</i>	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. Assicuratevi che l'ID segreto sia corretto. 2. Assicuratevi 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 <code>StartFileTransfer</code> richiesta. Inoltre, assicuratevi che il ruolo fornisca l'accesso in lettura e scrittura alla directory principale dei file con cui intendi inviare <code>StartFileTransfer</code>. 3. Se per il segreto viene utilizzata una chiave gestita dal cliente, assicuratevi 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 il messaggio. <i>message-ID</i> 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: <i>encryption-ID</i>	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: <i>local-profile-ID</i>	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	Crittografia del file <i>file-name</i> non riuscita.	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	<i>partner-URL</i> ha restituito lo stato 400 per il messaggio con <i>message-ID</i> 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.
INSUFFICIENT_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 risoluzioni 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. Assicurati 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 disposizioni Error: insufficient-message-security. Abilita la and/or crittografia della firma sul connettore per soddisfare le aspettative del partner commerciale.
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	Non applicabile	Il destinatario non può verificare e l'integrità del contenuto. Il partner commerciale restituisce un MDN a Transfer Family con il modificatore di disposizioni Error: integrity-check-failed.
PATH_NOT_FOUND	Impossibile creare <i>file-path</i> una cartella. 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 StartFile Transfer comando contenga il nome di un bucket esistente.

Codice	Errore	Descrizione e risoluzione
SEND_FILE_NOT_FOUND	Percorso del file <i>file-path</i> 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	<i>server-ID</i> Il server 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 disponibile per la firma oppure non è stato possibile eseguire la firma. Verificate 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: <i>local-profile-ID</i> .	Tentativo di firmare un messaggio in uscita, ma non viene 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 <i>hostname</i> .	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 <i>message-ID</i> 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 non è stato trovato alcun certificato pubblico corrispondente alla firma del messaggio <i>:partner-profile-ID</i>. - Impossibile ottenere certificati per un profilo inesistente: <i>partner-profile-ID</i> - Nessun certificato valido è stato trovato nel profilo: <i>partner-profile-ID</i>	AWS Transfer Family sta 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 sia il certificato di firma corretto per il partner.

Monitoraggio della scadenza dei certificati

AWS Transfer Family monitora automaticamente le date di scadenza dei certificati AS2 e pubblica una CloudWatch metrica Amazon per aiutarti a monitorare quando i certificati si avvicinano alla scadenza. Ciò consente di gestire in modo proattivo i rinnovi dei certificati ed evitare interruzioni del servizio.

DaysUntilExpiry parametro

Quando importi un certificato per l'utilizzo di AS2, Transfer Family crea automaticamente una CloudWatch metrica chiamata `DaysUntilExpiry`. Questa metrica tiene traccia del numero di giorni rimanenti alla scadenza del certificato in base al periodo specificato durante l'InactiveDateimportazione del certificato.

Dettagli metrici:

- Nome della metrica: `DaysUntilExpiry`
- Spazio dei nomi: `AWS/Transfer`
- Dimensioni: `CertificateId` (sempre presenti), `Description` (se fornite durante l'importazione del certificato)
- Unità: conteggio (giorni)
- Frequenza: pubblicata giornalmente

Important

Dopo l'importazione di un certificato, Transfer Family può impiegare fino a un giorno intero prima che Transfer Family emetta questa metrica sul tuo account.

Il valore della metrica diminuisce di una volta al giorno man mano che il certificato si avvicina alla data di inattività. Ad esempio, se mancano 30 giorni alla scadenza di un certificato, la metrica mostrerà 30, 29 il giorno successivo e così via.

Le migliori pratiche per il monitoraggio dei certificati

Segui queste best practice per configurare il monitoraggio della scadenza dei certificati:

- Imposta soglie di avviso multiple: crea allarmi per periodi di tempo diversi (ad esempio, 30 giorni, 14 giorni e 7 giorni prima della scadenza) per fornire un periodo di tempo adeguato per il rinnovo del certificato.
- Utilizza statistiche appropriate: utilizza la Maximum statistica durante la creazione di allarmi per assicurarti di acquisire il valore della metrica più recente.
- Configura le azioni di allarme appropriate: imposta le notifiche per avvisare i membri del team appropriati che possono rinnovare i certificati.
- Testa gli avvisi: verifica regolarmente il tuo sistema di notifica per assicurarti che gli avvisi vengano recapitati correttamente.
- Documenta il processo: conserva la documentazione sul processo di rinnovo dei certificati e su chi è responsabile dei diversi certificati.

Esempi di configurazioni di allarme

Ecco alcuni esempi di configurazioni di allarme per diversi scenari di notifica:

avviso di scadenza di 30 giorni

Crea un allarme che si attiva quando mancano 30 giorni o meno alla scadenza di un certificato:

- Metrica: DaysUntilExpiry
- Statistica: Maximum
- Periodo: 1 giorno
- Soglia: 30
- Confronto: inferiore o uguale alla soglia
- Trattamento dei dati mancanti: considera validi i dati mancanti (senza violarli)

Avviso critico di scadenza entro 7 giorni

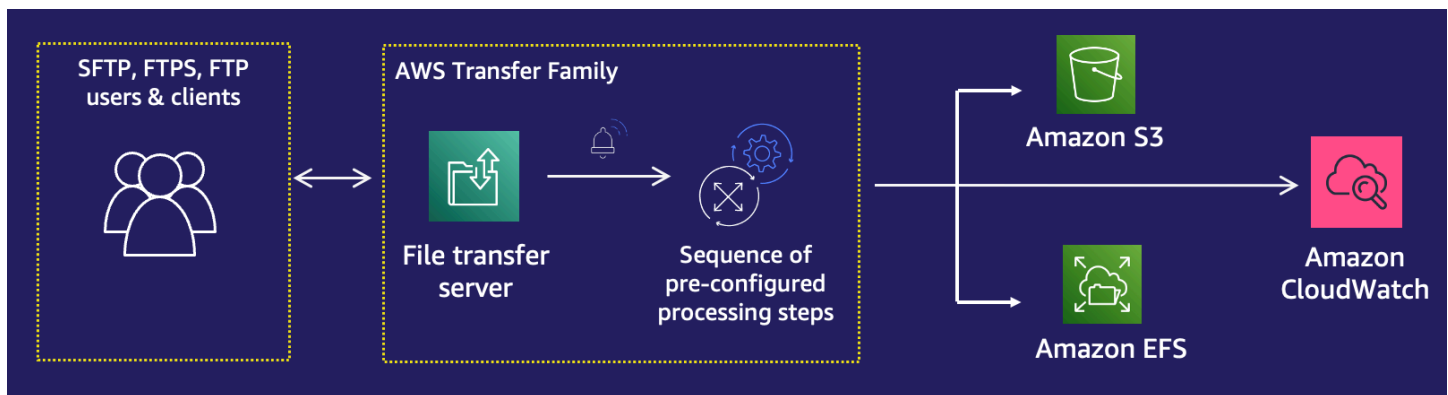
Crea un allarme critico che si attiva quando mancano 7 giorni o meno alla scadenza di un certificato:

- Metrica: DaysUntilExpiry
- Statistica: Maximum
- Periodo: 1 giorno
- Soglia: 7

- Confronto: inferiore o uguale alla soglia
- Trattamento dei dati mancanti: considera validi i dati mancanti (senza violarli)

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, beneficate del controllo e della visibilità end-to-end.



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. Built-in la gestione 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 log 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 CloudWatch delle metriche per i server 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 SFTP/FTPS endpoint 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.
- [Il seguente workshop offre laboratori pratici per creare flussi di lavoro completamente automatizzati e basati sugli eventi che prevedono il trasferimento di file da o verso server SFTP esterni ad Amazon S3 e la comune pre-elaborazione e post-elaborazione di tali file: workshop MFT. Event-driven](#)

Questo video fornisce una panoramica di questo workshop.

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 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 Console di gestione AWS, 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.
- **Exception-handling passaggi** — I gestori di eccezioni sono fasi di elaborazione dei file che vengono AWS Transfer Family eseguite nel caso in cui uno dei passaggi nominali fallisca o causi 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, vedere [the 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 quando il flusso di lavoro fallisce.

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](#). Scegli Save (Salva).

Managed workflows [Info](#)

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

w-

Create a new Workflow

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

w-

Create a new Workflow

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

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 /amzn-s3-demo-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.

The screenshot shows the AWS Transfer Family console interface. On the left is a navigation sidebar with links to Servers, Connectors, AS2 Trading Partners, Certificates, Profiles, Workflows (selected), Feature Spotlight, What's New, Documentation, About servers, and About SFTP connectors. The main content area displays details for a specific workflow 'W-1234567890abcdef0'. It includes a 'Description' section with the name 'Test my workflow' and a description 'Test workflow A'. Below this is a 'Nominal steps (1)' section with a table containing one step: a 'tag_step' of type 'TAG'. An 'Exception handlers (1)' section follows, with a table containing one handler: 'delete_if_exception' of type 'DELETE'. The 'In-flight executions (0)' section shows a search bar and a table with no data. At the bottom, the 'Tags (1)' section includes a 'Manage tags' button and a note about using tags to organize workflows.

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": "amzn-s3-demo-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 CloudFormation console (). <https://console.aws.amazon.com/cloudformation>

Transfer Family > Workflows > w-

W-

Delete

This workflow belongs to the AWS CloudFormation stack **stack-transfer-notifications-blog**. [Manage this stack](#) on the CloudFormation console.

Description

Name

Stack-managed

Workflow description

Workflow for blogpost

Nominal steps (4) Info

Number	Description	Type	Configuration
1	Lambda	CUSTOM	Details
2	CopyFile	COPY	Details
3	TagFileNotified	TAG	Details
4	DeleteOriginalSourceFile	DELETE	Details

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](#)
- [Decrittografa il file](#)
- [Tag: file](#)
- [Eliminare il file](#)
- [Variabili denominate per i flussi di lavoro](#)
- [Esempio di workflow di etichettatura ed eliminazione](#)

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 in *amzn-s3-demo-destination-bucket*.

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 workflow di etichettatura ed eliminazione](#).

Configure copy parameters

Step name

File location

Select the file location to use as an input for this step

☒ Copy the file created from previous step to a new location

Input file is selected from the previous step's output

☐ Copy the original source file to a new location

Originally uploaded file

Destination bucket name

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

☐ Overwrite existing

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 terminate 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 `${transfer:UserName}` o `${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. `amzn-s3-demo-destination-bucket/richard-roe/processed/` Se l'utente `mary-major` carica un file, questo viene copiato nella cartella. `amzn-s3-demo-destination-bucket/mary-major/processed/`

Configure parameters

Configure copy parameters

Step name

dynamic-copy

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UserName}/processed`

☐ Overwrite existing

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 `amzn-s3-demo-destination-bucket/2022-02-01/processed/` cartella.

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

amzn-s3-demo-destination-bucket ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UploadDate}/processed`

☐ Overwrite existing

È inoltre possibile utilizzare entrambe queste variabili insieme, combinandone le funzionalità. Ad esempio, è possibile impostare il prefisso della chiave di destinazione su **folder/**`${transfer:UserName}/${transfer:UploadDate}/`, che creerebbe ad esempio cartelle anndate. `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:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
```



```
"Effect": "Allow",
"Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
],
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

Note

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

Algoritmi di crittografia simmetrica supportati

Per la decrittografia PGP, Transfer Family supporta algoritmi di crittografia simmetrica utilizzati per crittografare i dati effettivi dei file all'interno dei file PGP.

- Per informazioni dettagliate sugli algoritmi di crittografia simmetrica supportati, vedere. [Algoritmi di crittografia simmetrica PGP](#)
- Per informazioni sugli algoritmi di key pair PGP utilizzati con questi algoritmi simmetrici, vedere. [Algoritmi di key pair PGP](#)

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 informazioni sugli algoritmi PGP supportati e sui consigli, consulta [Algoritmi di crittografia e decrittografia PGP](#)

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 Gestione dei segreti AWS con il nome segreto corretto.
2. Memorizza la tua chiave PGP Gestione dei segreti AWS 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 [Gestione dei segreti AWS Pricing](#).

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
```

⚠ Important

Quando crittografate i file per utilizzarli con i AWS Transfer Family flussi di lavoro, assicuratevi sempre di specificare un destinatario non anonimo utilizzando il parametro. -r La crittografia anonima (senza specificare un destinatario) può causare errori di decrittografia nel flusso di lavoro perché il sistema non sarà in grado di identificare quale chiave utilizzare per la decrittografia. Le informazioni di debug relative a questo problema sono disponibili all'indirizzo. [Risolvi i problemi di crittografia dei destinatari anonimi](#)

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. Altrimenti, riceverai un errore quando tenti 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:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}, {
  "Sid": "Decrypt",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue",
  ],
  "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
}
```

Note

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.

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

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:::amzn-s3-demo-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.

Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

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 workflow 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.

The screenshot shows the AWS Transfer Family console interface. On the left, a sidebar lists three steps: 'Step 1 Choose step type', 'Step 2 Configure parameters' (which is the active step), and 'Step 3 Review and create'. The main area is titled 'Configure parameters' and contains a section 'Configure copy parameters'. This section includes three input fields: 'Step name' with the value 'copy-step-first-step', 'Destination bucket name' with a dropdown menu showing 'example-bucket', and 'Destination key prefix' with the value 'test/'. Below these fields is a checkbox labeled 'Overwrite existing' which is currently unchecked. A small text note explains that the prefix can be parametrized using variables like \${transfer:UserName} or \${transfer:UploadDate}.

- 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).

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

- f. 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.

Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

- c. 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. Rivedi 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": "amzn-s3-demo-bucket",
          "Key": "test/"
        }
      }
    }
  },
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "demo"
        }
      ],
      "SourceFileLocation": "${previous.file}"
    }
  },
  {
    "Type": "DELETE",
    "DeleteStepDetails": {
```

```
        "Name": "DeleteStep",
        "SourceFileLocation": "${original.file}"
    }
}
```

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
```

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, vedi [Configurazione 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"}]}'
```

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.

Configure custom parameters

Step name
custom file processing step

File location
Select the file location to use as an input for this step

☒ Apply custom processing to the file created from previous step
Input file is selected from the previous step's output

☐ Apply custom processing to the original source file
Originally uploaded file

Target
am:aws:lambda:us-east-2:1234567... ▼

Timeout (seconds)
60

 Note

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 [SendWorkflowStepState](#) API. `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, consultare [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 Lambda-processed file da utilizzare come input del passaggio successivo. Quindi, se hai più passaggi personalizzati tutti configurati per utilizzare `previous.file` opzione, utilizzano tutti 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 `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": "amzn-s3-demo-bucket",
    "key": "path/to/mykey",
    "eTag": "d8e8fca2dc0f896fd7cb4cb0031ba249",
    "versionId": null
  }
}

```

Custom step that uses an Amazon EFS domain

```

{
  "token": "MTg0N2Y3N2UtNWl5Ny00ZmZlLTk5YTgtZTU3YzViYj11NmZm",
  "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 [SendWorkflowStepState](#) API 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, consulta [the 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:::amzn-s3-demo-bucket"
        ]
    },
    {
        "Sid": "AllObjectActions",
        "Effect": "Allow",
        "Action": "s3:*Object",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    },
    {
        "Sid": "GetObjectVersion",
        "Effect": "Allow",
        "Action": "s3:GetObjectVersion",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    },
    {
        "Sid": "Custom",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": [
            "arn:aws:lambda:us-east-1:123456789012:function:function-name"
        ]
    },
    {
        "Sid": "Tag",
        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",
            "s3:PutObjectVersionTagging"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    }
]

```

}

3. 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, vedere [Per 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, consulta [the section called "Cross-service prevenzione sostitutiva confusa"](#).

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:::amzn-s3-demo-source-bucket/*"
    }
  ],
}
```

```

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

```

```

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

```

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:us-east-1:123456789012: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”](#)

w-1234567890abcdef0

Delete

Description

Name

Delete after upload

Workflow description

test-my-workflow

Nominal steps (1) Info

Number	Description	Type	Configuration
1	is-CSV	CUSTOM	Details

Exception handlers (1) Info

Number	Description	Type	Configuration
1	send-email	CUSTOM	Details

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": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  }
}
```

```

    }
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
},
{
  "type": "StepStarted",
  "details": {
    "input": {
      "fileLocation": {
        "backingStore": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    },
    "stepType": "COPY",
    "stepName": "copyToShared"
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
},
{
  "type": "StepCompleted",
  "details": {
    "output": {},
    "stepType": "COPY",
    "stepName": "copyToShared"
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "server-id",

```

```
        "username": "mary",
        "sessionId": "session-id"
    },
    {
        "type": "ExecutionCompleted",
        "details": {},
        "workflowId": "w-abcdef01234567890",
        "executionId": "execution-id",
        "transferDetails": {
            "serverId": "s-server-id",
            "username": "mary",
            "sessionId": "session-id"
        }
    }
}
```

CloudWatch 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 in [Utilizzo CloudWatch delle metriche per i server Transfer Family](#).

Creare un flusso di lavoro da un modello

È possibile distribuire uno 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 CloudFormation stack che crei un AWS Transfer Family flusso di lavoro e un server

1. Apri la 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"  
  }  
]  
}  
}  
}
```

- 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`.
- Segui le istruzioni per distribuire uno 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.

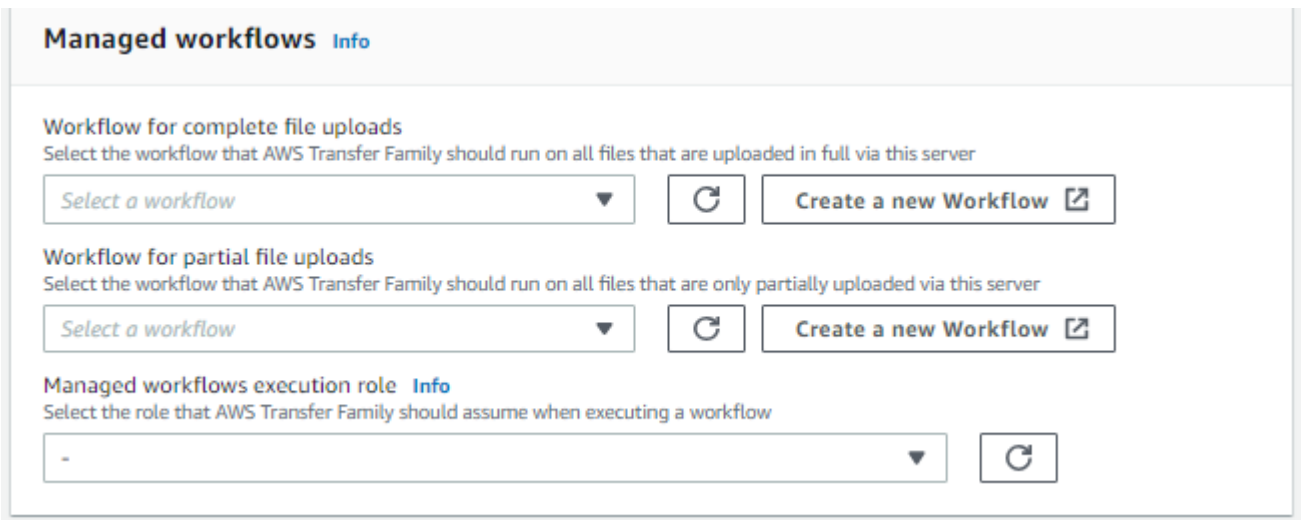
Console

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.



Managed workflows [Info](#)

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

Select a workflow ▼  [Create a new Workflow](#) 

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

Select a workflow ▼  [Create a new Workflow](#) 

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

- ▼ 

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":[]}'
```

Sostituisci *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

- Cross-account e le AWS Lambda funzioni interregionali non sono supportate. È tuttavia 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.
- È possibile collegare un flusso di lavoro di elaborazione file a un server Transfer Family che utilizza il protocollo AS2: tuttavia, i messaggi AS2 non eseguono flussi di lavoro collegati al server.

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 SFTP-enabled server.

Argomenti

- [Visualizza un elenco di server](#)
- [Eliminare un server](#)
- [Visualizza i dettagli dei server SFTP, FTPS e FTP](#)
- [Visualizza i dettagli del server AS2](#)
- [Supporto IPv6 per i server Transfer Family](#)
- [Modifica i dettagli del server](#)
- [Modifica la configurazione del provider di identità](#)
- [Gestisci le chiavi host per il tuo SFTP-enabled server](#)
- [Monitoraggio dell'utilizzo nella console](#)

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 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, consulta [Visualizza 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. Aprire 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, vedere [Modifica 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](#)

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider

[Edit](#)

Identity provider type
Service managed

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.

Additional details

[Edit](#)**Log group**[/aws/transfer/s-](#)**Logging role** [Info](#)

-

Security Policy [Info](#)

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

Domain

Amazon S3

Login display banner[View the display message](#)**Optimized directories** [Info](#)

ENABLED

SetStat option

Ignore

TLS session resumption

-

Passive IP

-

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.

Protocols

Edit

Protocols over which clients can connect to your server's endpoint

- AS2

Identity provider

Edit

**AS2 Auth**

Basic authentication is not supported for AS2. Access can be controlled through VPC security groups.

A ciascun server AS2 vengono assegnati tre indirizzi IP statici. Utilizza questi indirizzi IP per inviare mDNS asincroni ai tuoi partner commerciali tramite AS2.

AS2 asynchronous MDN egress IP details

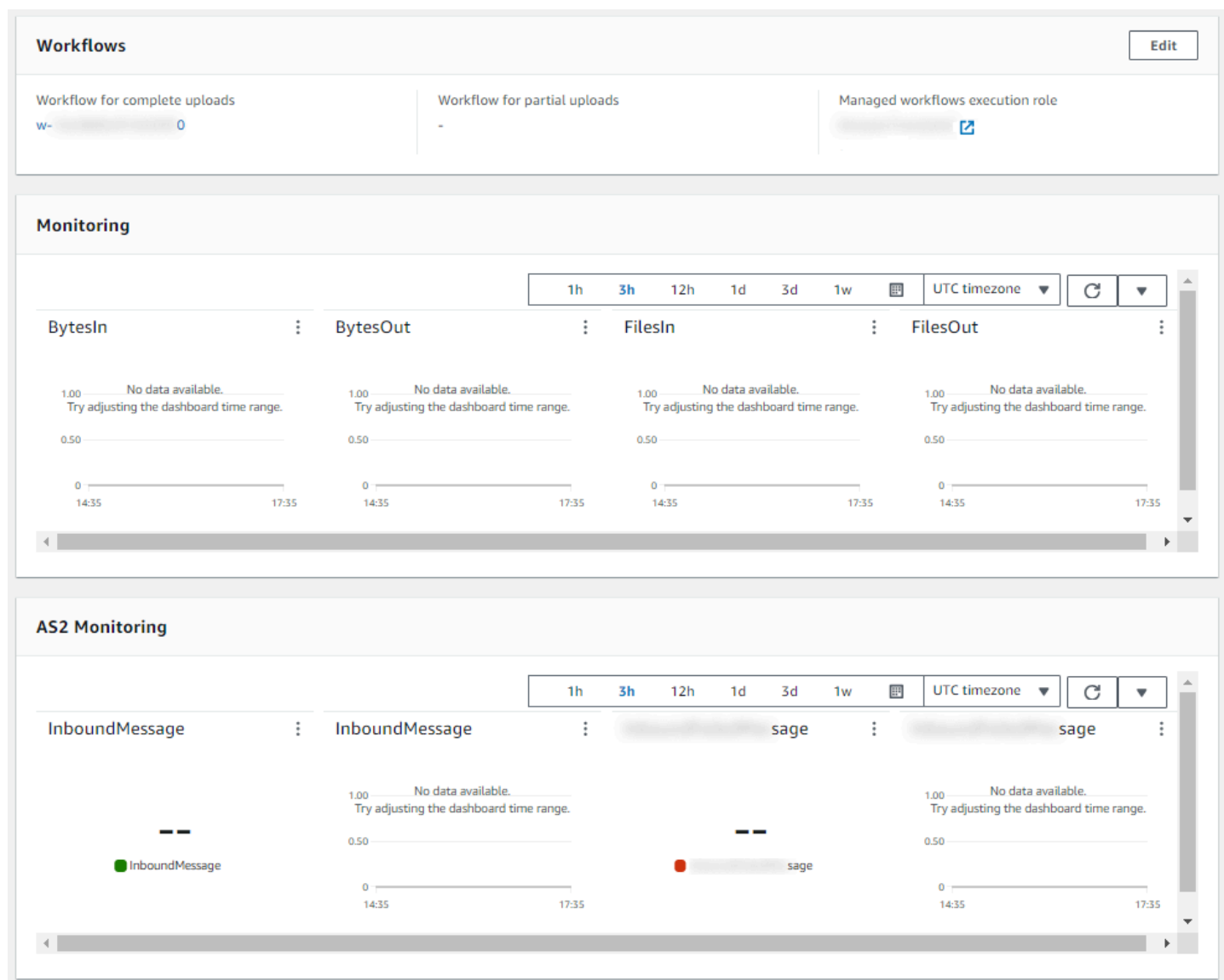
Below are the service managed static IP addresses used for sending your asynchronous MDNs to trading partners over AS2

La parte inferiore della pagina dei dettagli del server AS2 contiene i dettagli per qualsiasi flusso di lavoro associato e le informazioni di monitoraggio e etichettatura.



Supporto IPv6 per i server Transfer Family

AWS Transfer Family supporta endpoint dual-stack (IPv4 e IPv6) per le seguenti risorse:

- endpoint pubblici SFTP
- Endpoint interni VPC per tutti i protocolli (SFTP/FTPS/FTP e AS2)
- Endpoint pubblici per i server AS2-enabled Transfer Family, utilizzando la procedura fornita in [Utilizzo di un Application Load Balancer per la connettività del server AS2 dual-stack](#)
- Endpoint API

Con il supporto dual-stack, gli endpoint Transfer Family possono comunicare con client abilitati sia per IPv4 che per IPv6. Ciò consente di passare gradualmente dai sistemi basati su IPv4 a quelli basati su IPv6 senza dover passare da un sistema all'altro in una sola volta, soddisfare i requisiti di conformità IPv6 ed eliminare la necessità di costose apparecchiature di rete per gestire la conversione degli indirizzi tra IPv4 e IPv6. [Per i dettagli, consulta DNS ed endpoints nell'API Reference.AWS Transfer Family](#) Per un elenco completo degli endpoint disponibili, consulta [AWS Transfer Family endpoint e](#) quote nel. Riferimenti generali di AWS

Limitazioni IPv6

Le seguenti risorse Transfer Family attualmente non supportano IPv6:

- VPC-Internet endpoint
- tipo di endpoint VPC_ENDPOINT (obsoleto)

Il protocollo FTPS supporta i comandi PASV ed EPSV per la richiesta di una porta dati aperta per le operazioni di elenco, acquisizione e inserimento dei file. Tuttavia, PASV non funziona con IPv6 perché richiede una risposta. IPv4-specific EPSV continua a funzionare perché restituisce solo le informazioni sulla porta.

Per utilizzare FTPS, consigliamo una delle seguenti soluzioni:

- Configura il tuo client FTPS per utilizzare EPSV
- Usa IPv4 anziché IPv6

SFTP supporta sia IPv4 che IPv6. Si consiglia di utilizzare SFTP anziché FTPS quando si lavora con endpoint dual-stack.

Configurazione di IPv6 per i server

Quando si crea un nuovo server o si aggiorna un server esistente, è possibile scegliere il tipo di indirizzo IP:

- IPv4 (impostazione predefinita): per motivi di compatibilità con le versioni precedenti, il server accetterà solo connessioni IPv4.
- Dual-stack: Il server accetterà sia connessioni IPv4 che IPv6.

Per aggiornare il tipo di indirizzo IP di un server esistente:

1. Arresta il server.
2. Modifica i dettagli dell'endpoint.
3. Cambia il tipo di indirizzo IP in. Dual-stack
4. Avviare il server .

Note

Per gli VPC-Internet endpoint, la modalità dual-stack non è attualmente supportata.

Utilizzo di un Application Load Balancer per la connettività del server AS2 dual-stack

È possibile abilitare la connettività dual-stack (IPv4 e IPv6) al server AS2 utilizzando un Application Load Balancer con un endpoint rivolto al pubblico. Ciò consente ai partner commerciali di connettersi al server AS2 utilizzando IPv4 o IPv6.

Per configurare un Application Load Balancer dual-stack per il server AS2

1. Crea un VPC con le seguenti impostazioni:
 - Solo VPC
 - Ingresso CIDR IPv4 manuale
 - Amazon-provided Blocco CIDR IPv6
2. Crea almeno due sottoreti in diverse zone di disponibilità:
 - Aggiungere i CIDR IPv6 alle sottoreti
 - Quando crei sottoreti, alloca solo un sottoinsieme degli indirizzi del VPC per lasciare gli indirizzi disponibili per sottoreti aggiuntive IPv4/IPv6
3. Crea un gateway Internet per il VPC.
4. Modifica la tabella dei percorsi e aggiungi due percorsi:
 - Un percorso con destinazione `0.0.0.0/0`
 - Un percorso con destinazione `::/0`
 - Imposta entrambe le destinazioni del percorso verso il gateway Internet che hai creato

5. Crea un AS2-enabled server nel VPC creato nel passaggio 1. Assicurati di specificare l'IPAddressTypeasDUALSTACK.

Per i dettagli su come creare un server Transfer Family che utilizza il protocollo AS2, vedere [Creare un server AS2](#).

6. Crea un gruppo target:
 - Per Specificare i dettagli del gruppo, configura:
 - Tipo di destinazione: indirizzi IP
 - Nome: inserisci un nome
 - Protocol (Protocollo): HTTP
 - Porta: 5080
 - VPC: seleziona il VPC che hai creato
 - Versione del protocollo: HTTP1
 - Health checks: utilizza i valori predefiniti
 - Per gli obiettivi di Register:
 - Inserisci l'indirizzo IPv4 privato del tuo server AS2
 - Scegli Includi come in sospenso di seguito
7. Crea un Application Load Balancer:
 - Inserisci un nome
 - Per Scheme, scegli Internet-facing
 - Per il tipo di indirizzo IP, scegli Dualstack
 - Per la mappatura della rete:
 - Seleziona il VPC che hai creato
 - Seleziona le zone di disponibilità in cui hai creato le sottoreti
 - Per i gruppi di sicurezza, selezionare un gruppo di sicurezza che consenta il traffico IPv4 e IPv6 in entrata da qualsiasi indirizzo IP sulla porta 80
 - Per gli ascoltatori e il routing:
 - Protocol (Protocollo): HTTP
 - Port (Porta): 80
 - ~~Azione predefinita: inoltro al gruppo target creato~~
 - Scegli Crea sistema di bilanciamento del carico

Dopo aver creato l'Application Load Balancer, i partner commerciali possono utilizzarne il nome DNS per inviare traffico al server AS2. Questa configurazione consente al server AS2 di accettare connessioni da client IPv4 e IPv6 tramite l'Application Load Balancer dual-stack.

Modifica i dettagli del server

Dopo aver creato un AWS Transfer Family server, è possibile modificare la configurazione del server.

Argomenti

- [Modifica i protocolli di trasferimento dei file](#)
- [Modifica l'endpoint del server](#)
- [Modifica la configurazione di registrazione](#)
- [Modifica la politica di sicurezza](#)
- [Modifica il flusso di lavoro gestito per il tuo server](#)
- [Cambia i banner di visualizzazione per il tuo server](#)
- [Metti il tuo server online o offline](#)

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, vedere [Modifica i protocolli di trasferimento dei file](#).
- Per il provider di identità, ora puoi passare da un tipo all'altro (provider di identità gestito dal servizio, AWS Directory Service o provider di identità personalizzato). Per i dettagli sulla modifica dei tipi di provider di identità e le informazioni richieste per ogni transizione, consulta [Modifica la configurazione 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, vedi [Gestisci le chiavi host per il tuo SFTP-enabled server](#).
- In Dettagli aggiuntivi, puoi modificare le seguenti informazioni:
 - Per modificare il ruolo di registrazione, vedere [Modifica la configurazione di registrazione](#).
 - Per modificare la politica di sicurezza, vedere [Modifica la politica di sicurezza](#).
 - Per modificare la chiave dell'host del server, vedere [Gestisci le chiavi host per il tuo SFTP-enabled server](#).
 - Per modificare il flusso di lavoro gestito per il server, consulta [Modifica il flusso di lavoro gestito per il tuo server](#).
 - Per modificare i banner di visualizzazione per il tuo server, consulta [Cambia 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'[ProtocolDetails](#) argomento.

 Note

Evita di posizionare Network Load Balancer (NLB) o gateway NAT davanti ai server. AWS Transfer Family Questa configurazione aumenta i costi e può causare problemi di prestazioni. Per ulteriori dettagli, consulta [Evita di posizionare AWS Transfer Family NLB e NAT davanti ai server](#).

- Per avviare o arrestare il server, consulta [Metti il tuo server online o offline](#).
- Per eliminare un server, consulta [Eliminare un server](#).
- Per modificare le proprietà di un utente, vedere [Gestione dei controlli di accesso](#).

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider

[Edit](#)

Identity provider type
Service managed

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.

Additional details

[Edit](#)

Log group

[/aws/transfer/s-](#) 

Logging role

-

Security Policy

[Info](#)
TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

Domain

Amazon S3

Login display banner

[View the display message](#)

Optimized directories

[Info](#)
ENABLED

SetStat option

Ignore

TLS session resumption

-

Passive IP

-

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 SFTP-enabled server](#)

- File Transfer Protocol Secure (FTPS): trasferimento di file con crittografia TLS

Per ulteriori informazioni su FTP, vedere. [Creare un FTPS-enabled server](#)

- File Transfer Protocol (FTP): trasferimento di file non crittografato

Per ulteriori informazioni su FTPS, vedere. [Crea un FTP-enabled server](#)

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.

Edit protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

[Cancel](#)[Save](#)

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. Scegli Save (Salva). Si torna alla pagina dei dettagli del server.

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](#)

Transfer Family > Servers > s-[redacted] > Edit endpoint configuration

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID

Select a VPC ID [Create a VPC](#)

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Save](#)

4. Per gli endpoint VPC, puoi modificare le informazioni nel riquadro Zone di disponibilità.
5. Scegli Save (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 lo è FIPS-enabled, 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 i server AWS Transfer Family](#).

3. Scegli Save (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 i server AWS Transfer Family](#).

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](#). Scegli Save (Salva).

Managed workflows [Info](#)

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

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

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

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

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

[role name] [dropdown] [refresh]

3. Scegli Save (Salva). Si torna alla pagina dei dettagli del server.

Cambia i banner di visualizzazione per il tuo server

Sulla AWS Transfer Family console, è possibile 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. Scegli Save (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 Supporto AWS per aiutarti a risolvere i tuoi problemi.

Modifica la configurazione del provider di identità

È possibile modificare il tipo di provider di identità del server da qualsiasi tipo a qualsiasi altro tipo. I tipi di provider di identità disponibili sono:

- Servizio gestito: archivia le credenziali dell'utente all'interno del servizio
- AWS Directory Service: utilizza AWS Managed Microsoft AD o AWS Directory Service per i servizi di dominio Entra ID
- Personalizzato: utilizza la funzione Lambda o Amazon API Gateway per l'integrazione con il tuo provider di identità esistente

Quando cambi il tipo di provider di identità, devi fornire informazioni specifiche a seconda della transizione che stai effettuando. Le sezioni seguenti descrivono le informazioni richieste per ogni tipo di modifica.

Important

Considerazioni sulla modifica dei provider di identità:

- Migrazione degli utenti: quando si modificano i tipi di provider di identità, le configurazioni utente esistenti non vengono migrate automaticamente. Dovrai configurare gli utenti nel nuovo sistema di provider di identità.
- Test: verifica a fondo la configurazione del nuovo provider di identità prima di apportare la modifica agli ambienti di produzione.
- Autorizzazioni: assicurati che il nuovo provider di identità disponga delle autorizzazioni e dei ruoli IAM necessari configurati prima di apportare la modifica.

Passaggio a un provider di identità gestito dal servizio

Quando passi da qualsiasi altro tipo di provider di identità a uno gestito dal servizio, devi:

- Seleziona Servizio gestito come tipo di provider di identità
- Crea nuovi utenti direttamente AWS Transfer Family dopo il completamento della modifica, poiché le configurazioni utente esistenti di altri provider di identità non verranno trasferite

Esempio: se stai passando da un provider di identità personalizzato a uno gestito dal servizio, dovrai ricreare tutti gli account utente e le autorizzazioni associate all'interno del servizio. AWS Transfer Family

Passaggio al AWS Directory Service

Quando si passa da qualsiasi altro tipo di provider di identità a AWS Directory Service, è necessario fornire:

- Directory: selezionare una directory AWS Managed Microsoft AD o AWS Directory Service per Entra ID Domain Services esistente
- Accesso: scegli se limitare l'accesso a un gruppo specifico o consentire l'accesso a tutti gli utenti della directory
- Ruolo di accesso: un ruolo IAM che AWS Transfer Family consente di accedere alla directory

Esempio: se stai passando da un servizio gestito a un AWS Directory Service, devi selezionare la d-1234567890 directory esistente, scegliere di limitare l'accesso al TransferUsers gruppo e specificare il ruolo TransferDirectoryAccessRole IAM.

Passaggio a un provider di identità personalizzato

Quando passi da qualsiasi altro tipo di provider di identità a un provider di identità personalizzato, devi scegliere tra la funzione Lambda o Amazon API Gateway e fornire la configurazione richiesta:

Utilizzo della funzione Lambda

Per l'integrazione della funzione Lambda, fornisci:

- Funzione: seleziona una funzione Lambda esistente che gestisce l'autenticazione
- Metodo di autenticazione (per il protocollo SFTP): scegli la password, la chiave pubblica o entrambe

Esempio: se stai passando da AWS Directory Service a un provider di identità Lambda personalizzato, devi selezionare la tua `TransferCustomAuth` funzione e scegliere Password come metodo di autenticazione.

Transfer Family > Servers > s- > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

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

☐ Service managed
Create and manage users within the service

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

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

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

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

AWS Lambda function

▼



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

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

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

Cancel

Save

Utilizzo di Amazon API Gateway

Per l'integrazione con Amazon API Gateway, fornisci:

- URL API Gateway: l'URL di richiamo dell'endpoint API Gateway
- Ruolo di invocazione: un ruolo IAM che consente di AWS Transfer Family richiamare il tuo API Gateway
- Metodo di autenticazione (per il protocollo SFTP): scegli la password, la chiave pubblica o entrambe

Esempio: se stai passando dalla gestione del servizio all'API Gateway, devi fornire l'URL `https://abcdef123.execute-api.us-east-1.amazonaws.com/prod`, specificare il ruolo `TransferApiGatewayInvocationRole` IAM e scegliere la chiave pubblica come metodo di autenticazione.

Transfer Family > Servers > s-[redacted] > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

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

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

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

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

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

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

Provide an Amazon API Gateway URL

Invocation role
IAM role for the service to invoke your Amazon API Gateway URL

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

☒ **Password OR public key**
☐ Password ONLY
☐ Public Key ONLY
☐ Password AND public key

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

Cancel Save

Passaggio da Amazon API Gateway alla funzione Lambda

Una transizione comune è il passaggio da Amazon API Gateway alla funzione Lambda per l'integrazione personalizzata dei provider di identità. Questa modifica consente di semplificare l'architettura mantenendo la stessa logica di autenticazione.

Considerazioni chiave per questa transizione:

- Stessa funzione, autorizzazioni diverse: puoi utilizzare la stessa funzione Lambda sia per l'API Gateway che per l'integrazione diretta Lambda, ma la politica delle risorse deve essere aggiornata.
- Requisiti della politica delle risorse: quando si passa all'integrazione diretta con Lambda, la politica delle risorse della funzione deve concedere l'`transfer.amazonaws.com` autorizzazione a richiamare la funzione, oltre a `apigateway.amazonaws.com`

Per apportare questa modifica

1. Aggiorna la politica delle risorse della tua funzione Lambda per consentire di `transfer.amazonaws.com` richiamare la funzione.
2. Nella AWS Transfer Family console, cambia il provider di identità da API Gateway alla funzione Lambda.
3. Seleziona la tua funzione Lambda esistente.
4. Verifica la configurazione per assicurarti che l'autenticazione funzioni correttamente.

Esempio di politica delle risorse per l'integrazione diretta con Lambda:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "transfer.amazonaws.com",
        "apigateway.amazonaws.com"
      ]
    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:function-name"
  }]
}
```

Conservazione degli utenti durante le transizioni tra provider di identità

Quando si passa da un tipo di provider di identità all'altro, le configurazioni utente esistenti vengono mantenute in scenari specifici per consentire un ripristino efficiente in caso di problemi:

- Service-managed a provider di identità personalizzato e viceversa: se passi da un provider di identità gestito dal servizio a un provider di identità personalizzato e poi di nuovo a un provider di identità gestito dal servizio, tutti gli utenti vengono mantenuti nell'ultima configurazione nota.
- AWS Directory Service a provider di identità personalizzato e viceversa: se si passa da un provider di identità personalizzato AWS Directory Service a un provider di identità personalizzato e viceversa AWS Directory Service, tutte le definizioni per i gruppi di accesso delegato vengono mantenute nell'ultima configurazione nota.

Questo comportamento di conservazione consente di testare in sicurezza le configurazioni personalizzate dei provider di identità e ripristinare la configurazione precedente senza perdere le configurazioni di accesso degli utenti.

Considerazioni importanti sulla modifica dei provider di identità

- Migrazione degli utenti: quando si modificano i tipi di provider di identità, le configurazioni utente esistenti non vengono migrate automaticamente. Dovrai configurare gli utenti nel nuovo sistema di provider di identità.
- Test: verifica a fondo la configurazione del nuovo provider di identità prima di apportare la modifica agli ambienti di produzione.
- Autorizzazioni: assicurati che il nuovo provider di identità disponga delle autorizzazioni e dei ruoli IAM necessari configurati prima di apportare la modifica.

Gestisci le chiavi host per il tuo SFTP-enabled server

Le chiavi host del server sono chiavi private utilizzate dal server Transfer Family per fornire un'identità univoca al chiamante e per garantire che si tratti del server corretto. Tale garanzia è garantita dalla presenza della chiave pubblica corretta nel file del chiamante. `known_hosts` (Il `known_hosts` file è una funzionalità standard utilizzata dalla maggior parte dei client SSH per archiviare le chiavi pubbliche dei server a cui ti sei connesso.) È possibile recuperare la chiave pubblica corrispondente alla chiave dell'host del server eseguendo l'esecuzione `ssh-keyscan` per il server.

 Important

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 genera chiavi host per il server SFTP-enabled . È possibile importare le chiavi dell'host del server per preservare l'identità dell'host ed evitare di aggiornare gli archivi di fiducia dei client. [Quando importare le chiavi dell'host](#) elenca alcuni motivi per cui potresti volerlo fare. Se non fornite le chiavi host, ne verranno generate di nuove.

AWS Transfer Family supporta più chiavi host di diversi tipi (RSA, ECDSA ed ED25519) per fornire compatibilità con una gamma più ampia di algoritmi di firma dell'host client. Diversi tipi di chiavi consentono algoritmi specifici: le chiavi RSA abilitano gli algoritmi rsa-*, le chiavi ECDSA abilitano gli algoritmi ecdsa-* e le chiavi ED25519 abilitano gli algoritmi ed25519. Pianifica i tipi di chiave al momento della creazione del server, poiché l'introduzione di tipi di chiave aggiuntivi dopo che i client hanno iniziato a interagire con il server può causare interruzioni per alcuni client e può essere tanto problematica quanto la sostituzione delle chiavi host esistenti.

Per evitare che agli utenti venga richiesto di verificare nuovamente l'autenticità del server, importa sul SFTP-enabled server la chiave host per il server locale. SFTP-enabled Ciò impedisce inoltre agli utenti di ricevere un avvertenza su un potenziale attacco di tipo man-in-the-middle.

Puoi anche ruotare periodicamente le chiavi host, come misura di sicurezza aggiuntiva. Per informazioni dettagliate, vedi [Ruota le chiavi dell'host del server](#).

 Note

Le chiavi host del server vengono utilizzate dai server che supportano il protocollo SFTP.

Quando importare le chiavi dell'host

Sebbene sia AWS Transfer Family possibile generare chiavi host automaticamente, esistono diversi scenari in cui l'importazione di chiavi host personalizzate offre vantaggi operativi:

- **Migrazione del server:** state migrando da un server esistente a AWS Transfer Family e volete evitare di aggiornare gli archivi di fiducia dei client (`known_hosts`) per i client esistenti.
- **Disaster recovery e failover:** disponi di più AWS Transfer Family server (ad esempio, uno negli Stati Uniti orientali (Ohio) e uno negli Stati Uniti occidentali (Oregon)) che condividono lo stesso nome DNS pubblico. L'utilizzo delle stesse chiavi host su entrambi i server garantisce un failover senza problemi di autenticazione dei client.
- **Continuità operativa:** si desidera che il materiale chiave dell'host sia disponibile per l'uso con altri server (AWS Transfer Family o altro) in futuro per mantenere l'identità del server coerente in tutta l'infrastruttura.
- **Controllo degli algoritmi:** desiderate una maggiore compatibilità dei client fornendo più algoritmi a chiave host oppure desiderate controllare quali algoritmi possono utilizzare i client offrendo solo chiavi compatibili con algoritmi specifici.

I seguenti argomenti forniscono procedure dettagliate per la gestione delle chiavi host del server:

- [Aggiungere una chiave host del server aggiuntiva](#)- Aggiungi chiavi host aggiuntive al tuo server
- [Eliminare una chiave host del server](#)- Rimuovi le chiavi host dal tuo server
- [Ruota le chiavi dell'host del server](#)- Ruota le chiavi host per una maggiore sicurezza
- [Informazioni aggiuntive sulla chiave dell'host del server](#)- Visualizza e gestisci i dettagli delle chiavi dell'host

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 conatterà utilizzando la chiave più vecchia nella configurazione che corrisponde all'algoritmo della chiave. La chiave più vecchia per ogni tipo di chiave (RSA, ECDSA o ED25519) è la chiave attiva per il server per quel tipo.

Nota di sicurezza quando un server Transfer Family ha più tipi di chiavi host

Se un server ha più tipi di chiavi host, il client SFTP può assegnare una preferenza per tipo. Pertanto, quando esistono chiavi host RSA, ECDSA ed ED25519 per il server, la scelta è guidata dalla preferenza per tipo.

I client SFTP moderni preferiscono le chiavi host ECDSA ed ED25519 quando esistono. Ciò diventa importante se si desidera aggiungere una chiave ECDSA o ED25519 quando in precedenza il server disponeva solo di chiavi RSA. L'aggiunta della nuova chiave ECDSA o ED25519 potrebbe manifestarsi come avviso di sicurezza per un client.

Al client, la chiave apparirà come modificata, mentre in realtà non è stata modificata: la nuova chiave è stata aggiunta alla chiave RSA esistente. Tienilo a mente se decidi di aggiungere nuovi tipi di chiavi host del server.

Per aggiungere una chiave aggiuntiva per l'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.



	Name	Host key ID	Fingerprint	Description	Key type	Date imported
☐	Default host key	hostkey-	SHA256:/	Default	ssh-rsa	2023-06-30
☐	ecdsa-521	hostkey-	SHA256:	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13

4. 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. SFTP-enabled

Note

Quando crei una chiave host del server, assicurati di specificare -N "" (nessuna passphrase). Vedi [Creazione di chiavi SSH su macOS, Linux o Unix](#) i dettagli su come generare coppie di chiavi.

- (Facoltativo) Aggiungi una descrizione per distinguere tra più chiavi host del server. Puoi anche aggiungere tag per la tua chiave.
- 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 [ImportHostKey](#) API e fornisci la nuova chiave host. Se crei un nuovo SFTP-enabled server, fornisci la tua chiave host come parametro nell'operazione [CreateServer](#) API. Puoi anche 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 SFTP-enabled server specificato.

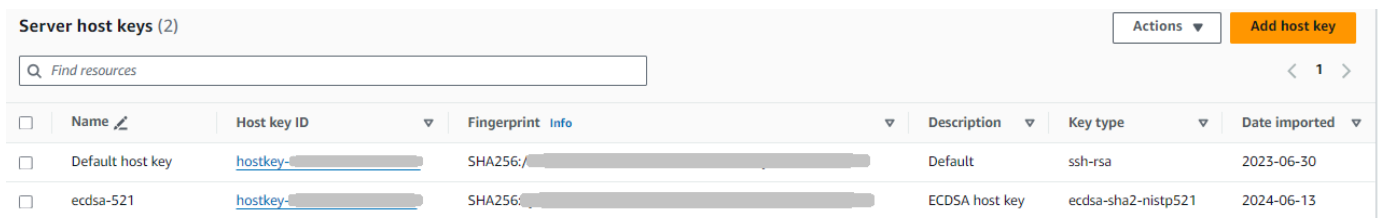
```
aws transfer import-host-key --description key-description --server-id your-server-id
--host-key-body file://my-host-key
```

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

- Apri la AWS Transfer Family console all'indirizzo <https://console.aws.amazon.com/transfer/>.
- Nel riquadro di navigazione a sinistra, scegli Server, quindi scegli un server che utilizza il protocollo SFTP.
- Nella pagina dei dettagli del server, scorri verso il basso fino alla sezione Chiavi host del server.



Server host keys (2)							Actions ▾	Add host key
	Name ↗	Host key ID ▾	Fingerprint Info	Description ▾	Key type ▾	Date imported ▾		
☒	Default host key	hostkey- 	SHA256: 	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey- 	SHA256: 	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

- Nella sezione Chiavi host del server, seleziona una chiave, quindi in Azioni scegli Elimina.
- 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 [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 SFTP-enabled server 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. Questo argomento descrive come il server sceglie la chiave da applicare e la procedura per ruotare queste chiavi.

In che modo il client sceglie una chiave 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

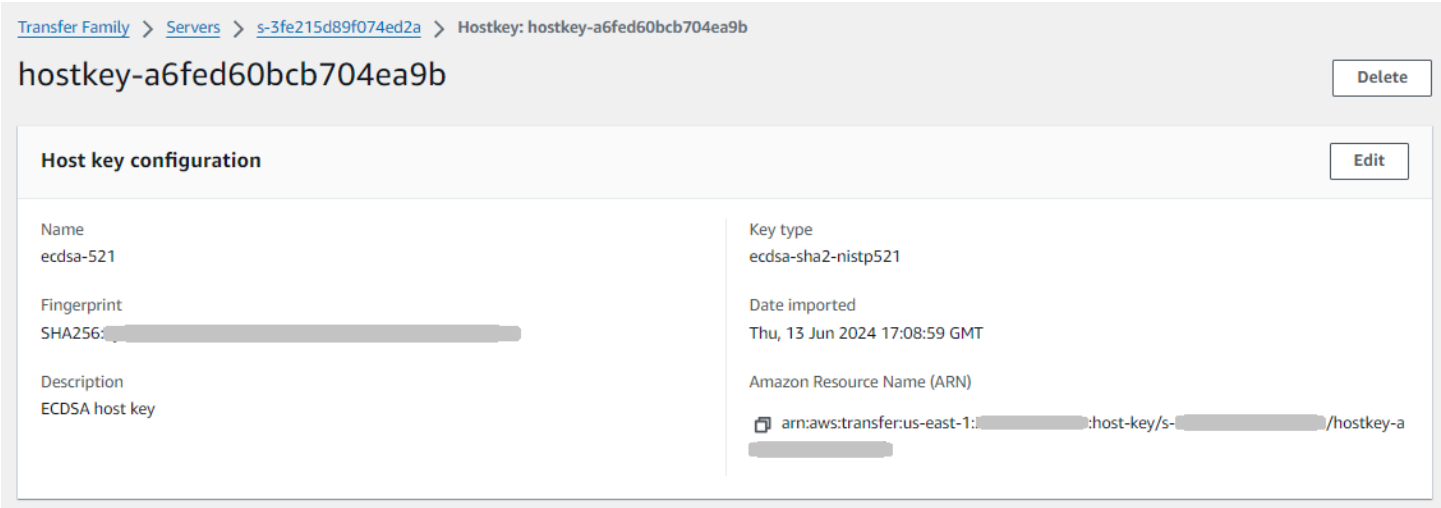
Tipo di chiave host	Data aggiunta al server
RSA	1 Aprile 2020
ECDSA	1 febbraio 2020
ED25519	1 dicembre 2019
RSA	1° ottobre 2019
ECDSA	1 giugno 2019
ED25519	1 marzo 2019

Per ruotare la chiave dell'host del server

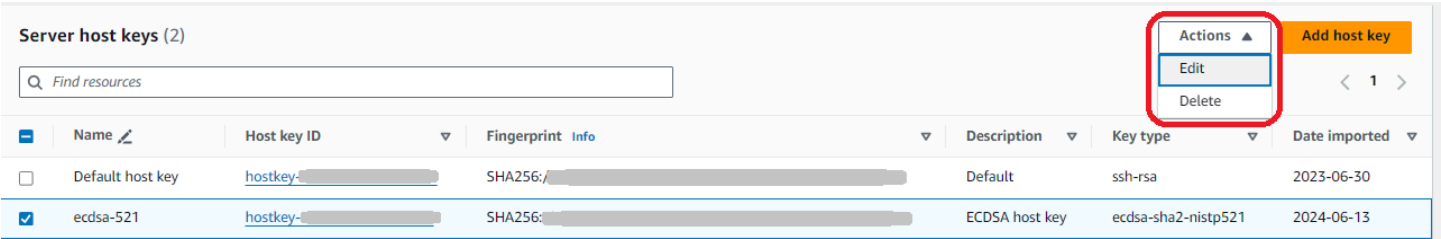
1. Aggiungere una nuova chiave dell'host del server. Questa procedura è descritta in [Aggiungere una chiave host del server aggiuntiva](#).
2. Eliminare una o più chiavi host dello stesso tipo aggiunte in precedenza. Questa procedura è descritta in [Eliminare una chiave host del server](#).
3. Tutti i tasti sono visibili e possono essere attivi, in base al comportamento descritto in precedenza in [In che modo il client sceglie una chiave 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.

Namespace	Metrica	Description
AWS/Transfer	BytesIn	Il numero totale di byte trasferiti nel server. Criteri di segnalazione: • Per SFTP/FTP/FTPS: emesso ogni 5 minuti mentre viene stabilita una connessione al server Transfer

Namespace	Metrica	Description
		Family. Se non viene trasferito alcun file o byte nel periodo, viene emesso «0». Per AS2: quando il cliente riceve un messaggio nel proprio server AS2 e viene emesso non appena il messaggio in entrata ha terminato l'elaborazione Unità: numero Periodo: 5 minuti
	BytesOut	Il numero totale di byte trasferiti dal server. Criteri di segnalazione: - Per SFTP/FTP/FTPS: emesso ogni 5 minuti mentre viene stabilita una connessione al server Transfer Family. Se non viene trasferito alcun file o byte nel periodo, viene emesso «0». - Per AS2: quando il cliente chiama <code>StartFile Transfer</code> dal connettore AS2 e viene emesso non appena il messaggio in uscita ha terminato l'elaborazione. Unità: numero Periodo: 5 minuti

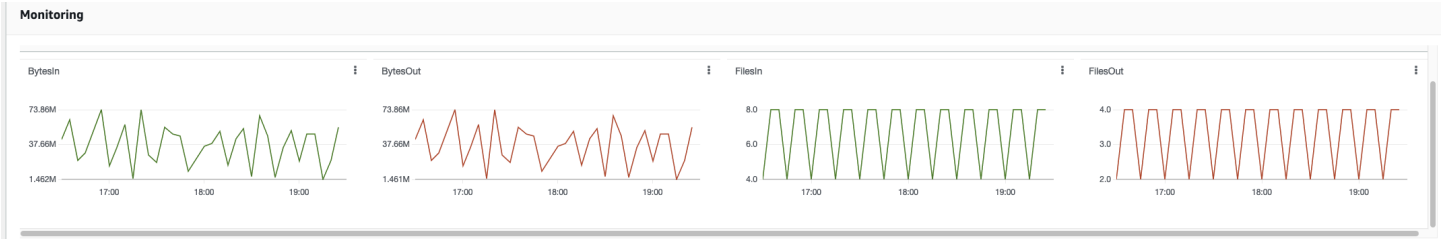
Namespace	Metrica	Description
	FilesIn	Il numero totale di file trasferiti nel server. Per i server che utilizzano il protocollo AS2, questa metrica rappresenta il numero di messaggi ricevuti. Criteri di segnalazione: • Per SFTP/FTP/FTPS: emesso ogni 5 minuti mentre viene stabilita una connessione al server Transfer Family. Se non viene trasferito alcun file o byte nel periodo, viene emesso «0». • Per AS2: quando il cliente riceve un messaggio nel proprio server AS2 e viene emesso non appena il messaggio in entrata ha terminato l'elaborazione. Unità: numero Periodo: 5 minuti
	FilesOut	Il numero totale di file trasferiti dal server. Criteri di segnalazione: • Per SFTP/FTP/FTPS: emesso ogni 5 minuti mentre viene stabilita una connessione al server Transfer Family. Se non viene trasferito alcun file o byte nel periodo, viene emesso «0». • Per AS2: quando il cliente chiama <code>StartFile Transfer</code> dal connettore AS2 e viene emesso non appena il messaggio in uscita ha terminato l'elaborazione. Unità: numero Periodo: 5 minuti

Namespace	Metrica	Description
	InboundMessage	Il numero totale di messaggi AS2 ricevuti con successo da un partner commerciale. Criteri di segnalazione: quando il cliente riceve un messaggio nel proprio server AS2 e lo invia non appena il messaggio in entrata ha terminato con successo l'elaborazione 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. Criteri di segnalazione: quando il cliente riceve un messaggio nel proprio server AS2 e lo invia non appena il messaggio in entrata ha terminato l'elaborazione senza successo Unità: numero Periodo: 5 minuti
	OnUploadExecutionsStarted	Il numero totale di esecuzioni del flusso di lavoro avviate sul server. Criteri di segnalazione: attivati ogni volta che inizia un'esecuzione Unità: numero Periodo: 1 minuto

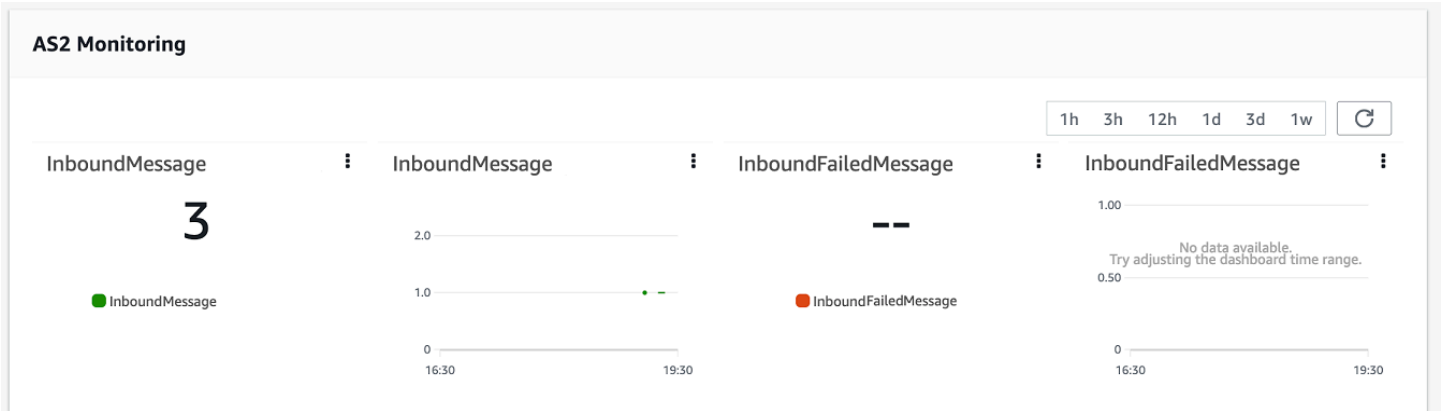
Namespace	Mettrica	Description
	OnUploadExecutionsSuccess	Il numero totale di esecuzioni di workflow riuscite sul server. Criteri di segnalazione: attivato ogni volta che un'esecuzione viene completata con successo Unità: numero Periodo: 1 minuto
	OnUploadExecutionsFailed	Il numero totale di esecuzioni di workflow non riuscite sul server. Criteri di segnalazione: attivato ogni volta che un'esecuzione non viene completata correttamente Unità: numero Periodo: 1 minuto
	OutboundMessage	Il numero totale di messaggi AS2 inviati con successo a un partner commerciale. Criteri di segnalazione: quando il cliente chiama <code>StartFileTransfer</code> dal proprio connettore AS2 e viene emessa non appena il messaggio in uscita ha terminato correttamente l'elaborazione Unità: numero Periodo: 5 minuti

Namespace	Metrica	Description
	OutboundFailedMessage	Il numero totale di messaggi AS2 inviati senza successo a un partner commerciale. Criteri di segnalazione: quando il cliente chiama <code>StartFileTransfer</code> dal connettore AS2 e viene emessa non appena il messaggio in uscita ha terminato l'elaborazione senza successo Unità: numero Periodo: 5 minuti

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 [Protezione e crittografia dei dati](#). 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](#)
- [Approcci di gestione dinamica delle autorizzazioni](#)

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 consente a tale utente di read/write accedere 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:::amzn-s3-demo-bucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/*"]
    }
  ]
}
```

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` 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.

Esempio di politica di sessione

Il codice seguente mostra un esempio di politica 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:HomeFolder`, `transfer:HomeBucket`, e `transfer:HomeDirectory` policy. Questi parametri sono impostati per `HomeDirectory` i parametri configurati per l'utente, come descritto in [HomeDirectory](#) and [Implementazione 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:HomeDirectorydiventahome/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'getaccesso 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 [Autorizzazioni per AssumeRole e AssumeRoleWithWebIdentity](#) nella Guida per l'utente IAM. AssumeRoleWithSAML

 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)"
```

Sostituzioni annidate per le politiche di sessione

Le sostituzioni annidate non vengono eseguite nelle politiche delle sessioni di Transfer Family. Le politiche di sessione possono utilizzare variabili annidate, come. `${transfer:HomeDirectory}`. Quando la policy viene elaborata, la variabile esterna (ad es. `${transfer:HomeDirectory}`) potrebbe essere sostituita con un valore che contiene un'altra variabile (ad esempio, `{amzn-s3-demo-bucket:/${transfer:UserName}}`). Tuttavia, la variabile annidata non viene ulteriormente sostituita con il nome utente effettivo (ad esempio, `johndoe`).

Ciò significa che quando si creano politiche di sessione per Transfer Family, è necessario tenere conto di questo comportamento e assicurarsi che la struttura delle politiche e l'utilizzo variabile siano progettati di conseguenza. Le variabili annidate potrebbero non essere risolte come previsto e la politica potrebbe non concedere le autorizzazioni previste. È importante testare e convalidare a fondo le politiche di sessione per assicurarsi che funzionino come previsto. Questo comportamento è una considerazione fondamentale quando si implementano il controllo degli accessi e le autorizzazioni per l'ambiente Transfer Family.

Una soluzione a questo problema consiste nell'utilizzare il nome effettivo del bucket Amazon S3 nella politica della sessione. Quindi, per esempio, anziché specificare `${transfer:HomeDirectory}` nella politica della sessione, usa quanto segue, dove `amzn-s3-demo-bucket` è il tuo bucket effettivo: `${amzn-s3-demo-bucket/transfer:UserName}`

Approcci di gestione dinamica delle autorizzazioni

Comprendere l'architettura delle autorizzazioni Transfer Family

AWS Transfer Family supporta la gestione dinamica delle autorizzazioni tramite policy di sessione, che consentono di limitare le autorizzazioni effettive dei ruoli IAM in fase di esecuzione. Questo approccio funziona sia per gli utenti gestiti dal servizio che per gli utenti di provider di identità personalizzati, ma è supportato solo per il trasferimento di file da o verso Amazon S3 (non Amazon EFS).

Ogni AWS Transfer Family utente opera con un modello di autorizzazione composto da:

1. Ruolo IAM di base: definisce le autorizzazioni fondamentali per l'utente
2. Politica di sessione opzionale: limita (riduce l'ambito) le autorizzazioni di base in fase di esecuzione

Le autorizzazioni effettive sono l'intersezione tra le autorizzazioni dei ruoli di base e le autorizzazioni dei criteri di sessione. I criteri di sessione possono solo limitare le autorizzazioni; non possono concedere autorizzazioni aggiuntive oltre a quelle consentite dal ruolo di base.

Questa architettura si applica a entrambi i tipi di utenti:

- Service-managed utenti: le politiche di sessione possono essere configurate direttamente nelle impostazioni dell'utente
- Utenti con provider di identità personalizzati: i criteri di sessione possono essere restituiti come parte della risposta di autenticazione o archiviati in Gestione dei segreti AWS

Due approcci alla gestione delle autorizzazioni

Quando si progettano le autorizzazioni per gli utenti di Transfer Family che necessitano di modelli di accesso unici, è possibile scegliere tra due approcci principali:

Un ruolo per utente

Crea un ruolo IAM separato per ogni utente Transfer Family con autorizzazioni specifiche adattate alle esigenze di quell'utente. Utilizza questo approccio quando:

- Ogni utente richiede autorizzazioni molto diverse
- L'amministrazione delle autorizzazioni è gestita da diverse persone all'interno dell'organizzazione
- È necessario un controllo granulare sull'accesso dei singoli utenti

Ruolo condiviso con le politiche di sessione

Utilizza un singolo ruolo IAM con ampie autorizzazioni (come l'accesso a un intero bucket Amazon S3 contenente più home directory di utenti) e applica policy di sessione per limitare ogni utente alla sua area specifica. Questo approccio riduce in modo significativo il sovraccarico amministrativo rispetto alla gestione di ruoli separati per ogni utente. Utilizza questo approccio quando:

- Gli utenti necessitano di tipi di accesso simili ma a risorse diverse (ad esempio, tutti gli utenti devono read/write accedere, ma ognuno solo alla propria cartella)
- Vuoi semplificare la gestione dei ruoli ed evitare di creare dozzine o centinaia di ruoli singoli
- Gli utenti devono accedere alle home directory designate solo all'interno di un bucket condiviso
- L'amministrazione delle autorizzazioni è centralizzata all'interno dell'organizzazione

Ad esempio, invece di creare ruoli separati per gli utenti «alice», «bob» e «charlie», puoi creare un ruolo con accesso all'intero `s3://company-transfers/` bucket, quindi utilizzare le policy di sessione per limitare alice a `s3://company-transfers/alice/`, bob a e così `s3://company-transfers/bob/` via.

Implementazione delle politiche di

Le policy di sessione funzionano limitando le autorizzazioni effettive del ruolo IAM di base assegnato a un utente. Le autorizzazioni finali sono l'intersezione tra le autorizzazioni del ruolo e le autorizzazioni della politica di sessione.

È possibile implementare politiche di sessione dinamiche in due modi:

Sostituzione variabile

Utilizza le variabili della politica di Transfer Family come

`${transfer:Username}${transfer:HomeDirectory}`, e `${transfer:HomeBucket}` nelle politiche di sessione. Queste variabili vengono sostituite automaticamente con i valori effettivi in fase di esecuzione. Per ulteriori informazioni su queste variabili, vedere [Creazione di una politica di sessione per un bucket Amazon S3](#).

Generazione dinamica

Per i provider di identità personalizzati, genera immediatamente policy di sessione come parte della risposta di autenticazione dalla funzione Lambda o dal metodo API Gateway. Questo approccio consente di creare policy altamente personalizzate basate sugli attributi degli utenti, sull'appartenenza ai gruppi o su fonti di dati esterne al momento dell'autenticazione.

È inoltre possibile memorizzare le politiche di sessione pregenerate Gestione dei segreti AWS includendo una chiave denominata `Policy` con la politica di sessione JSON come valore. Ciò consente di utilizzare lo stesso ampio ruolo IAM tra più utenti mantenendo controlli di accesso specifici dell'utente.

 Note

Le policy di sessione sono supportate solo per i trasferimenti di file da e verso Amazon S3. Non si applicano ai file system Amazon EFS. Per Amazon EFS, le autorizzazioni sono regolate UID/GID e i bit di autorizzazione applicati all'interno del file system stesso.

Implementazione per tipo di utente

Service-managed utenti

Per gli utenti gestiti dal servizio, è possibile specificare le politiche di sessione direttamente nella configurazione utente tramite la AWS Transfer Family console, l'API o la CLI. Per ulteriori informazioni, consulta [Lavorare con utenti gestiti dal servizio](#).

Utenti di provider di identità personalizzati

Per gli utenti di provider di identità personalizzati, puoi fornire politiche di sessione in due modi:

- Gestione dei segreti AWS Tramite l'inclusione di una chiave denominata Policy con la politica di sessione come valore
- Direttamente nella risposta della funzione Lambda o nella risposta API Gateway come parte del risultato dell'autenticazione

Per ulteriori informazioni, consulta [Soluzione personalizzata per provider di identità](#).

Esempio: semplificazione della gestione dei ruoli con policy di sessione

Questo esempio dimostra come la gestione dinamica delle autorizzazioni possa ridurre in modo significativo il sovraccarico amministrativo mantenendo al contempo la sicurezza.

Scenario

L'organizzazione ha 50 utenti che necessitano dell'accesso SFTP per trasferire i file. Ogni utente deve accedere alla propria cartella solo all'interno di un bucket Amazon S3 condiviso chiamato `company-transfers`. Senza policy di sessione, avresti bisogno di creare 50 ruoli IAM separati.

Approccio tradizionale (senza politiche di sessione)

- Crea 50 ruoli IAM: `TransferRole-Alice` `TransferRole-Bob` `TransferRole-Charlie`, ecc.

- Ogni ruolo dispone di autorizzazioni specifiche solo per la cartella di quell'utente
- La gestione delle autorizzazioni richiede l'aggiornamento dei singoli ruoli
- L'aggiunta di nuovi utenti richiede la creazione di nuovi ruoli

Approccio dinamico (con politiche di sessione)

- Crea 1 ruolo IAM: `TransferRole-Shared` con ampie autorizzazioni per l'intero bucket
- Utilizza le policy di sessione per limitare ogni utente alla sua cartella specifica in fase di esecuzione
- La gestione delle autorizzazioni richiede l'aggiornamento di un ruolo o di un modello di politica di sessione
- L'aggiunta di nuovi utenti non richiede nuovi ruoli, ma solo la configurazione dell'utente

Implementazione

Ecco come implementeresti l'approccio dinamico (usando il `company-transfers` bucket come esempio da sostituire con il tuo bucket Amazon S3 effettivo):

Per implementare la gestione dinamica delle autorizzazioni

1. Crea un ruolo IAM condiviso con ampie autorizzazioni Amazon S3:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers"
    }
  ]
}
```

```
}
```

2. Crea un modello di policy di sessione che limiti l'accesso alla cartella dell'utente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/${transfer:Username}/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${transfer:Username}*"
        }
      }
    }
  ]
}
```

3. Configura ogni utente con:

- Il ruolo IAM condiviso
- La politica della sessione si applicava come segue:
 - Service-managed utenti: utilizza l'API o la CLI per applicare il JSON tramite il parametro Policy durante la creazione o la modifica degli utenti (la console offre solo opzioni di policy predefinite)
 - Utenti di provider di identità personalizzati: lo restituiscono come parte della risposta della funzione Lambda durante l'autenticazione o lo archiviano Gestione dei segreti AWS come chiave denominata «Policy» insieme alle credenziali dell'utente
- Cartella principale: /company-transfers/\${transfer:Username}/

AWS CloudTrail registrazione per AWS Transfer Family

AWS Transfer Family si integra sia AWS CloudTrail con Amazon che con Amazon CloudWatch. CloudTrail e CloudWatch servono a scopi diversi ma complementari.

- Questo argomento tratta l'integrazione con CloudTrail , un AWS servizio che crea un registro delle azioni intraprese all'interno dell'utente Account AWS. Monitora e registra continuamente le operazioni delle API per attività come AWS Command Line Interface accessi, comandi e operazioni alla console. 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' AWS ambiente. Per i dettagli, consulta la [Guida per l'AWS CloudTrail utente](#).
- [CloudWatch Registrazione Amazon per server AWS Transfer Family](#) copre l'integrazione con CloudWatch, un servizio di monitoraggio di AWS risorse e applicazioni. Raccoglie metriche e log 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](#).

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 stack ordinata delle operazioni API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di AWS Transfer Family, crea un percorso. 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 della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail 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 root o AWS Identity and Access Management utente.
- 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 AWS servizio.

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 inviata AWS Transfer Family, l'indirizzo IP da cui è stata effettuata, 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](#)
- [Esempio di registrazione per la creazione di un server](#)
- [Esempi di log di accesso ai dati](#)

Abilita la AWS CloudTrail registrazione

Puoi monitorare le operazioni AWS Transfer Family dell'API utilizzando AWS CloudTrail. Monitorando le operazioni delle API, è possibile ottenere utili informazioni operative e di sicurezza. 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.

Abilitazione degli eventi relativi ai dati di Amazon S3

Per tenere traccia delle operazioni sui file eseguite AWS Transfer Family sui bucket Amazon S3, è necessario abilitare gli eventi relativi ai dati per tali bucket. Gli eventi relativi ai dati forniscono attività API a livello di oggetto e sono particolarmente utili per tenere traccia dei caricamenti, dei download e di altre operazioni eseguite dagli utenti. AWS Transfer Family

Per abilitare gli eventi relativi ai dati di Amazon S3 per il tuo AWS Transfer Family server:

1. Apri la CloudTrail console all'indirizzo <https://console.aws.amazon.com/cloudtrail/>.
2. Nel riquadro di navigazione, scegli Percorsi, quindi seleziona un percorso esistente o creane uno nuovo.
3. In Data events, scegli Modifica.
4. Per Tipo di evento Data, seleziona S3.
5. Scegli i bucket Amazon S3 per cui registrare gli eventi relativi ai dati. Puoi registrare gli eventi relativi ai dati per tutti i bucket o specificare singoli bucket.
6. Scegli se registrare gli eventi di lettura, gli eventi di scrittura o entrambi.
7. Scegli Save changes (Salva modifiche).

Dopo aver abilitato gli eventi relativi ai dati, puoi accedere a questi log nel bucket Amazon S3 configurato per il tuo trail. CloudTrail I log includono dettagli come l'utente che ha eseguito l'azione,

il timestamp dell'azione, l'oggetto specifico interessato e il `onBehalfOf` campo che consente di tracciare le azioni eseguite. `userId` AWS Transfer Family

Esempio di registrazione per la creazione di un server

L'esempio seguente mostra una voce di CloudTrail registro (in formato JSON) che illustra l'CreateServerazione.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAA4FFF5HHHHH6NNWWW:user1",
    "arn": "arn:aws:sts::123456789102:assumed-role/Admin/user1",
    "accountId": "123456789102",
    "accessKeyId": "AAAA52C2WWWWW3BB4Z",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-12-18T20:03:57Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAAA4FFF5HHHHH6NNWWW",
        "arn": "arn:aws:iam::123456789102:role/Admin",
        "accountId": "123456789102",
        "userName": "Admin"
      }
    }
  },
  "eventTime": "2024-02-05T19:18:53Z",
  "eventSource": "transfer.amazonaws.com",
  "eventName": "CreateServer",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "11.22.1.2",
  "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36",
  "requestParameters": {
    "domain": "S3",
    "hostKey": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "protocols": [
      "SFTP"
    ],
  },
}
```

```

    "protocolDetails": {
      "passiveIp": "AUTO",
      "tlsSessionResumptionMode": "ENFORCED",
      "setStatOption": "DEFAULT"
    },
    "securityPolicyName": "TransferSecurityPolicy-2020-06",
    "s3StorageOptions": {
      "directoryListingOptimization": "ENABLED"
    }
  },
  "responseElements": {
    "serverId": "s-1234abcd5678efghi"
  },
  "requestID": "6fe7e9b1-72fc-45b0-a7f9-5840268aeadf",
  "eventID": "4781364f-7c1e-464e-9598-52d06aa9e63a",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789102",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "transfer.us-east-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
}

```

Esempi di log di accesso ai dati

Quando abiliti gli eventi di dati di Amazon S3 per il tuo CloudTrail percorso, puoi tenere traccia delle operazioni sui file eseguite tramite AWS Transfer Family. Questi log ti aiutano a monitorare chi ha avuto accesso a quali dati, quando e come.

Esempio di immissione del registro per un accesso corretto ai dati

L'esempio seguente mostra una voce di CloudTrail registro per un'operazione di download di file eseguita correttamente AWS Transfer Family.

```

{
  "eventVersion": "1.09",
  "userIdentity": {

```

```

    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:TransferSessionUser",
    "arn": "arn:aws:sts::123456789012:assumed-role/TransferS3AccessRole/
TransferSessionUser",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/TransferS3AccessRole",
        "accountId": "123456789012",
        "userName": "TransferS3AccessRole"
      },
      "attributes": {
        "creationDate": "2025-07-15T16:12:05Z",
        "mfaAuthenticated": "true"
      }
    },
    "invokedBy": "transfer.amazonaws.com"
  },
  "eventTime": "2025-07-15T16:15:22Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "bucketName": "my-transfer-bucket",
    "key": "users/john.doe/reports/quarterly-report-2025-Q2.pdf",
    "Host": "my-transfer-bucket.s3.amazonaws.com",
    "x-amz-request-payer": "requester"
  },
  "responseElements": null,
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2458732,
    "x-amz-id-2":
"EXAMPLE123456789+abcdefghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZ="
  },
  "requestID": "EXAMPLE123456789",
  "eventID": "example12-3456-7890-abcd-ef1234567890",

```

```
{
  "readOnly": true,
  "resources": [
    {
      "type": "AWS::S3::Object",
      "ARN": "arn:aws:s3:::my-transfer-bucket/users/john.doe/reports/quarterly-report-2025-Q2.pdf"
    },
    {
      "accountId": "123456789012",
      "type": "AWS::S3::Bucket",
      "ARN": "arn:aws:s3:::my-transfer-bucket"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "123456789012",
  "eventCategory": "Data",
  "requestParameters": {
    "x-amz-onBehalfOf": "john.doe.sessionid@s-abcd1234efgh5678"
  }
}
```

In questo esempio, prendete nota dei seguenti campi importanti:

- `eventName`: Indica l'operazione API S3 che è stata eseguita (GetObject per il download di un file).
- `requestParameters.bucketName` e `requestParameters.key`: mostra a quale oggetto S3 è stato effettuato l'accesso.
- `additionalEventData.bytesTransferredOut`: mostra la dimensione del file scaricato in byte.
- `requestParameters.x-amz-onBehalfOf`: contiene il AWS Transfer Family nome utente e l'ID di sessione, che consentono di tracciare AWS Transfer Family l'utente che ha eseguito l'azione.

Il `x-amz-onBehalfOf` campo è particolarmente importante in quanto collega la chiamata API S3 all' AWS Transfer Family utente specifico che ha avviato l'azione. Questo campo segue il formato `username.sessionid@server-id`, in cui:

- `username` è il AWS Transfer Family nome utente.
- `sessionid` è un identificatore univoco per la sessione dell'utente.
- `server-id` è l'ID del AWS Transfer Family server.

Operazioni comuni di accesso ai dati

Quando monitori l'accesso ai dati tramite AWS Transfer Family, in genere vedrai le seguenti operazioni dell'API S3 nei tuoi CloudTrail log:

Operazioni S3 comuni nei log AWS Transfer Family

Funzionamento dell'API S3	AWS Transfer Family Azione	Description
GetObject	Scaricamento del file	L'utente ha scaricato un file dal server
PutObject	Caricamento di un file	L'utente ha caricato un file sul server
DeleteObject	Eliminazione di file	L'utente ha eliminato un file dal server
ListObjects o ListObjects V2	Elenco delle directory	L'utente ha elencato i file in una directory
CopyObject	Copia del file	L'utente ha copiato un file all'interno del server

Monitorando queste operazioni nei CloudTrail registri, è possibile tenere traccia di tutte le attività relative ai file eseguite tramite il AWS Transfer Family server, in modo da soddisfare i requisiti di conformità e rilevare gli accessi non autorizzati.

CloudWatch Registrazione Amazon per server AWS Transfer Family

Amazon CloudWatch è un potente servizio di monitoraggio e osservabilità che offre una visibilità completa AWS delle tue risorse, tra cui AWS Transfer Family.

- **Real-time monitoraggio:** CloudWatch monitora le risorse e le applicazioni Transfer Family in tempo reale, consentendoti di tracciare e analizzare le loro prestazioni.
- **Raccolta di metriche:** CloudWatch raccoglie e tiene traccia di varie metriche per le risorse e le applicazioni, che sono variabili che puoi misurare e utilizzare per l'analisi.
- **CloudWatch home page:** La CloudWatch home page mostra automaticamente le metriche su Transfer Family e altri AWS servizi che utilizzi, fornendo una visione centralizzata dei tuoi dati di monitoraggio.
- **Dashboard personalizzate:** puoi creare dashboard personalizzate CloudWatch per visualizzare metriche specifiche per le tue applicazioni personalizzate e le risorse che scegli di monitorare.
- **Allarmi e notifiche:** CloudWatch consente di creare allarmi che monitorano le metriche e attivano notifiche o azioni automatiche quando vengono superate determinate soglie. Questo può essere utile per monitorare l'attività di trasferimento dei file nei server Transfer Family e scalare le risorse di conseguenza.
- **Ottimizzazione dei costi:** è possibile utilizzare i dati raccolti da CloudWatch per identificare le risorse sottoutilizzate e intraprendere azioni, come il blocco o l'eliminazione delle istanze, per ottimizzare i costi.

Nel complesso, le funzionalità di monitoraggio complete lo CloudWatch rendono uno strumento prezioso per la gestione e l'ottimizzazione dell'infrastruttura Transfer Family e delle applicazioni in esecuzione su di essa.

I dettagli per CloudWatch la registrazione delle app web Transfer Family sono disponibili in [CloudTrail registrazione per le app web Transfer Family](#).

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": "*"
  }
]
}

```

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](#)

Creazione, aggiornamento e visualizzazione della registrazione per i server

Per tutti i AWS Transfer Family server, forniamo una registrazione strutturata. Si consiglia di utilizzare la registrazione strutturata per tutti i server Transfer Family nuovi ed esistenti. I vantaggi dell'utilizzo della registrazione strutturata includono quanto segue:

- 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.

Per abilitare la registrazione per i flussi di lavoro collegati ai server, è necessario utilizzare un ruolo di registrazione.

Note

Quando si aggiunge un ruolo di registrazione, il gruppo di registrazione è sempre attivo e non può essere `/aws/transfer/your-serverID` modificato. Ciò significa che, a meno che non inviate i log strutturati del server allo stesso gruppo, accederete a due gruppi di registrazione separati.

Se sai che assocerai un flusso di lavoro al tuo server e quindi devi aggiungere un ruolo di registrazione, puoi configurare la registrazione strutturata per accedere al gruppo di log predefinito di `/aws/transfer/your-serverID`

Per modificare il gruppo di registrazione, consulta l'API

[StructuredLogDestinations](#)Reference.AWS Transfer Family

Se crei un nuovo server utilizzando la console Transfer Family, la registrazione è abilitata per impostazione predefinita. Dopo aver creato il server, è possibile utilizzare l'operazione

UpdateServer API per modificare la configurazione di registrazione. Per informazioni dettagliate, vedi [StructuredLogDestinations](#).

Attualmente, per i flussi di lavoro, se si desidera abilitare la registrazione, è necessario specificare un ruolo di registrazione:

- Se si associa un flusso di lavoro a un server, utilizzando l'operazione CreateServer o l'UpdateServerAPI, 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.

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

Logging role is only required when selecting a workflow in the Managed workflows section below.

Se scegli Crea gruppo di log, la CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) si apre sulla 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.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/scooter ▼



Create log group [↗](#)



Enabling the structured JSON log format will override your existing logging configuration. Potential changes include new log format and log group.

Logging Role [Info](#)

Select an existing role from your account

AWSTransferLoggingAccess ▼



Workflows events will be delivered to a log group labelled with the server ID.

- Il server non ha alcuna registrazione abilitata.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☐ Enable structured JSON logging

Choose an existing log group ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- Nel server è già abilitata la registrazione JSON strutturata, ma non è stato specificato un ruolo di registrazione.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/  ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- Il server ha già abilitato la registrazione JSON strutturata e ha inoltre specificato un ruolo di registrazione.

Edit additional details

Logging [Info](#)

Log group [Info](#)
Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

▼

Logging Role [Info](#)
Select an existing role from your account

▼

 Workflows events will be delivered to a log group labelled with the server ID.

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.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role -	Passive IP -

- La registrazione JSON strutturata è abilitata.

Additional details
Edit

Log group /aws/transfer/s[redacted]	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role -	Passive IP -

- Il ruolo di registrazione è abilitato, ma la registrazione JSON strutturata non è abilitata.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-[redacted]	SetStat option Ignore
Server host key Info SHA256:lx39/[redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role [redacted] execution-role [redacted]	Passive IP -

- Entrambi i tipi di registrazione (ruolo di registrazione e registrazione JSON strutturata) sono abilitati.

Additional details

Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows	Passive IP -

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 CloudWatch delle metriche per i server 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/>.
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": "amzn-s3-demo-bucket",  
        "key": "mary/workflowSteps2.json",  
        "versionId": "version-id",  
        "etag": "etag-id"  
      }  
    }  
  },  
  "workflowId": "w-abcdef01234567890",  
  "executionId": "execution-id",  
  "transferDetails": {  
    "serverId": "s-server-id",  
    "username": "mary",  
    "sessionId": "session-id"  
  }  
}
```

```

    }
  },
  {
    "type": "StepStarted",
    "details": {
      "input": {
        "fileLocation": {
          "backingStore": "S3",
          "bucket": "amzn-s3-demo-bucket",
          "key": "mary/workflowSteps2.json",
          "versionId": "version-id",
          "etag": "etag-id"
        }
      },
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "StepCompleted",
    "details": {
      "output": {},
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "ExecutionCompleted",
    "details": {},
    "workflowId": "w-abcdef01234567890",

```

```
{
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
    "sessionId": "session-id"
  }
}
```

Configura 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 alleggi 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": "*"
    }
  ]
}
```

Nell'esempio precedente policy, for the **Resource**, sostituisci *region-id* and *Account AWS* con i tuoi valori. Ad esempio, **"Resource": "arn:aws::logs:us-east-1:11112223333:log-group:/aws/transfer/*"**

Quindi crei un ruolo e CloudWatch alleggi la politica Logs che hai creato.

Per creare un ruolo IAM e collegare una policy

1. Nel pannello 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 del server, puoi visualizzare i record di autenticazione degli utenti (esito positivo e negativo), i caricamenti dei dati (PUToperazioni) e i download dei dati (GEToperazioni).

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.

The screenshot shows the AWS CloudWatch console interface. On the left, the navigation sidebar is visible with the following items: CloudWatch, Favorites and recents, Dashboards, Alarms (0), Logs (4), Log groups (selected), Logs Insights, Metrics (All metrics, Explorer, Streams), X-Ray traces, Events, Application monitoring, Insights, Settings, and Getting Started.

The main content area displays the details for a specific log group, `/aws/transfer/s-`. The 'Log group details' section includes:

- ARN:** `arn:aws:logs:us-east-2:5:log-group:/aws/transfer/s-:*`
- Creation time:** 2 years ago
- Retention:** Never expire
- Stored bytes:** 39.39 MB
- Metric filters:** 0
- Subscription filters:** 0
- Contributor Insights rules:** -
- Data protection - new:** Inactive
- Sensitive data found - new:** -
- KMS key ID:** -

Below the details, there are tabs for different views: Log streams (selected), Metric filters, Subscription filters, Contributor Insights, Tags, and Data protection - new.

The 'Log streams' tab shows a list of 10 log streams. The first stream is 'ERRORS', and the others are prefixed with 'scooterstack4-'. The table has columns for 'Log stream' and 'Last event time'.

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.

CloudWatch > Log groups > /aws/transfer/s- > ERRORS

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions

Create metric filter

Q

Filter events

Clear

1m

30m

1h

12h

Custom

Display

	Timestamp	Message	
		There are older events to load. Load more.	
	2023-03-23T16:08:29.281-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:30.979-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:32.647-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:34.306-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:36.010-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:37.659-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:12:33.307-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
	2023-03-23T16:12:34.943-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
		ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" SourceIP=	Copy
	2023-03-23T16:12:56.857-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
	2023-03-23T16:12:58.430-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
	2023-03-23T16:13:00.106-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	

- Scegliete qualsiasi altra voce per vedere un esempio di flusso di log.

CloudWatch > Log groups > /aws/transfer/s- > scooterstack4.

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions

Create metric filter

Q

Filter events

Clear

1m

30m

1h

12h

Custom

Display

	Timestamp	Message	
		No older events at this moment. Retry	
	2023-03-23T16:19:43.747-04:00	scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- Client=SSH-2.0- OpenSSH_7.4 Role=arn:aws:iam:: :role/ Kex=	Copy
	2023-03-23T16:19:47.030-04:00	scooterstack4. DISCONNECTED scooterstack4. DISCONNECTED	Copy
		No newer events at this moment. Auto retry paused. Resume	

- 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**

CloudWatch > Log groups > /aws/transfer/s- > decrypt-user.w-

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions Create metric filter

Filter events Clear 1m 30m 1h 12h Custom Display

Timestamp	Message
	There are older events to load. Load more .
2023-03-21T13:37:57.795-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-...
2023-03-21T14:12:02.850-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-...
	<pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-user/test.json.gpg", "versionId": "...", "etag": "..." } } }, "stepType": "DECRYPT", "stepName": "decrypt-step" }, "workflowId": "w-...", "executionId": "...", "transferDetails": { "serverId": "s-...", "username": "decrypt-user", "sessionId": "..." } }</pre>
2023-03-21T14:12:03.464-04:00	{ "type": "StepCompleted", "details": { "output": {}, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-...

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-000000000000000000" },
  statistic: "Average",
  period: cdk.Duration.minutes(1),
}).createAlarm(this, "AWS/Transfer FilesIn", {
  threshold: 1000,
  evaluationPeriods: 10,
  datapointsToAlarm: 5,
  comparisonOperator:
    cloudwatch.ComparisonOperator.GREATER_THAN_OR_EQUAL_TO_THRESHOLD,
});
```

CloudFormation

```
Type: AWS::CloudWatch::Alarm
Properties:
  Namespace: AWS/Transfer
  MetricName: FilesIn
  Dimensions:
    - Name: ServerId
      Value: s-000000000000000000
  Statistic: Average
  Period: 60
  Threshold: 1000
  EvaluationPeriods: 10
  DatapointsToAlarm: 5
  ComparisonOperator: GreaterThanOrEqualToThreshold
```

Registrazione delle operazioni dell'API Amazon S3 nei log di accesso S3

Note

Questa sezione non si applica alle app web Transfer Family.

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

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. Nel AWS, l'impersonificazione intersettoriale può portare al problema del vice confuso. Per ulteriori dettagli, consultare [Cross-service confusa prevenzione sostitutiva](#).

Note

Negli esempi seguenti, sostituisci ciascuno di essi *user input placeholder* con le tue informazioni.

In questi esempi, puoi rimuovere i dettagli ARN per un flusso di lavoro se al server non è collegato alcun flusso di lavoro.

La seguente logging/invoke politica di esempio 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": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

La seguente logging/invoke politica di esempio 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": "111122223333"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:transfer:us-west-2:111122223333:server/server-id",
          "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-  

id"
        ]
      }
    }
  }
}
```

CloudWatch 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](#)
- [Log precedenti per Transfer Family](#)

Log strutturati JSON per Transfer Family

La tabella seguente contiene i dettagli per i campi di immissione del registro per SFTP/FTP/FTPS le azioni Transfer Family, nel nuovo formato di registro strutturato JSON.

Campo	Description	Esempio di inserimento
tipo di attività	L'azione dell'utente	I tipi di attività disponibili sono i seguenti: AUTH_FAIL URE_CONNECTED ,DISCONNEC TED_ERROR,EXIT_REAS

Campo	Description	Esempio di inserimento
		ON ,CLOSE,CREATE_SY MLINK ,DELETE,MKDIR,OPEN,PARTIA LOSE ,RENAME,RMDIR,SETSTAT,TLS_ E_FAILURE .
byte in ingresso	Numero di byte caricati dall'utente	29238420042
byte in uscita	Numero di byte scaricati dall'utente	23094032490328
ciphers	Specifica il codice SSH negoziato per la connessione (i codici disponibili sono elencati in) Algoritmi crittografici	aes256-gcm@openssh.com
client	Il software client dell'utente	SSH-2.0-OpenSSH_7.4
home directory	La directory a cui l'utente finale atterra quando si connette all'endpoint se il suo tipo di home directory èPATH: se dispone di una home directory logica, questo valore è sempre /	/userhome- bucket/test
chiave	Speciifica lo scambio di chiavi SSH negoziato (KEX) per la connessione (i KEX disponibili sono elencati in) Algoritmi crittografici	diffie-hellman-group14-sha256
message	Fornisce ulteriori informazioni relative all'errore	<string>
metodo	Il metodo di autenticazione	publickey

Campo	Description	Esempio di inserimento
mode	Specifica in che modo un client apre un file	CREA TRONCA SCRIVI
operation	L'operazione del client su un file	APRI CHIUDI
path	Il percorso effettivo del file è interessato	/amzn-s3-demo- -file-1.pdf bucket/test
chiave pubblica ssh-	Il corpo della chiave pubblica per l'utente che si connette	AAAAC3NzaC1lZDI1NT E5AAAAIA9OY0qV6XYV HaaOiWAcj2spDJVbgj rqDPY4pxd6GnHl
ssh-public-key-fingerprint	L'impronta digitale della chiave pubblica, mostrata nella console per gli utenti che gestiscono il servizio quando elencano le proprie chiavi utente.	SHA256:BY3gNMHwTfj d4n2VuT4pTyLOk82zW Zj4KEYEu7y4r/0

 Note

Nella console, l'impronta digitale viene visualizzata con i caratteri di riempimento (se presenti): da 0 a 3 segni uguali (=) alla fine. Nella voce di registro, questa imbottitura viene rimossa dall'output.

Campo	Description	Esempio di inserimento
tipo di chiave pubblica ssh-	Tipo di chiave pubblica: Transfer Family supporta RSA-, ECDSA- e chiavi ED25519-formatted	ssh-ed25519
resource-arn	Un identificatore univoco assegnato dal sistema per una risorsa specifica (ad esempio un server)	arn:aws:transfer:ap-northeast-1:12346789012: -1234567890akeu2js2 server/s
role	Il ruolo IAM dell'utente	arn:aws:iam: :0293883675: -role role/testuser
session-id	Un identificatore univoco assegnato dal sistema per una singola sessione	9ca9a0e1cec6ad9d
fonte-ip	Indirizzo IP client	18323,0129
user	Il nome utente dell'utente finale	myname192
politica dell'utente	Le autorizzazioni specificate per l'utente finale: questo campo viene compilato se la politica dell'utente è una politica di sessione.	Il codice JSON per la politica di sessione utilizzata

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
Errori di autenticazione	ERRORI METODO AUTH_FAILURE =PublicKey user=LHR message="RSA+b7+A +HXG0C7L1JIZ0" SourceIP = 3.8.172.211 SHA256:Lfz3R2nmLY4raK Rb1rSvUIbAE
COPY/TAG/DELETE/DECRYPT flusso di lavoro	<pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "BackingStore": "EFS", "fileSystemID": "fs-12345678", "path": "/lhr/regex.py" }, "stepType": "TAG", "stepName": "successful_tag_step", "workflowID": "w-1111aaaa2222bb3", "executionID": "81234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverID": "s-1234abcd5678efghi", "username": "lhr", "sessionID": "1234567890abcdef0" } } } }</pre>
Flusso di lavoro personalizzato in fasi	<pre>{ "tipo": "CustomStepInvoked", "details": { "output": { "token": "CustomStepInvoked", "stepType": "CUSTOM", "stepName": "efs-s3_copy_2", "workflowID": "MzM4Mjg5YWUtYTEzMy00YjIzLWI3OGMtYzU4OGI2ZjQyMzE5", "executionID": "w-9283e49d33297c3f7", "transferDetails": { "serverID": "s-zz1111aaaa22223", "username": "lhr", "sessionID": "1234567890abcdef0" } } } }</pre>
Eliminazioni	lhr.33a8fb495ffb383b ELIMINA Percorso =/bucket/user /123.jpg

Azione	Log corrispondenti all'interno di Amazon CloudWatch Logs
Download	lhr.33a8fb495ffb383b APRI PERCORSO =/ /123.jpg MODE=Leggi bucket/user lhr.33a8fb495ffb383b CHIUDI PERCORSO= / /123.jpg =3618546 bucket/user BytesOut
Logins/Logouts	user.914984e553bcd6db6 SORGENTE CONNESSA IP=1.22.111.222 utente=LH R =CLIENT LOGICO = _7.4 role=ARN: AWS: :iam: :123456789012: -s3-access HomeDir SSH-2.0-OpenSSH role/sftp user.914984e553bcd6db6 DISCONNESSO
Rinomina	lhr.33a8fb495ffb383b RINOMINA Percorso =/ / lambo.png =/ /ferrari.png bucket/user NewPath bucket/user
Esempio di registro degli errori del workflow	<pre>{ "type": "StepErrored", "details": { "errorType": "BAD_REQUEST", "errorMessage": "Impossibile etichettare il file Efs", "stepType": "TAG", "stepName": "successful_tag_step", "workflowID": "w-1234abcd5678efghi", "executionID": "81234abcd-1234-efgh-5678-ijklmnopqr90", "transferDetails": { "serverID": "s-1234abcd5678efghi", "username": "lhr", "sessionId": "1234567890abcdef0" } } }</pre>
Collegamenti simbolici	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK =/fs- /pqr.jpg =abc.jpg LinkPath 12345678/lhr TargetPath

Argomenti

- [Esempio di voci del registro delle sessioni di trasferimento](#)
- [Esempi di voci di registro per i connettori SFTP](#)
- [Esempi di voci di registro per connettori VPC Lattice](#)
- [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/transfer-s3",
  "activity-type": "CONNECTED",
  "ciphers": "chacha20-poly1305@openssh.com,chacha20-poly1305@openssh.com",
  "client": "SSH-2.0-OpenSSH_7.4",
  "source-ip": "52.94.133.133",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "home-dir": "/test/log-me",
  "ssh-public-key":
"AAAAC3NzaC1lZDI1NTE5AAAAIA90Y0qV6XYVHaa0iWAcj2spDJVbgjrqpDY4pxd6GnH1",
  "ssh-public-key-fingerprint": "SHA256:BY3gNMHwTfjd4n2VuT4pTyL0k82zWZj4KEYEu7y4r/0",
  "ssh-public-key-type": "ssh-ed25519",
  "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": "/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": "/test/log-me/config-file",
  "activity-type": "CLOSE",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "bytes-in": "121",
  "session-id": "9ca9a0e1cec6ad9d"
}

{
  "activity-type": "DISCONNECTED",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

Note

I tipi di attività disponibili sono i

seguenti: AUTH_FAILURE, CONNECTED, DISCONNECTED, ERROR, EXIT_REASON, CLOSE, CREATE_SYMLINK, OPENPARTIAL_CLOSE, RENAME, RMDIR, SETSTAT, TLS_RESUME_FAILURE

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 si *connector-id* trova l'identificatore del connettore SFTP. Le voci di registro per i connettori SFTP vengono generate quando si esegue un comando `or.StartFileTransfer` o `or.StartDirectoryListing`.

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:account-id:connector/connector-id",
"local-directory-path": "/connectors-localbucket",
"bytes": 514,
"egress-type": "SERVICE_MANAGED"
}

```

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:account-id:connector/connector-id",
  "local-directory-path": "/connectors-localbucket",
  "egress-type": "SERVICE_MANAGED"
}

```

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": "/amzn-s3-demo-bucket/my-test-folder/connector-metrics-us-east-1-2024-01-02.csv",
    "status-code": "COMPLETED",
    "start-time": "2024-04-24T18:16:12.295235884Z",
    "end-time": "2024-04-24T18:16:12.461840732Z",
    "account-id": "255443218509",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "bytes": 275,
    "egress-type": "SERVICE_MANAGED"
  }

```

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 un'unica operazione `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 per connettori VPC Lattice

Questa sezione contiene log di esempio per i connettori VPC Lattice. Per i connettori VPC Lattice, i log includono campi aggiuntivi che forniscono informazioni sulla configurazione del connettore e sulla configurazione della rete.

Questa voce di registro riguarda un'operazione `SEND` del connettore VPC Lattice completata correttamente.

```

{
  "operation": "SEND",
  "timestamp": "2025-09-05T14:20:19.577192454Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "file-path": ""/amzn-s3-demo-bucket/my-test-folder/connector-vpc-lattice-us-east-1-2025-03-22.csv"",

```

```

"status-code": "COMPLETED",
"start-time": "2025-09-05T14:20:19.434072509Z",
"end-time": "2025-09-05T14:20:19.481453346Z",
"account-id": "account-id",
"connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
"remote-directory-path": "/test-bucket/test-folder/",
"bytes": 262,
"egress-type": "VPC_LATTICE",
"vpc-lattice-resource-configuration-arn": "arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/resource-configuration-arn-id",
"vpc-lattice-port-number": 22
}

```

I log dei connettori VPC Lattice includono i seguenti campi aggiuntivi:

- `egress-type`- Tipo di configurazione di uscita per il connettore
- `vpc-lattice-resource-configuration-arn`- ARN della configurazione delle risorse VPC Lattice che definisce la posizione del server SFTP di destinazione
- `vpc-lattice-port-number`- Numero di porta per la connessione al server SFTP tramite VPC Lattice

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 CloudWatch delle metriche per i server Transfer Family

Note

Puoi anche ottenere le metriche per Transfer Family direttamente dalla console Transfer Family stessa. Per maggiori dettagli, consultare [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.

Namespace	Metrica	Description
AWS/Transfer	BytesIn	Il numero totale di byte trasferiti nel server. Criteri di segnalazione: • Per SFTP/FTP/FTPS: emesso ogni 5 minuti mentre viene stabilita una connessione al server Transfer Family. Se non viene trasferito alcun file o byte nel periodo, viene emesso «0».

Namespace	Metrica	Description
		Per AS2: quando il cliente riceve un messaggio nel proprio server AS2 e viene emesso non appena il messaggio in entrata ha terminato l'elaborazione Unità: numero Periodo: 5 minuti
	BytesOut	Il numero totale di byte trasferiti dal server. Criteri di segnalazione: - Per SFTP/FTP/FTPS: emesso ogni 5 minuti mentre viene stabilita una connessione al server Transfer Family. Se non viene trasferito alcun file o byte nel periodo, viene emesso «0». - Per AS2: quando il cliente chiama <code>StartFileTransfer</code> dal connettore AS2 e viene emesso non appena il messaggio in uscita ha terminato l'elaborazione. Unità: numero Periodo: 5 minuti

Namespace	Metrica	Description
	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. Criteri di segnalazione: • Per SFTP/FTP/FTPS: emesso ogni 5 minuti mentre viene stabilita una connessione al server Transfer Family. Se non viene trasferito alcun file o byte nel periodo, viene emesso «0». • Per AS2: quando il cliente riceve un messaggio nel proprio server AS2 e viene emesso non appena il messaggio in entrata ha terminato l'elaborazione. Unità: numero Periodo: 5 minuti
	FilesOut	Il numero totale di file trasferiti dal server. Criteri di segnalazione: • Per SFTP/FTP/FTPS: emesso ogni 5 minuti mentre viene stabilita una connessione al server Transfer Family. Se non viene trasferito alcun file o byte nel periodo, viene emesso «0». • Per AS2: quando il cliente chiama <code>StartFile Transfer</code> dal connettore AS2 e viene emesso non appena il messaggio in uscita ha terminato l'elaborazione. Unità: numero Periodo: 5 minuti

Namespace	Metrica	Description
	InboundMessage	Il numero totale di messaggi AS2 ricevuti con successo da un partner commerciale. Criteri di segnalazione: quando il cliente riceve un messaggio nel proprio server AS2 e lo invia non appena il messaggio in entrata ha terminato con successo l'elaborazione 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. Criteri di segnalazione: quando il cliente riceve un messaggio nel proprio server AS2 e lo invia non appena il messaggio in entrata ha terminato l'elaborazione senza successo Unità: numero Periodo: 5 minuti
	OnUploadExecutionsStarted	Il numero totale di esecuzioni del flusso di lavoro avviate sul server. Criteri di segnalazione: attivati ogni volta che inizia un'esecuzione Unità: numero Periodo: 1 minuto

Namespace	Metrica	Description
	OnUploadExecutionsSuccess	Il numero totale di esecuzioni di workflow riuscite sul server. Criteri di segnalazione: attivato ogni volta che un'esecuzione viene completata correttamente Unità: numero Periodo: 1 minuto
	OnUploadExecutionsFailed	Il numero totale di esecuzioni di workflow non riuscite sul server. Criteri di segnalazione: attivato ogni volta che un'esecuzione non viene completata correttamente Unità: numero Periodo: 1 minuto
	OutboundMessage	Il numero totale di messaggi AS2 inviati con successo a un partner commerciale. Criteri di segnalazione: quando il cliente chiama <code>StartFileTransfer</code> dal proprio connettore AS2 e viene emessa non appena il messaggio in uscita ha terminato correttamente l'elaborazione Unità: numero Periodo: 5 minuti

Namespace	Metrica	Description
	OutboundFailedMessage	Il numero totale di messaggi AS2 che sono stati inviati senza successo a un partner commerciale. Criteri di segnalazione: quando il cliente chiama <code>StartFileTransfer</code> dal connettore AS2 e viene emessa non appena il messaggio in uscita ha terminato l'elaborazione senza successo Unità: numero Periodo: 5 minuti

Dimensioni Transfer Family

Una dimensione è una name/value coppia che fa parte dell'identità di una metrica. Per ulteriori informazioni sulle dimensioni, consulta [Dimensions](#) nella Amazon CloudWatch User Guide.

La tabella seguente descrive le CloudWatch dimensioni di Transfer Family.

Dimensione	Description
ServerId	L'ID univoco del server.
ConnectorId	L'ID univoco del connettore. Utilizzato per AS2, per OutboundMessage e OutboundFailedMessage

Utilizzo con Notifiche all'utente AWS AWS Transfer Family

Per ricevere notifiche sugli AWS Transfer Family eventi, puoi [Notifiche all'utente AWS](#) impostare 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, [Amazon Q Developer in applicazioni chat](#), notifiche chat, 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 interrogazioni 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. Accedi a Console di gestione AWS e apri 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 responsabili degli 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.

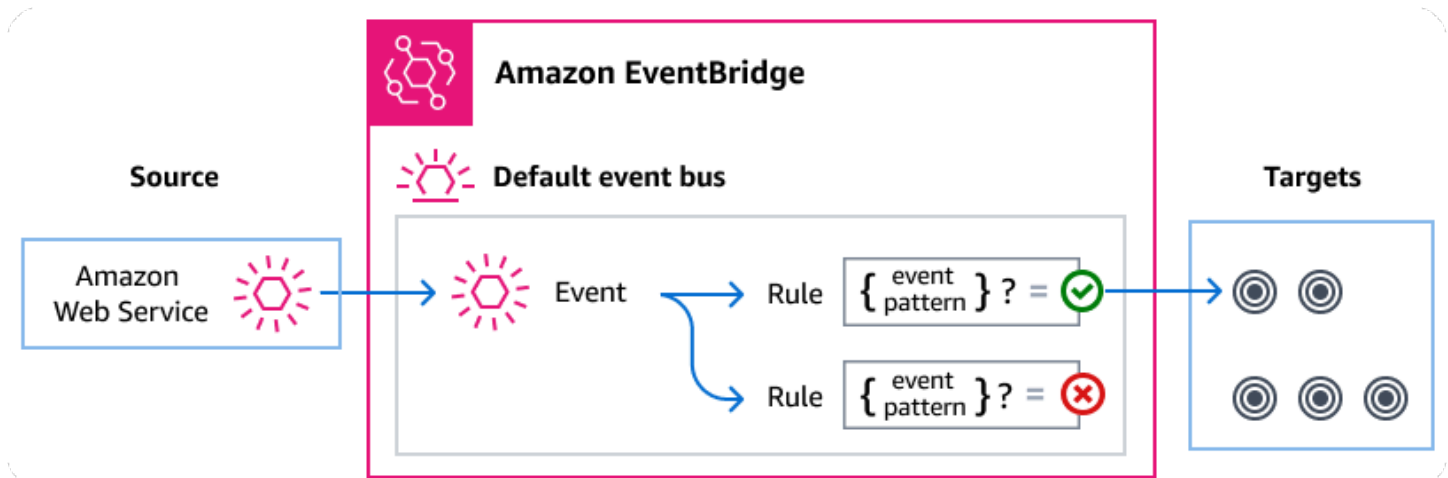
```
filter `activity-type` = 'OPEN'
```

```
| 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. Event-driven l'architettura 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 predefinito. EventBridge 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 zero o 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 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 distribuiti agli obiettivi specificati con il massimo impegno possibile o su base duratura (si noti che alcuni eventi potrebbero essere distribuiti in modo errato). Questi livelli di consegna sono descritti nella sezione [Livello di consegna per gli eventi AWS di servizio](#) in Amazon EventBridge Events Reference.

- Server-level gli eventi per i server SFTP, FTPS e FTP vengono forniti con la massima diligenza possibile.
- Gli eventi del connettore SFTP vengono forniti in modo duraturo.
- Gli eventi AS2 vengono erogati in modo duraturo.

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

Le tabelle seguenti elencano gli eventi per i server SFTP, FTPS e FTP, organizzati per tipo di evento.

Eventi di caricamento e download di file

Tipo di dettaglio dell'evento	Description
Scaricamento dei file dal server FTP completato	Un file è stato scaricato correttamente per il protocollo FTP.
Scaricamento del file dal server FTP non riuscito	Un tentativo di scaricare un file non è riuscito per il protocollo FTP.
Caricamento del file sul server FTP completato	Un file è stato caricato correttamente per il protocollo FTP.
Caricamento del file sul server FTP non riuscito	Un tentativo di caricamento di un file non è riuscito per il protocollo FTP.

Tipo di dettaglio dell'evento	Description
<u>Scaricamento del file dal server FTPS completato</u>	Un file è stato scaricato correttamente per il protocollo FTPS.
<u>Scaricamento del file dal server FTPS non riuscito</u>	Un tentativo di scaricare un file non è riuscito per il protocollo FTPS.
<u>Caricamento del file sul server FTPS completato</u>	Un file è stato caricato correttamente per il protocollo FTPS.
<u>Caricamento del file sul server FTPS non riuscito</u>	Un tentativo di caricamento di un file non è riuscito per il protocollo FTPS.
<u>Download del file dal server SFTP completato</u>	Un file è stato scaricato correttamente per il protocollo SFTP.
<u>Scaricamento del file dal server SFTP non riuscito</u>	Un tentativo di scaricare un file non è riuscito per il protocollo SFTP.
<u>Caricamento del file sul server SFTP completato</u>	Un file è stato caricato correttamente per il protocollo SFTP.
<u>Caricamento del file sul server SFTP non riuscito</u>	Un tentativo di caricamento di un file non è riuscito per il protocollo SFTP.

Altri eventi relativi alle operazioni sui file

Tipo di dettaglio dell'evento	Description
<u>Creazione della directory del server FTP completata</u>	È stata creata correttamente una directory per il protocollo FTP.
<u>Creazione della directory del server FTP non riuscita</u>	Tentativo di creazione di una directory non riuscito per il protocollo FTP.
<u>Eliminazione della directory del server FTP completata</u>	Una directory è stata eliminata con successo per il protocollo FTP.

Tipo di dettaglio dell'evento	Description
Eliminazione della directory del server FTP non riuscita	Un tentativo di eliminare una directory non è riuscito per il protocollo FTP.
Eliminazione del file dal server FTP completata	Un file è stato eliminato con successo per il protocollo FTP.
Eliminazione del file dal server FTP non riuscita	Tentativo di eliminazione di un file non riuscito per il protocollo FTP.
Rinomina file del server FTP completata	Un file è stato rinominato correttamente per il protocollo FTP.
Rinomina file del server FTP non riuscita	Un tentativo di rinominare un file non è riuscito per il protocollo FTP.
Creazione della directory del server FTPS completata	È stata creata correttamente una directory per il protocollo FTPS.
Creazione della directory del server FTPS non riuscita	Tentativo di creazione di una directory non riuscito per il protocollo FTPS.
Eliminazione della directory del server FTPS completata	Una directory è stata eliminata con successo per il protocollo FTPS.
Eliminazione della directory del server FTPS non riuscita	Un tentativo di eliminare una directory non è riuscito per il protocollo FTPS.
Eliminazione del file dal server FTPS completata	Un file è stato eliminato con successo per il protocollo FTPS.
Eliminazione del file dal server FTPS non riuscita	Tentativo di eliminazione di un file non riuscito per il protocollo FTPS.
Rinomina file del server FTPS completata	Un file è stato rinominato correttamente per il protocollo FTPS.
Rinomina file del server FTPS non riuscita	Un tentativo di rinominare un file non è riuscito per il protocollo FTPS.

Tipo di dettaglio dell'evento	Description
Creazione della directory del server SFTP completata	È stata creata correttamente una directory per il protocollo SFTP.
Creazione della directory del server SFTP non riuscita	Un tentativo di creare una directory non è riuscito per il protocollo SFTP.
Eliminazione della directory del server SFTP completata	Una directory è stata eliminata con successo per il protocollo SFTP.
Eliminazione della directory del server SFTP non riuscita	Un tentativo di eliminare una directory non è riuscito per il protocollo SFTP.
Eliminazione dei file dal server SFTP completata	Un file è stato eliminato con successo per il protocollo SFTP.
Eliminazione del file dal server SFTP non riuscita	Un tentativo di eliminare un file non è riuscito per il protocollo SFTP.
Rinomina file del server SFTP completata	Un file è stato rinominato correttamente per il protocollo SFTP.
Rinomina file del server SFTP non riuscita	Un tentativo di rinominare un file non è riuscito per il protocollo SFTP.

Eventi del connettore SFTP

Note

Questi eventi vengono erogati a un EventBridge livello durevole, come descritto nella sezione [Livello di consegna per gli eventi AWS di servizio](#) in Amazon EventBridge Events Reference.

Tipo di dettaglio dell'evento	Description
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 e SFTP completato	Il trasferimento di file da un server SFTP remoto a un connettore è stato completato correttamente.
Recupero dei file del connettore e 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.
Spostamento remoto del connettore SFTP completato	I file o le directory sono stati spostati o rinominati correttamente sul server remoto.
Spostamento remoto del connettore SFTP non riuscito	Impossibile spostare o rinominare file o directory sul server remoto.
Eliminazione remota del connettore SFTP completata	I file o le directory sono stati eliminati correttamente sul server remoto.
Eliminazione remota del connettore SFTP non riuscita	Impossibile eliminare file o directory sul server remoto.

Eventi AS2

Note

Questi eventi vengono erogati a un EventBridge livello durevole, come descritto nella sezione [Livello di consegna per gli eventi AWS di servizio](#) in Amazon EventBridge Events Reference.

Tipo di dettaglio dell'evento	Description
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.

Per registrare AWS Transfer Family eventi in Amazon EventBridge

1. Accedi a Console di gestione AWS e apri la EventBridge console Amazon all'indirizzo <https://console.aws.amazon.com/events/>.
2. Nel riquadro di navigazione, scegli Regole, quindi scegli Crea regola.
3. Inserisci un nome descrittivo per la regola e, facoltativamente, inserisci una descrizione.

4. Per Tipo di regola, seleziona Regola con un modello di evento, quindi scegli Avanti.
5. Nella sezione Origine dell'evento, seleziona AWS eventi o eventi EventBridge partner.
6. Nella sezione Metodo di creazione, scegli Usa modulo modello.
7. Nella sezione Schema di eventi, fornisci le seguenti informazioni.
 - a. Per Origine evento, scegli Servizi AWS .
 - b. Per AWS assistenza, scegli Trasferimento.
 - c. Per Tipo di evento, scegli il tipo di evento Transfer Family che desideri attivare la regola.

A seconda del tipo di evento selezionato, è possibile che venga visualizzata la sezione Specificazione del tipo di evento 1.

- d. Se vedi la sezione Specificazione del tipo di evento 1, seleziona gli eventi specifici che desideri acquisire (oppure seleziona Qualsiasi evento per acquisire tutti gli eventi per il tipo di evento selezionato).
 - e. (Facoltativo) Utilizzate l'editor del modello di evento per specificare i filtri per i dettagli degli eventi.
 - f. Scegli Next (Successivo).
8. Scegliete un obiettivo tra le scelte disponibili in Seleziona obiettivi. Scegli tra i seguenti obiettivi disponibili.
 - AWS servizio. Le opzioni più comuni sono le funzioni Lambda per l'elaborazione senza server, le code Amazon SQS per l'elaborazione dei messaggi, gli argomenti di Amazon SNS per le notifiche e per l'orchestrazione dei flussi di lavoro. AWS Step Functions
 - EventBridge Destinazione API. Se desideri inviare eventi a un endpoint HTTP esterno a AWS, puoi utilizzare una destinazione API come destinazione.
 - EventBridge bus per eventi. Puoi inviare eventi a un altro bus di eventi, nello stesso account e nella stessa regione o in un account o regione diversi.

Per istruzioni complete sulla creazione di regole per i bus degli eventi, consulta [la sezione Creazione di regole che reagiscono agli eventi](#) nella Amazon EventBridge User Guide.

Per assistenza nella selezione di un obiettivo, consulta [Select targets](#) nella Amazon EventBridge User Guide.

9. Configura eventuali opzioni aggiuntive per il tuo obiettivo, quindi scegli Avanti.
10. (Facoltativo) Aggiungi tag alla regola e scegli Avanti.

11. Nella schermata Rivedi e crea, se tutto sembra corretto, scegli Crea regola.

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 l'utente *username*:

```
{
  "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 la 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 Server File 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:

- Creazione della directory del server FTP completata
- Creazione della directory del server FTP non riuscita
- Eliminazione della directory del server FTP completata
- Eliminazione della directory del server FTP non riuscita
- Eliminazione del file dal server FTP completata
- Eliminazione del file dal server FTP non riuscita
- Scaricamento del file dal server FTP completato
- Scaricamento del file dal server FTP non riuscito
- Rinomina file del server FTP completata
- Rinomina file del server FTP non riuscita
- Caricamento del file sul server FTP completato
- Caricamento del file sul server FTP non riuscito
- Creazione della directory del server FTPS completata
- Creazione della directory del server FTPS non riuscita
- Eliminazione della directory del server FTPS completata
- Eliminazione della directory del server FTPS non riuscita
- Eliminazione del file dal server FTPS completata
- Eliminazione del file dal server FTPS non riuscita
- Scaricamento del file dal server FTPS completato
- Scaricamento del file dal server FTPS non riuscito
- Rinomina file del server FTPS completata
- Rinomina file del server FTPS non riuscita
- Caricamento del file sul server FTPS completato
- Caricamento del file sul server FTPS non riuscito
- Creazione della directory del server SFTP completata
- Creazione della directory del server SFTP non riuscita

- Eliminazione della directory del server SFTP completata
- Eliminazione della directory del server SFTP non riuscita
- Eliminazione dei file dal server SFTP completata
- Eliminazione del file del server SFTP non riuscita
- Scaricamento del file dal server SFTP completato
- Scaricamento del file dal server SFTP non riuscito
- Rinomina dei file del server SFTP completata
- Rinomina file del server SFTP non riuscita
- Caricamento dei file del 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",
    "original-file-path" : "string",
    "renamed-file-path" : "string",
    "directory-path" : "string",
    "server-id" : "string",
    "username" : "string",
    "session-id" : "string",
    "start-timestamp" : "string"
  }
}
```

```
}
```

detail-type

Identifica 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 trasferito, eliminato o utilizzato in altro modo.

original-file-path

Per gli eventi di ridenominazione dei file, il percorso originale del file prima della ridenominazione.

renamed-file-path

Per gli eventi di ridenominazione dei file, il nuovo percorso del file dopo la ridenominazione.

directory-path

Per gli eventi di creazione ed eliminazione della directory, il percorso della directory.

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 Server File 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": "/amzn-s3-demo-bucket/test/1mb_file",
    "server-id": "s-1111aaaa2222bbbb3",
    "username": "test",
    "session-id": "event-ID",
    "start-timestamp": "2024-01-29T16:31:42.462088327Z"
  }
}

```

Example Evento di esempio SFTP Server File Delete Completed

L'esempio seguente mostra un evento in cui un file è stato eliminato con successo su un server SFTP.

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Delete Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T14:30:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T14:30:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file-to-delete.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T14:30:26.706282454Z"
  }
}

```

Example Evento di esempio SFTP Server File Rename Completed

L'esempio seguente mostra un evento in cui un file è stato rinominato correttamente su un server SFTP.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Rename Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T15:45:12Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "SFTP",
    "client-ip": "IP-address",
    "end-timestamp": "2025-05-15T15:45:12.749749117Z",
    "original-file-path": "/fs-1234abcd5678efghi/user0/old-filename.txt",
    "renamed-file-path": "/fs-1234abcd5678efghi/user0/new-filename.txt",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2025-05-15T15:45:11.706282454Z"
  }
}
```

Example Evento di esempio SFTP Server Directory Create Completed

L'esempio seguente mostra un evento in cui una directory è stata creata correttamente su un server SFTP.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server Directory Create Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2025-05-15T16:20:05Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "status-code": "COMPLETED",
```

```
{
  "protocol": "SFTP",
  "client-ip": "IP-address",
  "end-timestamp": "2025-05-15T16:20:05.749749117Z",
  "directory-path": "/fs-1234abcd5678efghi/user0/new-directory",
  "server-id": "s-1234abcd5678efghi",
  "username": "test",
  "session-id": "session-ID",
  "start-timestamp": "2025-05-15T16:20:04.706282454Z"
}
```

Eventi del connettore SFTP

Note

Questi eventi vengono erogati a un EventBridge livello durevole, come descritto nella sezione [Livello di consegna per gli eventi AWS di servizio](#) in Amazon EventBridge Events Reference.

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
- Spostamento remoto del connettore SFTP completato
- Spostamento remoto del connettore SFTP non riuscito
- Eliminazione remota del connettore SFTP completata
- Eliminazione remota del connettore SFTP non riuscita

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",
  "egress-type" : "string",
  "vpc-lattice-resource-configuration-arn" : "string",
  "vpc-lattice-port-number" : "number",
  "local-file-location" : {
    "domain" : "string",
    "bucket" : "string",
    "key" : "string"
  },
  "output-file-location" : {
    "domain" : "string",
    "bucket" : "string",
    "key" : "string"
  }
}
}
}

```

detail-type

Identifica 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 directory/file nomi 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 archiviare i risultati dell'elenco. `file/directory`

`listing-id`

Un identificatore univoco per il funzionamento dell'API. `StartDirectoryListing` Questo identificatore può essere utilizzato 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.

`egress-type`

Tipo di configurazione di uscita per il connettore. Valori: `SERVICE_MANAGED` o `VPC_LATTICE`

`vpc-lattice-resource-configuration-arn`

ARN della configurazione delle risorse VPC_LATTICE che definisce la posizione del server SFTP di destinazione. Questo campo è nullo per i connettori gestiti dai servizi.

`vpc-lattice-port-number`

Numero di porta per la connessione al server SFTP tramite VPC_LATTICE.

`local-file-location`

Questo parametro contiene i dettagli della posizione del file di archiviazione. AWS

`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": "/amzn-s3-demo-bucket/testfile.txt",
    "status-code": "FAILED",
    "failure-code": "CONNECTION_ERROR",
    "failure-message": "Unknown Host",
    "remote-directory-path": "",
    "bytes": 0,
    "start-timestamp": "2024-01-24T18:29:33.658729Z",
    "end-timestamp": "2024-01-24T18:29:33.993196Z",
    "local-file-location": {
      "domain": "S3",
      "bucket": "amzn-s3-demo-bucket",
      "key": "testfile.txt"
    }
  }
}
```

Example 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": "/amzn-s3-demo-bucket",
  "bytes": 63533,
  "start-timestamp": "2024-01-24T18:28:07.632388Z",
  "end-timestamp": "2024-01-24T18:28:07.774898Z",
  "local-file-location": {
    "domain": "S3",
    "bucket": "amzn-s3-demo-bucket",
    "key": "testfile.txt"
  }
}
}

```

Example 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": "/amzn-s3-demo-bucket/example/file-listing-output",
"listing-id": "123456-23aa-7980-abc1-1a2b3c4d5e",
"url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",

"status-code": "COMPLETED",
"remote-directory-path": "/home",
"item-count": 10000,
"truncated": true,
"start-timestamp": "2024-01-24T18:28:07.632388Z",
"end-timestamp": "2024-01-24T18:28:07.774898Z",
"output-file-location": {
  "domain": "S3",
  "bucket": "amzn-s3-demo-bucket",
  "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
}
}
```

Eventi AS2

Note

Questi eventi vengono erogati a un EventBridge livello durevole, come descritto nella sezione [Livello di consegna per gli eventi AWS di servizio](#) in Amazon EventBridge Events Reference.

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": "amzn-s3-demo-bucket"
    },
    "client-ip": "client-IP-address",
    "requester-file-name": "testAs2MessageVerifyFile.dat",
    "end-timestamp": "2024-02-07T06:47:06.040031Z",
    "as2-from": "as2-from-ID",
    "as2-message-id": "as2-message-ID",
    "message-subject": "Message from AS2 tests",
```

```

    "start-timestamp": "2024-02-07T06:47:05.410Z",
    "status-code": "PROCESSING",
    "bytes": 63,
    "as2-to": "as2-to-ID",
    "agreement-id": "a-1111aaaa2222bbbb3",
    "server-id": "s-1234abcd5678efghi"
  }
}

```

Example 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": "amzn-s3-demo-bucket1",
      "file-key": "/as2Integ/TestOutboundWrongCert.dat",
      "file-bucket": "amzn-s3-demo-bucket2",
      "json-key": "/as2Integ/failed/TestOutboundWrongCert.dat.json"
    },
    "mdn-message-id": "MDN-message-ID",
    "end-timestamp": "2024-02-06T22:05:09.479878Z",
    "as2-from": "PartnerA",
    "as2-message-id": "as2-message-ID",
    "connector-id": "c-1234abcd5678efghj",
    "message-subject": "Test run from Id 123456789abcde to partner ijklmnop987654",
    "start-timestamp": "2024-02-06T22:05:03Z",
    "failure-code": "VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND",
    "status-code": "FAILED",
    "as2-to": "MyCompany",
    "failure-message": "No public certificate matching message signature could be found in profile: p-1234abcd5678efghj",
    "transfer-id": "transfer-ID"
  }
}

```

```
}
```

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 conformità Servizi 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. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la [Documentazione AWS sulla sicurezza](#).

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

- [Vantaggi della sicurezza della connettività VPC](#)
- [Politiche di sicurezza per i server AWS Transfer Family](#)
- [Politiche di sicurezza per AWS Transfer Family i connettori SFTP](#)
- [Utilizzo dello scambio di chiavi post-quantistiche ibrido con AWS Transfer Family](#)
- [Protezione e crittografia dei dati](#)

- [Gestione delle chiavi SSH e PGP in Transfer Family](#)
- [Gestione delle identità e degli accessi per AWS Transfer Family](#)
- [Convalida della conformità per AWS Transfer Family](#)
- [Resilienza in AWS Transfer Family](#)
- [Crea una connessione privata tra un VPC e le API AWS Transfer Family](#)
- [Sicurezza dell'infrastruttura in AWS Transfer Family](#)
- [Aggiungi un firewall per applicazioni Web](#)
- [Cross-service confusa prevenzione sostitutiva](#)
- [AWS politiche gestite per AWS Transfer Family](#)

Vantaggi della sicurezza della connettività VPC

I connettori SFTP con tipo di uscita VPC offrono vantaggi Cross-VPC di sicurezza avanzati tramite Resource Access:

- Isolamento della rete: tutto il traffico rimane all'interno dell'ambiente VPC, garantendo un isolamento completo della rete dalla rete Internet pubblica per le connessioni endpoint private.
- Controllo IP di origine: i server SFTP remoti vedono solo gli indirizzi IP dell'intervallo CIDR VPC, offrendoti il pieno controllo sugli indirizzi IP di origine utilizzati per le connessioni.
- Accesso privato agli endpoint: Connettiti direttamente ai server SFTP nel tuo VPC utilizzando indirizzi IP privati, eliminando l'esposizione alla rete Internet pubblica.
- Connettività ibrida: accesso sicuro ai server SFTP locali tramite connessioni VPN o Direct Connect consolidate senza ulteriore esposizione a Internet.
- Controlli di sicurezza VPC: sfrutta i gruppi di sicurezza VPC, i NACL e le policy di routing esistenti per controllare e monitorare il traffico dei connettori SFTP.

Modello di sicurezza VPC Lattice

La connettività VPC per connettori SFTP utilizza AWS VPC Lattice con reti di servizi per fornire un accesso multi-tenant sicuro:

- Prevenzione alternativa confusa: i controlli di autenticazione e autorizzazione assicurano che i connettori possano accedere solo alle risorse specifiche per cui sono configurati, impedendo l'accesso non autorizzato tra tenant.

- IPv6-only rete di servizi: utilizza l'indirizzamento IPv6 per evitare potenziali conflitti di indirizzi IP e migliorare l'isolamento della sicurezza.
- Forward Access Session (FAS): la gestione temporanea delle credenziali elimina la necessità di archiviare le credenziali a lungo termine o di condividere manualmente le risorse.
- Resource-level controllo degli accessi: ogni connettore è associato a una configurazione di risorse specifica, che garantisce un controllo granulare degli accessi ai singoli server SFTP.

Best practice di sicurezza per la connettività VPC

Quando utilizzi connettori di tipo VPC in uscita, segui queste best practice di sicurezza:

- Gruppi di sicurezza: configura i gruppi di sicurezza per consentire il traffico SFTP (porta 22) solo tra le risorse necessarie. Limita gli intervalli IP di origine e destinazione al minimo richiesto.
- Posizionamento dei Resource Gateway: implementate i Resource Gateway in sottoreti private quando possibile e assicuratevi che si estendano su almeno due zone di disponibilità per un'elevata disponibilità.
- Monitoraggio della rete: utilizza VPC Flow Logs e Amazon CloudWatch per monitorare i modelli di traffico di rete e rilevare attività anomale.
- Registrazione degli accessi: abilita la registrazione dei connettori per tenere traccia delle attività di trasferimento dei file e mantenere gli audit trail per i requisiti di conformità.
- Gestione della configurazione delle risorse: rivedi e aggiorna regolarmente le configurazioni delle risorse per assicurarti che puntino ai server SFTP corretti e utilizzino le impostazioni di rete appropriate.

Politiche di sicurezza per i server AWS Transfer Family

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), suite di crittografia, cifrari di crittografia dei contenuti e algoritmi di hash) associati al server.

AWS Transfer Family supporta politiche di sicurezza post-quantistiche che utilizzano algoritmi di scambio di chiavi ibridi, combinando metodi crittografici tradizionali con algoritmi post-quantistici per fornire una maggiore sicurezza contro le future minacce informatiche quantistiche. Per ulteriori informazioni, consulta [Utilizzo dello scambio di chiavi post-quantistiche ibrido con AWS Transfer Family](#).

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. [Gestione delle chiavi SSH e PGP in Transfer Family](#)

 Note

A partire dal 2025, tutte le nuove politiche di AWS Transfer Family sicurezza includono il supporto crittografico post-quantistico che utilizza algoritmi di scambio di chiavi ibridi. Per ulteriori informazioni sulla sicurezza post-quantistica, vedere. [Utilizzo dello scambio di chiavi post-quantistiche ibrido con AWS Transfer Family](#)

 Note

Consigliamo vivamente di aggiornare i server alla nostra politica di sicurezza più recente.

- `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.
- Se si crea un server Transfer Family utilizzando CloudFormation e si accetta la politica di sicurezza predefinita, il server viene assegnato `TransferSecurityPolicy-2018-11`.

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](#)

 Note

Le precedenti politiche post-quantistiche (`TransferSecurityPolicy-PQ-SSH-Experimental-2023-04` e `TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04`) sono obsolete. Ti consigliamo invece di utilizzare le nuove politiche.

Per ulteriori informazioni sulla sicurezza in Transfer Family, consulta i seguenti post del blog:

- [Sei suggerimenti per migliorare la sicurezza del tuo AWS Transfer Family server](#)

- [In che modo Transfer Family può aiutarti a creare una soluzione di trasferimento di file gestita sicura e conforme](#)

Argomenti

- [Algoritmi crittografici](#)
- [Dettagli della politica di sicurezza](#)

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`:

- `TransferSecurityPolicy-2018-11`
- `TransferSecurityPolicy-2020-06`
- `TransferSecurityPolicy-FIPS-2020-06`
- `TransferSecurityPolicy-FIPS-2023-05`
- `TransferSecurityPolicy-FIPS-2024-01`

Note

È importante comprendere la distinzione tra il tipo di chiave RSA, che è sempre, `ssh-rsa` e l'algoritmo della chiave host RSA, che può essere uno qualsiasi degli algoritmi supportati.

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.
- I server AS2 utilizzano solo algoritmi nelle sezioni e.
ContentEncryptionCiphersHashAlgorithms Queste sezioni definiscono gli algoritmi utilizzati per crittografare e firmare il contenuto dei file.
- Le politiche FIPS-2024-05 di FIPS-2024-01 sicurezza sono identiche, tranne per il fatto che FIPS-2024-05 non supporta l'`ssh-rsa` algoritmo.
- Transfer Family ha introdotto nuove politiche limitate che sono strettamente parallele alle politiche esistenti:
 - Le TransferSecurityPolicy-Restricted-2018-11 politiche di TransferSecurityPolicy-2018-11 sicurezza sono identiche, tranne per il fatto che la politica limitata non supporta il `chacha20-poly1305@openssh.com` codice.
 - Le politiche TransferSecurityPolicy-Restricted-2020-06 di TransferSecurityPolicy-2020-06 sicurezza sono identiche, tranne per il fatto che la politica con restrizioni non supporta il `chacha20-poly1305@openssh.com` codice.

* Nella tabella seguente, il `chacha20-poly1305@openssh.com` codice è incluso solo nella politica senza restrizioni,

[illegible]

Policy di sicurezza	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-2025-07	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2024-05	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-11	TransferSecurityPolicy-2018-11
SshKexs											
mlkem768x25519-sha256	◆		◆								
mlkem768nistp256-sha256	◆		◆								
mlkem1024nistp384-sha384	◆		◆								
curva25519-sha256	◆	◆	◆	◆		◆		◆			◆
curve25519-sha256@libssh.org		◆	◆	◆		◆		◆			◆

Policy di sicurezza	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11	TransferSecurityPolicy-2018-11
diffie-he												◆
llman-gro												
up14-sha1												
diffie-he									◆	◆	◆	
llman-gru												
ppo14-sha												
256												
diffie-he	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
llman-gru												
ppo16-sha												
512												

Policy di sicurezza	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-ComRestricted-2025-07	TransferSecurityPolicy-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-05	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-03	TransferSecurityPolicy-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-11	TransferSecurityPolicy-2018
diffie-he	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
llman-gru														
ppo18-sha														
512														
diffie-he	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆
llman-gro														
up-exchan														
ge-sha256														
ecdh-sha2	◆	◆		◆	◆	◆					◆	◆	◆	
-nistp256														

Policy di sicurezza	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-ComRestricted-2025-07	TransferSecurityPolicy-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-05	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-03	TransferSecurityPolicy-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-11	TransferSecurityPolicy-2018
ecdh-sha2-nistp384	◆	◆		◆	◆	◆					◆	◆	◆	
ecdh-sha2-nistp521	◆	◆		◆	◆	◆					◆	◆	◆	
SshMacs														
hmac-sha1														◆
hmac-sha1-etm@openssh.com														◆
hmac-sha2-256									◆	◆	◆	◆	◆	

Policy di sicurezza	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-2024-05	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11
hmac-sha256-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
hmac-sha2-512									◆	◆	◆	◆
hmac-sha2-512-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
umac-128-etm@openssh.com										◆		◆
umac-128@openssh.com										◆		◆

Policy di sicurezza	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-FIPS-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Restricted-2025-07			TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06		TransferSecurityPolicy-2018-11
umac-64-hmac@openssh.com											◆
umac-64@openssh.com											◆
ContentEncryptionCiphers											
aes256-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes192-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes128-cbc	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
3des-cbc	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆
HashAlgorithms											
sha256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Policy di sicurezza	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-2024-05	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2023-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Restricted-2025-07			TransferSecurityPolicy-2024-05				TransferSecurityPolicy-2020-06		TransferSecurityPolicy-2018-11
sha384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha512	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha1	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆
TlsCiphers												
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Policy di sicurezza	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-FIPS-2024-05	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11
			Compliant-2025-02	Restricted-2025-07		TransferSecurityPolicy-FIPS-2024-05				TransferSecurityPolicy-Restricted-2020-06		TransferSecurityPolicy-Restricted-2018-11
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	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11
			Compliant-2025-02	Restricted-2025-07		TransferSecurityPolicy-FIPS-2024-05			TransferSecurityPolicy-FIPS-Restricted-2020-06		TransferSecurityPolicy-FIPS-Restricted-2018-11
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_RSA_WITH_AES_128_CBC_SHA256											◆
TLS_RSA_WITH_AES_128_CBC_SHA256											◆

Dettagli della politica di sicurezza

Le seguenti sezioni contengono la rappresentazione JSON di ogni policy di sicurezza.

TransferSecurityPolicy-2025-03

Di seguito viene illustrata la politica TransferSecurityPolicy-2025-03 di sicurezza.

```
{
  "SecurityPolicy": {
```

```
"Fips": false,
"SecurityPolicyName": "TransferSecurityPolicy-2025-03",
"SshCiphers": [
    "aes256-gcm@openssh.com",
    "aes128-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
],
"SshKexs": [
    "mlkem768x25519-sha256",
    "mlkem768nistp256-sha256",
    "mlkem1024nistp384-sha384",
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "curve25519-sha256",
    "curve25519-sha256@libssh.org",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group-exchange-sha256"
],
"SshMacs": [
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com"
],
"ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
],
"HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
],
"TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
```

```

        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-FIPS-2025-03

Di seguito viene illustrata la politica TransferSecurityPolicy-FIPS-2025-03 di sicurezza.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2025-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr",
      "aes128-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [

```

```

        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}

```

TransferSecurityPolicy-AS2Restricted-2025-07

Questa politica di sicurezza è progettata per i trasferimenti di file AS2 che richiedono una maggiore sicurezza escludendo gli algoritmi crittografici legacy. Supporta i moderni algoritmi di crittografia AES e SHA-2 hash, rimuovendo al contempo il supporto per algoritmi più deboli come 3DES e SHA-1.

Note

Questa politica di sicurezza è identica a TransferSecurityPolicy-2025-03, tranne per il fatto che non supporta 3DES (in ContentEncryptionCiphers) e non supporta SHA1 (in HashAlgorithms Include tutti gli algoritmi del periodo 2025-03, inclusi gli algoritmi crittografici post-quantistici (mlkem* KeXs).

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-AS2Restricted-2025-07",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",

```



```

        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}
}

```

TransferSecurityPolicy-SshAuditCompliant-2025-02

Di seguito viene illustrata la politica TransferSecurityPolicy-SshAuditCompliant-2025-02 di sicurezza.

Note

Questa politica di sicurezza è progettata sulla base delle raccomandazioni fornite dallo `ssh-audit` strumento ed è conforme al 100% a tale strumento.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "Protocols": [
      "SFTP",
      "FTPS"
    ],
    "SecurityPolicyName": "TransferSecurityPolicy-SshAuditCompliant-2025-02",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group18-sha512",

```

```

    "diffie-hellman-group16-sha512",
    "diffie-hellman-group-exchange-sha256"
  ],
  "SshMacs": [
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ],
  "Type": "SERVER"
}

```

TransferSecurityPolicy-2024-01

Di seguito viene illustrata la politica TransferSecurityPolicy-2024-01 di sicurezza.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",

```

```
        "aes256-gcm@openssh.com",
        "aes128-ctr",
        "aes256-ctr",
        "aes192-ctr"
    ],
    "SshKexs": [
        "ecdh-sha2-nistp256",
        "ecdh-sha2-nistp384",
        "ecdh-sha2-nistp521",
        "curve25519-sha256",
        "curve25519-sha256@libssh.org",
        "diffie-hellman-group18-sha512",
        "diffie-hellman-group16-sha512",
        "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
        "hmac-sha2-256-etm@openssh.com",
        "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}
```

TransferSecurityPolicy-FIPS-2024-01/TransferSecurityPolicy-FIPS-2024-05

Di seguito vengono illustrate le TransferSecurityPolicy-FIPS-2024-01 e le politiche di TransferSecurityPolicy-FIPS-2024-05 sicurezza.

Note

Gli endpoint TransferSecurityPolicy-FIPS-2024-01 e le politiche di TransferSecurityPolicy-FIPS-2024-05 sicurezza del servizio FIPS sono disponibili solo in alcune AWS regioni. 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 TransferSecurityPolicy-FIPS-2024-01 supporta l'`ssh-rsa` algoritmo e TransferSecurityPolicy-FIPS-2024-05 non lo supporta.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
```

```

        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-2023-05

Di seguito viene illustrata la politica TransferSecurityPolicy-2023-05 di sicurezza.

```

{
  "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"
    ]
  }
}

```

```

    ],
    "SshMac": [
        "hmac-sha2-512-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "sha1"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-FIPS-2023-05

I dettagli della certificazione FIPS per sono AWS Transfer Family disponibili all'indirizzo <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Di seguito viene illustrata la politica TransferSecurityPolicy-FIPS-2023-05 di sicurezza.

Note

L'endpoint e la politica di TransferSecurityPolicy-FIPS-2023-05 sicurezza del servizio FIPS sono disponibili solo in alcune AWS regioni. 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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}
```

TransferSecurityPolicy-2022-03

Di seguito viene illustrata la politica TransferSecurityPolicy-2022-03 di sicurezza.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2022-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
```



```

    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-2020-06 e TransferSecurityPolicy-Restricted-2020-06

Di seguito viene illustrata la politica TransferSecurityPolicy-2020-06 di sicurezza.

Note

Le TransferSecurityPolicy-Restricted-2020-06 politiche di TransferSecurityPolicy-2020-06 sicurezza sono identiche, tranne per il fatto che la politica con restrizioni non supporta il `chacha20-poly1305@openssh.com` codice.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2020-06
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [

```

```

    "umac-128-etm@openssh.com",
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com",
    "umac-128@openssh.com",
    "hmac-sha2-256",
    "hmac-sha2-512"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-FIPS-2020-06

I dettagli della certificazione FIPS per sono AWS Transfer Family disponibili all'indirizzo <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Di seguito viene illustrata la politica TransferSecurityPolicy-FIPS-2020-06 di sicurezza.

 Note

L'endpoint e la politica di TransferSecurityPolicy-FIPS-2020-06 sicurezza del servizio FIPS sono disponibili solo in alcune AWS regioni. 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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
```

```

    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
}

```

TransferSecurityPolicy-2018-11 e TransferSecurityPolicy-Restricted-2018-11

Di seguito viene illustrata la politica TransferSecurityPolicy-2018-11 di sicurezza.

Note

Le TransferSecurityPolicy-Restricted-2018-11 politiche di TransferSecurityPolicy-2018-11 sicurezza sono identiche, tranne per il fatto che la politica con restrizioni non supporta il `chacha20-poly1305@openssh.com` codice.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2018-11
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "curve25519-sha256",

```

```

    "curve25519-sha256@libssh.org",
    "ecdh-sha2-nistp256",
    "ecdh-sha2-nistp384",
    "ecdh-sha2-nistp521",
    "diffie-hellman-group-exchange-sha256",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group14-sha256",
    "diffie-hellman-group14-sha1"
  ],
  "SshMacs": [
    "umac-64-etm@openssh.com",
    "umac-128-etm@openssh.com",
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com",
    "hmac-sha1-etm@openssh.com",
    "umac-64@openssh.com",
    "umac-128@openssh.com",
    "hmac-sha2-256",
    "hmac-sha2-512",
    "hmac-sha1"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
    "TLS_RSA_WITH_AES_128_CBC_SHA256",

```

```
    "TLS_RSA_WITH_AES_256_CBC_SHA256"  
  ]  
}  
}
```

Politiche di sicurezza per AWS Transfer Family 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.

Algoritmi crittografici

Per le chiavi host, i connettori SFTP supportano tutti gli algoritmi supportati per i server Transfer Family, ad eccezione di `ed25519`:

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

Inoltre, per le chiavi host, `ssh-rsa` supportiamo, ma solo per.

`TransferSFTPConnectorSecurityPolicy-2023-07`

Per l'autenticazione, i connettori SFTP supportano i seguenti tipi di chiavi:

- ssh-rsa
- ecdsa

Dettagli sulla politica di sicurezza del connettore SFTP

La tabella seguente mostra gli algoritmi crittografici specifici supportati da ogni politica di sicurezza del connettore SFTP.

Policy di sicurezza	TransferSFTPConne torSecurityPolicy- FIPS-2024-10	TransferSFTPConne torSecurityPolicy- 2024-03	TransferSFTPConne torSecurityPolicy- 2023-07
Ciphers			
aes128-ctr			◆
aes128-gc m@openssh.com	◆	◆	◆
aes192-ctr		◆	◆
aes256-ctr		◆	◆
aes256-gc m@openssh.com	◆	◆	◆
Kexs			
curva 25519-sha256		◆	◆
curve25519-sha256@ libssh.org		◆	◆
diffie-hellman-gro up14-sha1			◆
diffie-hellman-gru ppo16-sha512		◆	◆

Policy di sicurezza	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
diffie-hellman-group18-sha512		◆	◆
diffie-hellman-group-exchange-sha256		◆	◆
ecdh-sha2-nistp256	◆		
ecdh-sha2-nistp384	◆		
ecdh-sha2-nistp521	◆		
Macs			
hmac-sha2-512-etm@openssh.com		◆	◆
hmac-sha2-256-etm@openssh.com		◆	◆
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		◆	◆

Policy di sicurezza	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
ecdsa-sha2-nistp521		◆	◆
ssh rsa			◆

Utilizzo dello scambio di chiavi post-quantistiche ibrido con AWS Transfer Family

Transfer Family supporta un'opzione ibrida di creazione di chiavi post-quantistiche per il protocollo Secure Shell (SSH). Post-quantum la definizione delle chiavi 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 che si chiama 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). Post-quantum la creazione di chiavi ibride 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 della crittografia. Post-Quantum](#)

Indice

- [Informazioni sullo scambio di chiavi ibride post-quantistiche in SSH](#)
- [Come funziona la creazione di chiavi ibride post-quantistiche in Transfer Family](#)
 - [Perché? ML-KEM](#)
 - [Post-quantum scambio di chiavi SSH ibride e requisiti crittografici \(FIPS 140\)](#)
- [Test dello scambio di chiavi ibride post-quantistiche in Transfer Family](#)
 - [Abilita lo scambio di chiavi ibride post-quantistiche sul tuo endpoint SFTP](#)
 - [Configura un client SFTP che supporti lo scambio di chiavi ibride post-quantistiche](#)
 - [Conferma lo scambio di chiavi ibride post-quantistiche in SFTP](#)

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 \(ECDH\)](#), sia. ML-KEM ML-KEM 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 standard di accordo di chiavi post-quantistiche.

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 file da azienda a azienda verso i 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 e ML-KEM-768, con ECDH, su curve P256 ML-KEM-1024, P384 o Curve25519. [I seguenti metodi di scambio di chiavi SSH corrispondenti sono specificati nella bozza di scambio di chiavi SSH ibrida post-quantistica.](#)

- mlkem768nistp256-sha256
- mlkem1024nistp384-sha384
- mlkem768x25519-sha256

Perché? ML-KEM

AWS si impegna a supportare algoritmi standardizzati e interoperabili. ML-KEM [è l'unico algoritmo di scambio di chiavi post-quantistico standardizzato e approvato dal progetto NIST Cryptography. Post-Quantum](#). Gli enti di normazione si stanno già integrando nei protocolli. ML-KEM AWS supporta già TLS ML-KEM in alcuni endpoint AWS API.

Come parte di questo impegno, AWS ha presentato una bozza di proposta all'IETF per la crittografia post-quantistica che si combina ML-KEM con NIST-approved curve 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 sezione [Come funziona la creazione di chiavi ibride post-quantistiche in Transfer Family](#)) potrebbero cambiare man mano che la bozza si evolve verso la standardizzazione.

Note

Post-quantum Il supporto degli algoritmi è attualmente disponibile per lo scambio di chiavi ibride post-quantistiche in TLS AWS KMS (vedi [Utilizzo del TLS ibrido post-quantistico](#) con) e gli endpoint API. AWS KMSAWS Certificate Manager Gestione dei segreti AWS

Post-quantum scambio di chiavi SSH ibride e requisiti crittografici (FIPS 140)

Per i clienti che richiedono la conformità FIPS, Transfer Family fornisce la FIPS-approved crittografia in SSH utilizzando la libreria crittografica open source certificata AWS FIPS 140, -LC. AWS I metodi di scambio di chiavi ibridi post-quantistici supportati TransferSecurityPolicy-FIPS-2025-03 nella 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 ibride post-quantistiche.

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 esempio [Configura 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 Console di gestione AWS policy SSH.

Cryptographic algorithm options [Info](#)

Security Policy

Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 ▲

Find a security policy

TransferSecurityPolicy-2018-11
TransferSecurityPolicy-2020-06
TransferSecurityPolicy-2022-03
TransferSecurityPolicy-2023-05
TransferSecurityPolicy-2024-01
TransferSecurityPolicy-2025-03 ✓
TransferSecurityPolicy-Restricted-2018-11
TransferSecurityPolicy-Restricted-2020-06

to it. Additi

I nomi delle policy SSH che supportano lo scambio di chiavi post-quantistiche sono e. TransferSecurityPolicy-2025-03TransferSecurityPolicy-FIPS-2025-03 Per maggiori dettagli sulle politiche di Transfer Family, consulta [Politiche di sicurezza per i server AWS Transfer Family](#).

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. Installa il client OpenSSH più recente (ad esempio la versione 9.9) sul tuo sistema locale per eseguire il test.

Note

Assicurati che il tuo client supporti uno o più degli ML-KEM algoritmi elencati in precedenza. Puoi visualizzare gli algoritmi supportati per la tua versione di OpenSSH eseguendo questo comando: `ssh -Q kex`

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 mostrato nel comando seguente.

```
sftp -v -o \
  KexAlgorithms=mlkem768x25519-sha256 \
  -i username_private_key_PEM_file \
  username@server-id.server.transfer.region-id.amazonaws.com
```

Nel comando precedente, sostituite i seguenti elementi con le vostre informazioni:

- Sostituisci *username_private_key_PEM_file* con il file di chiave PEM-encoded privata dell'utente SFTP
- Sostituisci *username* 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 OpenSSH 9.9, l'output dovrebbe essere simile al seguente (omettendo informazioni irrilevanti per brevità):

```
% sftp -o KexAlgorithms=mlkem768x25519-sha256 -v -o IdentitiesOnly=yes -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_9.9p2, OpenSSL 3.4.1 11 Feb 2025
debug1: Reading configuration data /Users/username/.ssh/config
debug1: /Users/username/.ssh/config line 146: Applying options for *
debug1: Reading configuration data /Users/username/.ssh/bastions-config
debug1: Reading configuration data /opt/homebrew/etc/ssh/ssh_config
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
[xxx.yyy.zzz.nnn] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_9.9
debug1: Remote protocol version 2.0, remote software version AWS_SFTP_1.1
debug1: compat_banner: no match: AWS_SFTP_1.1
debug1: Authenticating to s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com:22 as 'username'
debug1: load_hostkeys: fopen /Users/username/.ssh/known_hosts2: No such file or
directory
[...]
```

```
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: mlkem768x25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: kex: client->server cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:Ic1Ti0cdDmFdStj06rfU0cmmNccwAha/ASH2unr6zX0
[...]
debug1: rekey out after 4294967296 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 4294967296 blocks
[...]
Authenticated to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
([xxx.yyy.zzz.nnn]:22) using "publickey".
debug1: channel 0: new session [client-session] (inactive timeout: 0)
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
sftp>
```

L'output mostra che la negoziazione con il client è avvenuta utilizzando il metodo ibrido post-quantistico e ha stabilito con successo una sessione SFTP. `mlkem768x25519-sha256`

Protezione e crittografia dei dati

Il modello di [responsabilità AWS condivisa Modello](#) 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 del controllo dei 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 dell' AWS account e di configurare account utente individuali con AWS IAM Identity Center. 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.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. 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.

Crittografia dei dati in Transfer Family

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 di Amazon S3 SSE-S3 () AWS Key Management Service o () chiavi gestite AWS KMS(). SSE-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 Include 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",
    "kms:GetPublicKey",
    "kms:ListKeyPolicies"
  ],
  "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](#).

AWS Transfer Family crittografia a riposo

Poiché AWS Transfer Family è un servizio di trasferimento di file, non gestisce i dati di archiviazione inattivi. I servizi e i sistemi di archiviazione che lo AWS Transfer Family supportano sono responsabili della protezione dei dati in tale stato. Tuttavia, alcuni dati relativi ai servizi vengono AWS Transfer Family gestiti a riposo.

Cosa è crittografato?

Gli unici dati AWS Transfer Family archiviati riguardano i dettagli necessari per gestire i server di trasferimento file ed elaborare i trasferimenti. AWS Transfer Family archivia i seguenti dati con crittografia completa a riposo in Amazon DynamoDB:

- configurazioni del server (ad esempio, impostazioni del server, configurazioni dei protocolli e dettagli degli endpoint).
- Dati di autenticazione utente, incluse chiavi pubbliche SSH e metadati utente.
- Dettagli sull'esecuzione del flusso di lavoro e configurazioni delle fasi.
- Configurazioni dei connettori e credenziali di autenticazione per sistemi di terze parti. Queste credenziali vengono crittografate utilizzando chiavi di crittografia AWS Transfer Family gestite.

Gestione delle chiavi

Non è possibile gestire le chiavi di crittografia AWS Transfer Family utilizzate per archiviare le informazioni in DynamoDB relative alla gestione dei server e all'elaborazione dei trasferimenti. Queste informazioni includono le configurazioni del server, i dati di autenticazione degli utenti, i dettagli del flusso di lavoro e le credenziali dei connettori.

Cosa non è crittografato?

Sebbene AWS Transfer Family non controlli il modo in cui i dati di archiviazione vengono crittografati quando sono archiviati, consigliamo comunque di configurare le posizioni di archiviazione con il massimo livello di sicurezza supportato. Ad esempio, puoi crittografare oggetti con chiavi di crittografia gestite di Amazon S3 SSE-S3 () AWS KMS o chiavi SSE-KMS ().

Scopri di più su come i servizi AWS di storage crittografano i dati inattivi:

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

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 AWS Transfer Family and AWS Lambda](#). Per la distribuzione e la gestione automatizzate degli utenti con più chiavi SSH, consulta [Moduli Transfer Family Terraform](#).

Note

AWS Transfer Family accetta le chiavi RSA, ECDSA ed ED25519 per l'autenticazione SSH.

Questa sezione spiega anche come generare e gestire le chiavi Pretty Good Privacy (PGP).

Per una panoramica completa di tutti gli algoritmi di crittografia e chiave supportati, inclusi consigli per diversi casi d'uso, consulta [Panoramica sulla crittografia e sugli algoritmi chiave](#).

Panoramica sulla crittografia e sugli algoritmi chiave

AWS Transfer Family supporta diversi tipi di algoritmi per scopi diversi. La comprensione degli algoritmi da utilizzare per il caso d'uso specifico aiuta a garantire trasferimenti di file sicuri e compatibili.

Riferimento rapido all'algoritmo

Caso d'uso	Algoritmo consigliato	Conforme a FIPS	Note
SSH/SFTP Autenticazione	RSA (rsa-sha2-256/512), ECDSA o ED25519	RSA: Sì, ECDSA: Sì, ED25519: no	Compatibile con tutti i client e server SSH
Generazione di chiavi PGP	RSA o ECC (NIST)	Sì	Per la decrittografia del flusso di lavoro
Crittografia dei file PGP	AES-256	Sì	Determinata dal software PGP

Algoritmi di autenticazione SSH

Questi algoritmi vengono utilizzati per SSH/SFTP l'autenticazione tra client e AWS Transfer Family server. Scegli uno di questi quando generi coppie di chiavi SSH per l'autenticazione dell'utente o le chiavi dell'host del server.

RSA (consigliato)

Compatibile con tutti i client e server SSH e. FIPS-compliant Utilizzalo con l' SHA-2 hashing per una maggiore sicurezza:

- `rsa-sha2-256`- Consigliato per la maggior parte dei casi d'uso
- `rsa-sha2-512`- Opzione di sicurezza più elevata

ED25519

Moderno ed efficiente. Chiavi di dimensioni ridotte con elevata sicurezza:

- `ssh-ed25519`- Veloce e sicuro, ma non FIPS-compliant

ECDSA

Opzione curva ellittica. Buon equilibrio tra sicurezza e prestazioni:

- `ecdsa-sha2-nistp256`- Curva standard
- `ecdsa-sha2-nistp384`- Curva di sicurezza più elevata
- `ecdsa-sha2-nistp521`- Curva di sicurezza più elevata

Note

`ssh-rsa`Supportiamo SHA1 per le politiche di sicurezza precedenti. Per informazioni dettagliate, vedi [Algoritmi crittografici](#).

Scegliere l'algoritmo SSH giusto

- Per la maggior parte degli utenti: usa RSA con o `rsa-sha2-256` `rsa-sha2-512`
- Per la conformità FIPS: utilizza algoritmi RSA o ECDSA
- Per ambienti moderni: ED25519 offre sicurezza e prestazioni eccellenti

Algoritmi di crittografia e decrittografia PGP

PGP (Pretty Good Privacy) utilizza due tipi di algoritmi che collaborano per crittografare e decrittografare i file nei flussi di lavoro:

1. Algoritmi di coppie di chiavi: utilizzati per generare le coppie di chiavi per la crittografia e le firme digitali public/private
2. Algoritmi simmetrici: utilizzati per crittografare i dati effettivi del file (gli algoritmi di key pair crittografano la chiave simmetrica)

Algoritmi di key pair PGP

Scegli uno di questi algoritmi quando generi coppie di chiavi PGP per la decrittografia del flusso di lavoro:

RSA (consigliato)

Consigliato per la maggior parte degli utenti. Ampiamente supportato, consolidato e FIPS-compliant. Fornisce un buon equilibrio tra sicurezza e compatibilità.

ECC (crittografia a curva ellittica)

Più efficiente di RSA con chiavi di dimensioni ridotte pur mantenendo una sicurezza elevata:

- Curve NIST: curve standard ampiamente supportate e FIPS-compliant
- BrainPool curve - Curve alternative per requisiti di conformità specifici
- Curve25519 - Curva moderna ad alte prestazioni che offre una forte sicurezza con un calcolo efficiente

ElGamal

Algoritmo legacy. Supportato per la compatibilità con i sistemi precedenti. Usa RSA o ECC per nuove implementazioni.

Per istruzioni dettagliate sulla generazione di chiavi PGP, consulta [Genera chiavi PGP](#)

Algoritmi di crittografia simmetrica PGP

Questi algoritmi crittografano i dati effettivi dei file. L'algoritmo utilizzato dipende da come il file PGP è stato creato dal software PGP:

FIPS-compliant algoritmi (consigliati per ambienti regolamentati)

- AES-128, AES-192, AES-256 - Advanced Encryption Standard (consigliato)
- 3DES - Triple Data Encryption Standard (versione precedente, usa AES quando possibile)

Altri algoritmi supportati

- IDEA, CAST5, Blowfish, DES,,, TwoFish CAMELLIA-128 CAMELLIA-192 CAMELLIA-256

Note

Non si sceglie direttamente l'algoritmo simmetrico quando si utilizzano i AWS Transfer Family flussi di lavoro: è determinato dal software PGP utilizzato per creare il file crittografato. Tuttavia, puoi configurare il tuo software PGP in modo da preferire algoritmi come FIPS-compliant AES-256

Per ulteriori informazioni sugli algoritmi simmetrici supportati, consulta [Algoritmi di crittografia simmetrica supportati](#)

Genera chiavi SSH per gli utenti che gestiscono il 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 di AWS Directory Service per Microsoft Active Directory](#).

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](#)
- [Conversione di una chiave SSH2 in formato chiave pubblica SSH](#)

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.

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 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 RSA-, ECDSA- e chiavi. ED25519-formatted Scegli il comando appropriato in base al tipo di coppia di chiavi che stai generando.

Suggerimento: *key_name* sostituiscilo con il nome effettivo del tuo file di key pair SSH.

- 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
```

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.

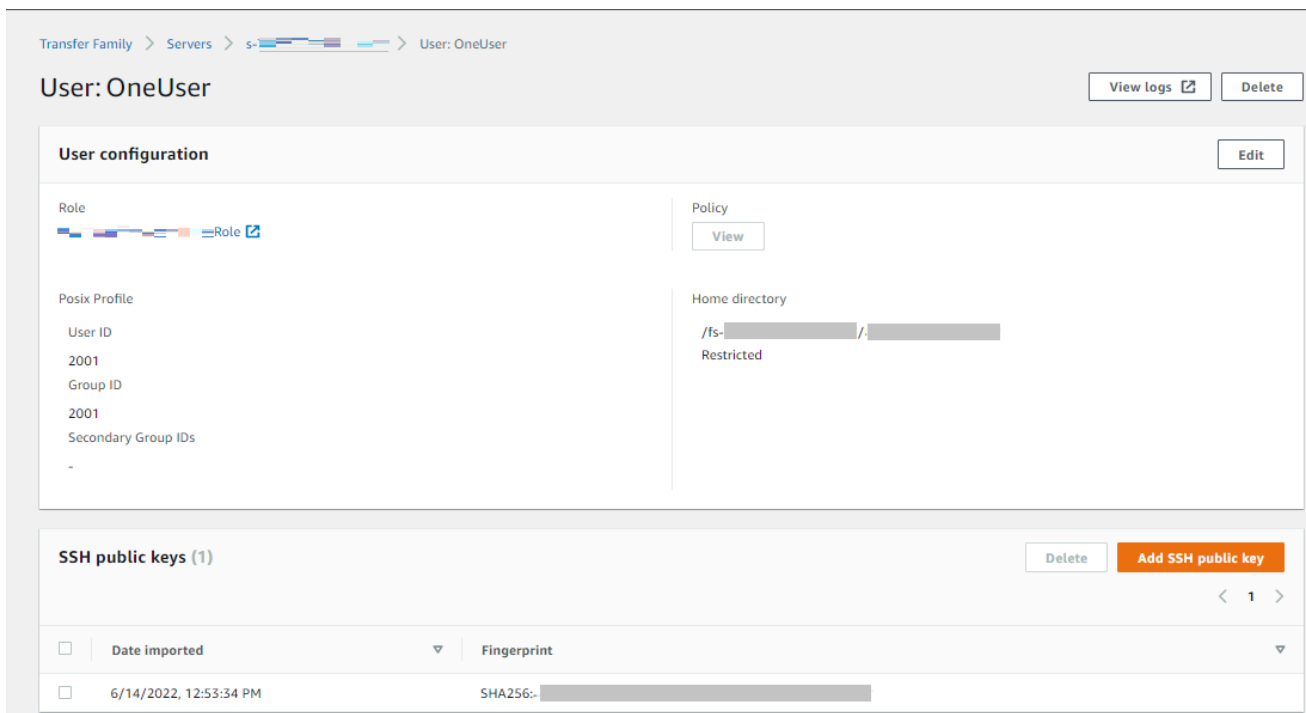
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_name.
Your public key has been saved in key_name.pub.
The key fingerprint is:
SHA256:8tDDwPmanTFcEzjTwPGETVW0GW1nVz+gtCCE8hL7PrQ bob.amazon.com
The key's randomart image is:
+---[RSA 4096]-----+
|    . ....E        |
| .   = ...         |
|. . . = ..o        |
| . o +  oo =       |
| + =  .S.= *       |
| . o o ..B + o     |
|    .o.+.* .       |
|    =o*+*.         |
|    ..*o*+.        |
+----[SHA256]-----+
```

Suggerimento: quando si esegue il `ssh-keygen` comando come illustrato in precedenza, vengono create le chiavi pubbliche e private come file nella directory corrente.

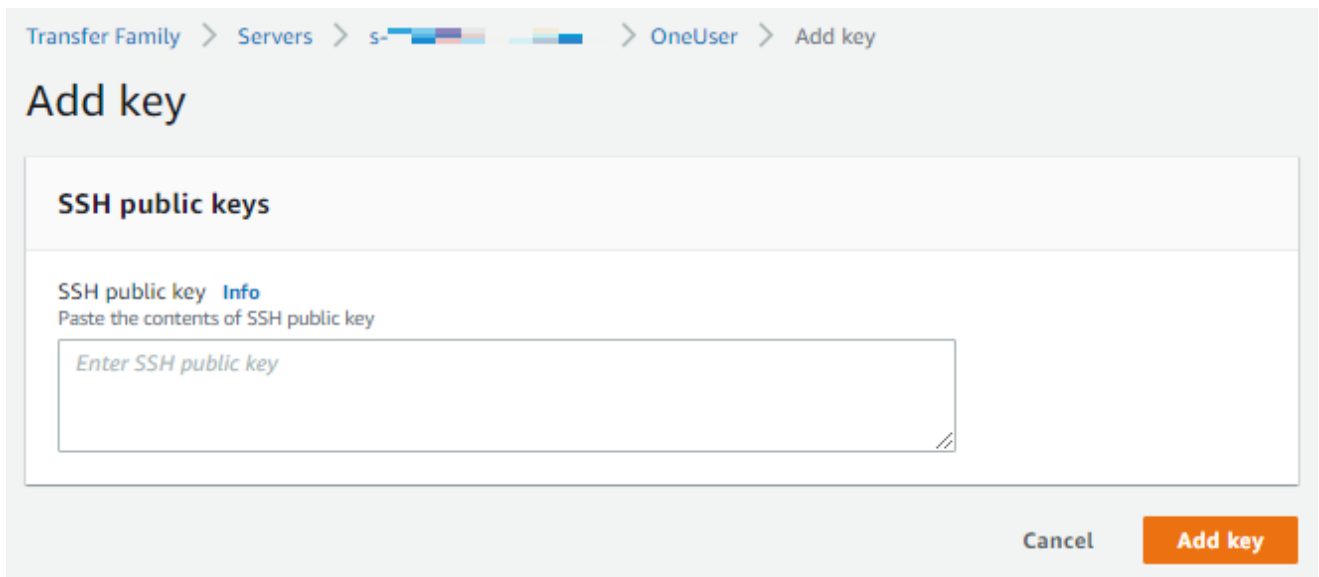
La tua coppia di chiavi SSH è ora pronta per l'uso. Segui i passaggi 3 e 4 per archiviare la chiave pubblica SSH per gli utenti gestiti dal servizio. Questi utenti utilizzano le chiavi quando trasferiscono file sugli endpoint del server Transfer Family.

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.

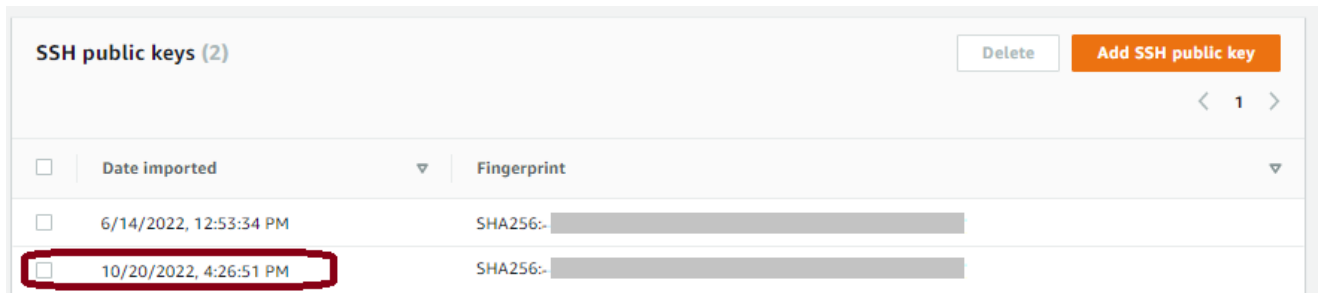
- a. Apri la AWS Transfer Family console all'indirizzo <https://console.aws.amazon.com/transfer/>, quindi seleziona Server dal pannello di navigazione.
- b. Nella pagina Server, seleziona l'ID server per il server che contiene l'utente che desideri aggiornare.
- c. Seleziona l'utente per il quale stai 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.



SSH public keys (2)			Delete	Add SSH public key
			< 1 >	
☐	Date imported	Fingerprint		
☐	6/14/2022, 12:53:34 PM	SHA256:-		
☐	10/20/2022, 4:26:51 PM	SHA256:-		

Creazione di chiavi SSH su Microsoft Windows

Windows include OpenSSH come funzionalità integrata, che puoi usare per generare chiavi SSH nello stesso formato di Linux o macOS. In alternativa, puoi utilizzare strumenti di terze parti come il generatore di chiavi di PuTTY (PuTTYgen).

Utilizzo di OpenSSH integrato in Windows

Le versioni recenti di Windows includono OpenSSH per impostazione predefinita. È possibile utilizzare gli stessi `ssh-keygen` comandi descritti nella macOS/Linux sezione:

1. Apri Windows PowerShell o il prompt dei comandi.
2. Esegui uno dei seguenti comandi in base al tipo di chiave che desideri generare:
 - 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:

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Per generare una coppia di chiavi ED25519:

```
ssh-keygen -t ed25519 -f key_name
```

3. Segui gli stessi passaggi della macOS/Linux sezione per caricare la tua chiave pubblica su AWS Transfer Family

Utilizzo di PuTTYgen (strumento di terze parti)

Alcuni client SSH di terze parti per Windows, come PuTTY, utilizzano formati di chiave diversi. PuTTY utilizza il formato per PPK le chiavi private. Se utilizzi PuTTY o strumenti correlati come WinSCP, puoi usare PuTTYgen per creare chiavi in questo formato.

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, consulta il sito Web. SSH.com](#)

Conversione di una chiave SSH2 in formato chiave pubblica SSH

AWS Transfer Family accetta solo chiavi SSH-formatted pubbliche. Se hai una chiave pubblica SSH2, devi convertirla. Una chiave pubblica SSH2 ha il seguente formato:

```
---- BEGIN SSH2 PUBLIC KEY ----  
Comment: "rsa-key-20160402"  
AAAAB3NzaC1yc2EAAAABJQAAAQEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI  
:  
:  
---- END SSH2 PUBLIC KEY ----
```

Una chiave pubblica SSH ha il seguente formato:

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

Esegui il comando seguente per convertire una chiave SSH2-formatted pubblica in una chiave SSH-formatted pubblica. Sostituiscila `ssh2-key` con il nome della tua chiave SSH2 e `ssh-key` con il nome della tua chiave SSH.

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

Note

Per la rotazione automatica delle chiavi SSH utilizzando l'infrastruttura come codice, vedi. [Moduli Transfer Family Terraform](#)

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. Aprire 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.

or

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` o `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 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* sostituisilo con l'ID del server Transfer Family e sostituisilo *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, sostituisilo *serverID* con l'ID del server Transfer Family, sostituisilo *username* con il tuo nome utente e sostituisilo *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, sostituisilo *serverID* con l'ID del server Transfer Family, sostituisilo *username* con il tuo nome utente e *keyID-from-step-2* sostituisilo 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 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. Per informazioni dettagliate sugli algoritmi delle chiavi PGP, compresi i consigli e la conformità FIPS, vedere. [Algoritmi di key pair 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

L'operatore utilizzato per generare le chiavi PGP dipende dal sistema operativo e dalla versione del software di generazione di 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 per te.

```
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. Se scegli ECC, puoi scegliere tra BrainPool e Curve25519 per la NIST curva ellittica.

Sottocomandi utili **gpg**

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 [Gestione dei segreti AWS](#)

Note

Il tuo nome segreto include l'ID del server Transfer Family. Ciò significa che dovresti aver già identificato o creato un server prima di poter memorizzare le informazioni della chiave PGP.

[Gestione dei segreti AWS](#)

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 segreto `aws/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 è `aws/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 usando, esegui uno dei seguenti comandi per generare una coppia di key pair PGP.
 - Se stai usando la **GnuPG** versione 2.3.0 o successiva, esegui il seguente comando:

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

Puoi scegliere **oRSA**, se lo desideri, puoi scegliere **ECC** uno dei due **BrainPool** o **Curve25519** per la **NIST** curva ellittica. Se `gpg --gen-key` invece esegui, crei una key pair che utilizza l'algoritmo di crittografia ECC Curve 25519.

- Per le versioni **GnuPG** precedenti alla 2.3.0, è possibile utilizzare il comando seguente, 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. Assicuratevi di prendere nota di questi valori. È necessario fornire la passphrase quando si inseriscono i dettagli della chiave in una fase Gestione dei segreti AWS 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.gpg* 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.gpg --armor --export-secret-key marymajor@example.com
```

3. Gestione dei segreti AWS Utilizzatelo per memorizzare la vostra chiave PGP.
 - a. Accedi a Console di gestione AWS e apri la Gestione dei segreti AWS 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 Key/value coppie, scegli la Key/valuescheda.
 - 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 **Key/value** coppie, scegli la **Key/value** scheda.

- **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.

Choose secret type

Secret type [Info](#)

☐ Credentials for Amazon RDS database
 ☐ Credentials for Amazon DocumentDB database
 ☐ Credentials for Amazon Redshift cluster

☐ Credentials for other database
 ☒ Other type of secret
API key, OAuth token, other.

Key/value pairs [Info](#)

Key/value | Plaintext

PGPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----	Remove
PGPPassphrase	mypassphrase	Remove

[+ Add row](#)

Encryption key [Info](#)

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

aws/secretsmanager [Add new key](#)

Note

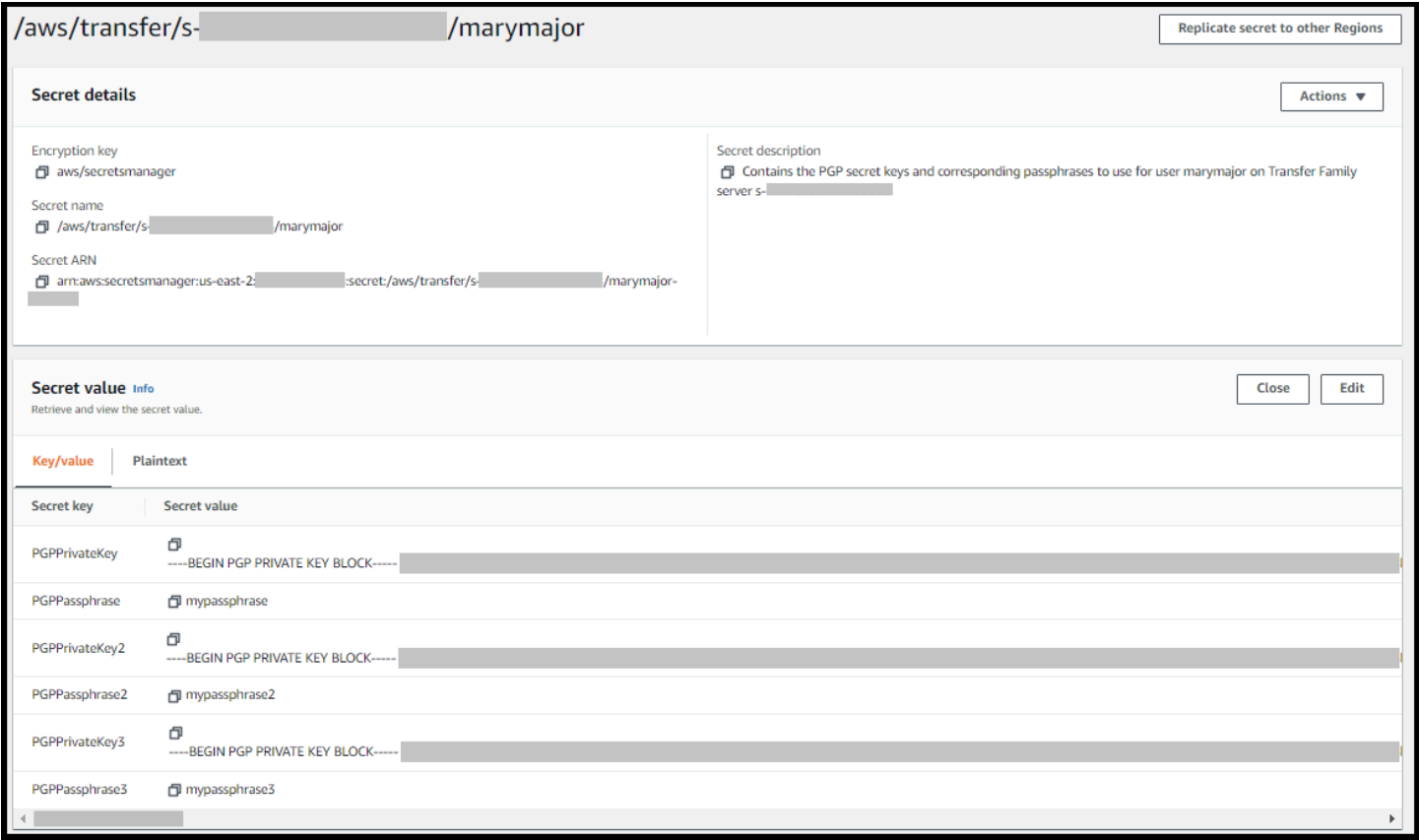
Puoi aggiungere fino a 3 set di chiavi e passphrase. Per aggiungere un secondo set, aggiungi due nuove righe e inserisci **PGPPassphrase2** per le chiavi **PGPrivateKey2** e incolla un'altra chiave privata e passphrase. Per aggiungere un terzo set, i valori chiave devono essere e. **PGPrivateKey3 PGPPassphrase3**

- g. Scegli Next (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**. Sostituisci **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**. Sostituisci **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.



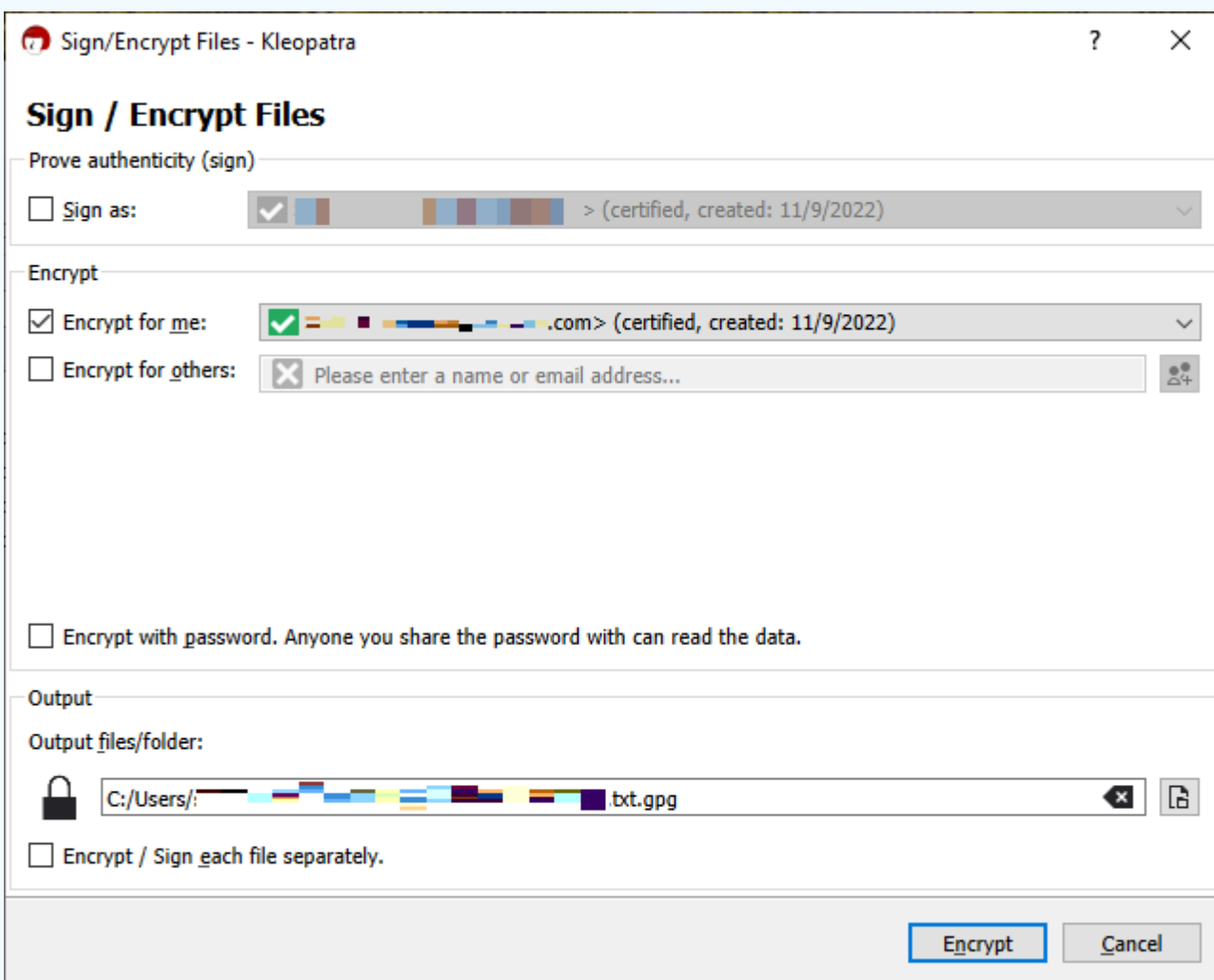
Client PGP supportati

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](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Come AWS Transfer Family funziona con IAM](#)
- [AWS Transfer Family esempi di politiche basate sull'identità](#)
- [AWS Transfer Family esempi di policy basate su tag](#)
- [Risoluzione dei problemi di AWS Transfer Family identità e accesso](#)
- [Chiavi delle condizioni IAM per la governance organizzativa](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi di AWS Transfer Family identità e accesso](#))
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [Come AWS Transfer Family funziona con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (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 autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

Utente root dell'account AWS

Quando si crea una Account AWS, si inizia con un'identità di accesso chiamata utente Account AWS root che ha accesso completo a tutte le risorse. Servizi AWS Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta [Che cos'è il Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un ruolo utente a un ruolo IAM \(console\)](#) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Identity-based politiche

Identity-based le politiche sono documenti di policy sulle autorizzazioni JSON che alleggi a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Identity-based le politiche possono essere politiche in linea (incorporate direttamente in una singola identità) o politiche gestite (politiche autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Resource-based politiche

Resource-based le politiche sono documenti di policy JSON allegati a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

Resource-based le politiche sono politiche in linea che si trovano in quel servizio. Non è possibile 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 entità 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 che possono impostare le autorizzazioni massime concesse da tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): specifica il numero massimo di autorizzazioni per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- Policy di controllo delle risorse (RCP): imposta le autorizzazioni massime disponibili per le risorse degli account. Per ulteriori informazioni, consulta [Policy di controllo delle risorse \(RCP\)](#) nella Guida per l'utente di AWS Organizations .
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno 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

- [AWS Transfer Family politiche basate sull'identità](#)
- [AWS Transfer Family politiche basate sulle risorse](#)
- [Autorizzazione basata su tag AWS Transfer Family](#)
- [AWS Transfer Family Ruoli IAM](#)

AWS Transfer Family politiche basate sull'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 utilizzati in una policy JSON, consulta il [riferimento agli elementi della policy JSON di IAM nella Guida](#) per l'utente AWS Identity and Access Management.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di 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 `transfer:CreateServer` nella

sua politica. Le istruzioni delle policy devono includere un elemento `Action` o `NotAction`. AWS Transfer Family definisce una propria serie di operazioni che descrivono le attività eseguibili 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.

Resources

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si 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. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile 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. 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](#) Per le policy IAM specifiche per gli endpoint VPC, consulta. [Limitazione dell'accesso agli endpoint VPC per i server Transfer Family](#)

AWS Transfer Family politiche basate sulle risorse

Resource-based le politiche sono documenti di policy JSON che specificano quali azioni un determinato principale può eseguire sulla AWS Transfer Family risorsa e in quali condizioni. Amazon S3 supporta politiche di autorizzazione basate sulle risorse per Amazon S3. *buckets* Resource-based le politiche consentono di concedere l'autorizzazione all'utilizzo ad altri account in base alla risorsa. Puoi anche utilizzare una policy basata sulle risorse per consentire a un AWS servizio di accedere al tuo Amazon S3. *buckets*

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'entità 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 denominata *bucket* policy, che è allegata 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, fornire 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, consulta [AWS 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 [AssumeRole](#). [GetFederationToken](#)

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'AWS API Console di gestione AWS AWS CLI, o. 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 AWS Transfer Family](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)

Best practice per le policy

Identity-based le politiche determinano se qualcuno può creare, accedere o eliminare AWS Transfer Family risorse nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account

AWS. Quando si creano o modificano policy basate sull'identità, seguire 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 AWS gestite che concedono le autorizzazioni per molti casi d'uso comuni. 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 maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di 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, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di 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 AWS Transfer Family

Per accedere alla AWS Transfer Family console, è necessario 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, è possibile 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 collegate 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 AWS Transfer Family risorse

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`, `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: consenti 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 `TagResource`, `UntagResource`, `StartServer`, `StopServer`, `DescribeServer`,

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 Console di gestione AWS 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 tenta di utilizzare la console per visualizzare i dettagli relativi a *widget*, ma non dispone delle 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 chiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *my-example-widget* mediante 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 trasmettere 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. Sostituiscilo **123456789012** con l'ID del tuo account AWS e **MyTransferRole** con il nome effettivo del ruolo IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/MyTransferRole",
      "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), utilizzare tali policy per concedere alle persone l'accesso alle proprie risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS Transfer Family supporta queste funzionalità, consulta [Come 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 di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente di IAM.

Chiavi delle condizioni IAM per la governance organizzativa

AWS Transfer Family fornisce chiavi di condizione IAM che consentono di limitare le configurazioni delle risorse in qualsiasi policy IAM. Queste chiavi di condizione possono essere utilizzate nelle policy basate sull'identità collegate a utenti o ruoli o nelle Service Control Policies (SCP) per la governance organizzativa.

Le policy di controllo dei servizi sono policy IAM che si applicano a un'intera AWS organizzazione e forniscono protezioni preventive su più account. Se utilizzate negli SCP, queste chiavi di condizione aiutano a far rispettare i requisiti di sicurezza e conformità a livello di organizzazione.

Consulta anche

- [Azioni, risorse e chiavi di condizione per Transfer Family](#)
- [Policy di controllo dei servizi \(Service Control Policies, SCP\)](#)
- Guarda [questo video](#) che descrive come applicare i guardrail preventivi utilizzando le policy di controllo dei servizi

Chiavi delle condizioni disponibili

AWS Transfer Family supporta le seguenti chiavi di condizione da utilizzare nelle politiche IAM:

`transfer:RequestServerEndpointType`

Limita la creazione e gli aggiornamenti del server in base al tipo di endpoint (PUBLIC, VPC, VPC_ENDPOINT). Utilizzato comunemente per impedire che gli endpoint siano rivolti al pubblico.

`transfer:RequestServerProtocols`

Limita la creazione e gli aggiornamenti dei server in base ai protocolli supportati (SFTP, FTPS, FTP, AS2).

`transfer:RequestServerDomain`

Limita la creazione di server in base al tipo di dominio (S3, EFS).

`transfer:RequestConnectorProtocol`

Limita la creazione di connettori in base al protocollo (AS2, SFTP).

Azioni supportate

Le chiavi delle condizioni possono essere applicate alle seguenti azioni: AWS Transfer Family

- `CreateServer`: Supporti `RequestServerEndpointType` `RequestServerProtocols` e chiavi di `RequestServerDomain` condizione
- `UpdateServer`: Supporti `RequestServerEndpointType` e chiavi di `RequestServerProtocols` condizione
- `CreateConnector`: Supporta la chiave di `RequestConnectorProtocol` condizione

Esempio di politica SCP

L'esempio seguente SCP impedisce la creazione di AWS Transfer Family server pubblici in tutta l'organizzazione:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyPublicTransferServers",
    "Effect": "Deny",
    "Action": ["transfer:CreateServer", "transfer:UpdateServer"],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "transfer:RequestServerEndpointType": "PUBLIC"
      }
    }
  }]
}
```


Convalida della conformità per AWS Transfer Family

Third-party i revisori valutano la sicurezza e la conformità nell' AWS Transfer Family ambito di più programmi di conformità. AWS 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. AWS HIPAA-compliant
- [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 CSPM](#)— 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.

Per tutti gli endpoint Transfer Family:

- La Zone-level ridondanza della disponibilità è integrata nel servizio.
- Esistono flotte ridondanti per ogni AZ.
- Questa ridondanza viene fornita automaticamente.

Note

Per gli endpoint in un Virtual Private Cloud (VPC), è possibile fornire una singola sottorete. Tuttavia, ti consigliamo di creare endpoint in più zone di disponibilità all'interno del tuo VPC, per ridurre il rischio di interruzioni del servizio durante le interruzioni della zona di disponibilità.

Consulta anche

- Per i dettagli su come creare server Transfer Family in un VPC, consulta [Crea un server in un cloud privato virtuale](#)
- Per ulteriori informazioni sulle zone Regioni AWS 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 Latency-based routing, consulta il post sul blog [Minimizza la latenza di rete](#) con i server. AWS Transfer Family

Crea una connessione privata tra un VPC e le API AWS Transfer Family

Puoi stabilire una connessione privata tra il tuo VPC e le AWS Transfer Family API creando un endpoint VPC di interfaccia, alimentato da [AWS PrivateLink](#). Puoi accedere alle AWS Transfer Family API come se fossero nel tuo VPC, senza utilizzare un gateway Internet, un dispositivo NAT,

una connessione VPN o una connessione Direct AWS Connect. Le istanze presenti nel VPC non richiedono indirizzi IP pubblici per comunicare con le API dell' AWS Transfer Family .

In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Per ulteriori informazioni, consulta [Accedere ai AWS servizi AWS PrivateLink nella Guida](#).AWS PrivateLink Prima di configurare un endpoint VPC di interfaccia per le AWS Transfer Family API, consulta le [considerazioni](#) nella Guida.AWS PrivateLink

Controllo dell'accesso tramite le policy degli endpoint VPC

Per impostazione predefinita, l'accesso completo alle AWS Transfer Family API è consentito tramite l'endpoint. È possibile controllare l'accesso all'endpoint dell'interfaccia utilizzando le policy degli endpoint VPC. Puoi allegare una policy per gli endpoint al tuo endpoint VPC che controlla l'accesso alle API. AWS Transfer Family La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire azioni.
- Le azioni che possono essere eseguite.
- Le risorse su cui è possibile eseguire le azioni.

Per ulteriori informazioni, consulta [Controllo degli accessi ai servizi con endpoint VPC](#) in Guida per l'utente di Amazon VPC.

Di seguito è riportato un esempio di policy degli endpoint per le AWS Transfer Family API. Se collegata a un endpoint, questa policy garantisce l'accesso a tutte le azioni delle AWS Transfer Family API su tutte le risorse, ad eccezione di quelle contrassegnate con chiave e valore.

Environment Test

```
{
  "Statement": [{
    "Effect": "Deny",
    "Action": "transfer:StartFileTransfer",
    "Principal": "*",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Environment": "Test"
      }
    }
  }], {
```

```
    "Effect": "Allow",
    "Action": "transfer:*",
    "Principal": "*",
    "Resource": "*"
  }
}
```

Crea un endpoint VPC di interfaccia per le API AWS Transfer Family

Puoi creare un endpoint VPC per le AWS Transfer Family API utilizzando la console Amazon VPC o l'interfaccia a riga di comando (). AWS CLI Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint VPC](#) nella Guida di AWS PrivateLink.

Crea un endpoint VPC per le AWS Transfer Family API utilizzando uno dei seguenti nomi di servizio:

- `com.amazonaws.region.transfer`
- `com.amazonaws.region.transfer-fips`— Creare un endpoint VPC di interfaccia conforme allo standard governativo statunitense Federal Information Processing Standard (FIPS) Publication 140-3.

Se si abilita il DNS privato per l'endpoint, AWS Transfer Family è possibile effettuare richieste API alle API utilizzando il nome DNS predefinito per la regione, ad esempio. `transfer.us-east-1.amazonaws.com`

Sicurezza dell'infrastruttura in AWS Transfer Family

In quanto servizio gestito, AWS Transfer Family è protetto dalla sicurezza della 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 crittografia con Perfect Forward Secrecy (PFS) come DHE (Ephemeral) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Evita di posizionare AWS Transfer Family NLB e NAT davanti ai server

Note

I server configurati con i protocolli FTP e FTPS consentono solo una configurazione con un VPC: non è disponibile alcun endpoint pubblico per. FTP/FTPS

Molti clienti configurano un Network Load Balancer (NLB) per indirizzare il traffico verso il proprio server. AWS Transfer Family In genere lo fanno perché hanno creato il loro server prima che gli fosse AWS offerto un modo per accedervi sia dall'interno del loro VPC che da Internet, o perché supportano l'FTP su Internet. Questa configurazione non solo aumenta i costi per i clienti, ma può anche causare altri problemi, descritti in questa sezione.

I gateway NAT sono un componente obbligatorio quando i client si connettono da una rete privata del cliente dietro un firewall aziendale. Tuttavia, è necessario tenere presente che quando molti client si trovano dietro lo stesso gateway NAT, ciò può influire sulle prestazioni e sui limiti di connessione. Se nel percorso di comunicazione dal client al server FTP o FTPS è presente un NLB o NAT, il server non è in grado di riconoscere con precisione l'indirizzo IP del client, poiché AWS Transfer Family vede solo l'indirizzo IP del NLB o del NAT.

Se utilizzi la configurazione di un server Transfer Family dietro un NLB, ti consigliamo di passare a un endpoint VPC e utilizzare un indirizzo IP elastico invece di utilizzare un NLB. Quando utilizzi i gateway NAT, tieni presente le limitazioni di connessione descritte di seguito.

Se utilizzi il protocollo FTPS, questa configurazione non solo riduce la tua capacità di controllare chi accede al tuo server, ma può anche influire sulle prestazioni. AWS Transfer Family utilizza l'indirizzo IP di origine per condividere le connessioni sul nostro piano dati. Per FTPS, ciò significa che invece di avere 10.000 connessioni simultanee, i server Transfer Family con gateway NLB o NAT sulla via di comunicazione sono limitati a sole 300 connessioni simultanee.

Sebbene consigliamo di evitare i Network Load Balancer davanti ai AWS Transfer Family server, se l'implementazione FTP o FTPS richiede un NLB o NAT nel percorso di comunicazione del client, segui questi consigli:

- Per un NLB, utilizzate la porta 21 per i controlli sanitari, anziché le porte 8192-8200.
- Per il AWS Transfer Family server, abilita la ripresa della sessione TLS impostando.
`TlsSessionResumptionMode = ENFORCED`

 Note

Questa è la modalità consigliata, in quanto offre una maggiore sicurezza:

- Richiede ai client di utilizzare la ripresa della sessione TLS per le connessioni successive.
- Fornisce garanzie di sicurezza più solide garantendo parametri di crittografia coerenti.
- Aiuta a prevenire potenziali attacchi di downgrade.
- Mantiene la conformità agli standard di sicurezza ottimizzando al contempo le prestazioni.

- Se possibile, abbandona l'utilizzo di un NLB per sfruttare appieno i limiti di AWS Transfer Family prestazioni e connessione.

Per ulteriori indicazioni sulle alternative NLB, contatta il team di gestione dei AWS Transfer Family prodotti tramite Support AWS . Per ulteriori informazioni su come migliorare il livello di sicurezza, consulta il post sul blog [Sei suggerimenti per migliorare la sicurezza del](#) tuo server. AWS Transfer Family

Sicurezza dell'infrastruttura di connettività VPC

I connettori SFTP con tipo di uscita VPC offrono una maggiore sicurezza dell'infrastruttura attraverso l'isolamento della rete e la connettività privata:

Vantaggi dell'isolamento della rete

- Traffico di rete privato: tutto il traffico dei connettori verso i server SFTP privati rimane all'interno del tuo VPC, senza mai attraversare la rete Internet pubblica.
- Uscita controllata: per gli endpoint pubblici a cui si accede tramite VPC, il traffico indirizza il traffico attraverso i gateway NAT, offrendoti il controllo sugli indirizzi IP in uscita e sulle politiche di rete.
- Controlli di sicurezza VPC: sfrutta i gruppi di sicurezza VPC, gli ACL di rete e le tabelle di routing esistenti per controllare l'accesso alla rete dei connettori.
- Connettività ibrida: accedi ai server SFTP locali tramite connessioni VPN o Direct Connect consolidate senza ulteriore esposizione a Internet.

Considerazioni sulla sicurezza di Resource Gateway

I Resource Gateway forniscono punti di ingresso sicuri per Cross-VPC l'accesso alle risorse:

- Multi-AZ implementazione: i Resource Gateway richiedono sottoreti in almeno due zone di disponibilità per un'elevata disponibilità e tolleranza agli errori.
- Controlli dei gruppi di sicurezza: configura i gruppi di sicurezza per limitare l'accesso alle porte SFTP (in genere la porta 22) solo da fonti autorizzate.
- Posizionamento di sottoreti private: implementa i Resource Gateway in sottoreti private durante la connessione a server SFTP privati per mantenere l'isolamento della rete.
- Limiti di connessione: ogni Resource Gateway supporta fino a 350 connessioni simultanee con un timeout di inattività di 350 secondi per le connessioni TCP.

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. Apri la console API Gateway 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 delle seguenti 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 su come proteggere Transfer Family con il firewall delle applicazioni AWS web, consulta [Securing Transfer Family with AWS application firewall e Amazon API Gateway](#) nel blog sullo AWS storage.

Cross-service confusa prevenzione sostitutiva

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. Nel AWS, l'impersonificazione intersettoriale può portare al confuso problema del sostituto. Cross-service l'impersonificazione può verificarsi quando un servizio (il servizio chiamante)

chiama un altro servizio (il servizio chiamato). Il servizio chiamante 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, sostituisci ciascuno *user input placeholder* con le tue 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": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012: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": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012: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:us-
east-1:123456789012: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": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-
west-2:111122223333: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:us-
west-2:111122223333:workflow/workflow-id"
        }
      }
    }
  ]
}
```

AWS Transfer Family Connector: ruolo interservizio, prevenzione confusa

La seguente politica di esempio consente a qualsiasi connettore 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": "123456789012"
        }
      }
    }
  ]
}
```

```

        "ArnLike": {
            "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/*"
        }
    }
}
]
}

```

La seguente politica di esempio consente a un connettore 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:us-
east-1:123456789012:connector/connector-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.

La seguente logging/invoke politica di esempio 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": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

La seguente logging/invoke politica di esempio 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": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": [
                "arn:aws:transfer:us-west-2:111122223333:server/server-id",
                "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-id"
            ]
        }
    }
}

```

AWS politiche gestite per AWS Transfer Family

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite piuttosto che scrivere le politiche autonomamente. 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, consultare [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, consultare 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. Per ulteriori informazioni, consulta [Service-linked il ruolo di AWS Transfer Family](#).

AWS politica gestita: `AWSTransferFullAccess`

La `AWSTransferFullAccess` politica fornisce l'accesso completo ai servizi Transfer Family. Per ulteriori informazioni, consulta [Service-linked il ruolo di AWS Transfer Family](#).

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. Per ulteriori informazioni, consulta [Service-linked il ruolo di AWS Transfer Family](#).

AWS politica gestita: `AWSTransferReadOnlyAccess`

La `AWSTransferReadOnlyAccess` politica fornisce l'accesso in sola lettura ai servizi Transfer Family. Per ulteriori informazioni, consulta [Service-linked il ruolo di AWS Transfer Family](#).

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 di 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

Moduli Transfer Family Terraform

[HashiCorpTerraform](#) è un motore Infrastructure as Code (IaC) open source sviluppato utilizzando il HashiCorp Configuration Language (HCL). Terraform fornisce un flusso di lavoro coerente con interfaccia a riga di comando (CLI) che, insieme a Transfer AWS Family per l'infrastruttura di back-end, può gestire centinaia di servizi cloud e codificare le API cloud in file di configurazione dichiarativi.

Puoi utilizzare Terraform per distribuire in sicurezza i server SFTP AWS Transfer Family e i connettori SFTP, insieme alle dipendenze e alle personalizzazioni associate. Per il repository che contiene il codice Terraform per creare le risorse necessarie per eseguire AWS Transfer Family, vedere il codice sorgente del [modulo Terraform Transfer Family](#) su GitHub.

Note

I moduli AWS Transfer Family per Terraform sono uno sforzo supportato dalla comunità. Non fanno parte di un AWS servizio. Best-effort il supporto è fornito dalla community AWS di Storage.

server SFTP

Questa automazione fornisce un modulo Terraform personalizzabile ed esempi end-to-end per creare un endpoint SFTP (PUBLICon tipi di VPC endpoint), integrarsi con Amazon CloudWatch per la registrazione e il monitoraggio, gestire le identità degli utenti per l'accesso agli endpoint e configurare i ruoli IAM per l'accesso ai bucket Amazon S3 in cui sono archiviati i file. Il modulo supporta più chiavi pubbliche SSH per utente (fino a 50 chiavi) per una maggiore sicurezza e funzionalità di rotazione delle chiavi.

Connettori SFTP

AWS Il modulo Transfer Family Terraform ora supporta l'implementazione di connettori SFTP per trasferire file tra Amazon S3 e server SFTP remoti. I connettori SFTP offrono una funzionalità completamente gestita e a basso codice per copiare file tra Amazon S3 e server SFTP remoti.

Ora puoi utilizzare Terraform per effettuare il provisioning programmatico dei connettori SFTP, delle dipendenze e delle personalizzazioni associate in un'unica implementazione. Il modulo fornisce anche esempi completi per automatizzare i flussi di lavoro di trasferimento di file in base a una

pianificazione o a trigger di eventi. L'utilizzo di Terraform per l'implementazione elimina la necessità di configurazioni manuali dispendiose in termini di tempo e soggette a errori e offre un'opzione di implementazione rapida, ripetibile e sicura in grado di scalare.

AS2

Per mostrare il supporto per i modelli AS2 Terraform, aggiungi una reazione con il pollice in su (#) alla richiesta di funzionalità dei modelli [Transfer Family Terraform](#). Puoi anche aggiungere un commento che descriva il tuo caso d'uso.

Scambio di dati B2B

AWS B2B Data Interchange automatizza la trasformazione, la convalida e la generazione di documenti EDI (Electronic Data Interchange) da e verso i formati di dati JSON e XML. [Per mostrare il supporto per i modelli Terraform per B2B Data Interchange, aggiungi una reazione con il pollice rivolto verso l'alto \(#\) alla richiesta di funzionalità.](#) Puoi anche aggiungere un commento che descriva il tuo caso d'uso.

Risoluzione dei problemi AWS Transfer Family

Questo capitolo fornisce informazioni sulla risoluzione dei problemi più comuni che potrebbero verificarsi durante l'utilizzo AWS Transfer Family. Ogni sezione si concentra su un'area specifica di funzionalità per aiutarti a trovare rapidamente soluzioni ai tuoi problemi.

- Per problemi con IAM in Transfer Family, consulta [Risoluzione dei problemi di AWS Transfer Family identità e accesso](#).
- Per problemi con le app web Transfer Family, vedi [Risoluzione dei problemi relativi alle app Web](#).

Argomenti

- [Risolvi i problemi di autenticazione](#)
- [Risolvi i problemi relativi al connettore SFTP](#)
- [Risolvi i problemi di connettività e trasferimento SFTP](#)
- [Risolvi i problemi relativi ai provider di identità personalizzati](#)
- [Risolvi i problemi relativi al flusso di lavoro](#)
- [Risolvi i problemi di EFS](#)
- [Risolvi i problemi di archiviazione e crittografia](#)
- [Risolvi i problemi di monitoraggio e avviso](#)
- [Risolvi i problemi di trasferimento tra regioni](#)
- [Risolvi i problemi di distribuzione di Terraform](#)
- [Risolvi i problemi di integrazione del Web Application Firewall](#)
- [Risolvi i problemi relativi agli utenti gestiti dal servizio](#)
- [Risolvi i problemi relativi a AS2](#)

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](#)

- [I limiti dei gruppi di Active Directory sono stati superati](#)
- [Problemi di autenticazione vari](#)
- [Risolvi i problemi relativi ad Amazon API Gateway](#)
- [Risolvi i problemi relativi al test del tuo provider di identità](#)
- [Bucket Amazon S3 duplicati nell'app Web](#)

Errori di autenticazione— SSH/SFTP

Descrizione

Quando tenti di connetterti al tuo 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, consulta [Troppi 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. 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).

I limiti dei gruppi di Active Directory sono stati superati

Descrizione

Quando si tenta di aggiungere altri gruppi di Active Directory al AWS Transfer Family server, viene visualizzato un errore che indica che è stato raggiunto il numero massimo di gruppi consentito.

Causa

AWS Transfer Family ha un limite predefinito di 100 gruppi Active Directory per server.

Soluzione

Queste sono due soluzioni possibili:

- Consolida i gruppi di Active Directory per ridurre il numero totale necessario.
- Se il tuo caso d'uso richiede più di 100 gruppi, prendi in considerazione l'utilizzo di una soluzione di provider di identità personalizzata, come descritto in [Semplificare l'autenticazione di Active Directory con un provider di identità personalizzato per AWS Transfer Family](#).

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, /amzn-s3-demo-bucket/images è accettabile, ma non lo amzn-s3-demo-bucket/images è. /amzn-s3-demo-bucket/images/

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](#)
- [Connessione chiusa](#)

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 console all' CloudFormation 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. Scegliere Aggiorna. Nella pagina Aggiorna stack, scegli Usa il modello corrente, quindi scegli Avanti.
5. Sostituiscilo UserRoleArn con 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 *stack* pagina di revisione, 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 al test del tuo provider di identità

Descrizione

Se esegui il test del tuo provider di identità utilizzando la console o l'operazione TestIdentityProvider API, il Response campo è vuoto. 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.

Bucket Amazon S3 duplicati nell'app Web

Descrizione

Lo stesso bucket Amazon S3 appare più volte nell'interfaccia dell'app web Transfer Family.

Causa

Ciò si verifica quando un utente appartiene a più gruppi di Active Directory che dispongono di concessioni per lo stesso bucket Amazon S3. L'app Web elenca tutte le sovvenzioni di primo livello associate all'UID o GID dell'utente, incluse le concessioni duplicate alla stessa posizione del bucket.

Soluzione

Per evitare offerte duplicate, consolida le sovvenzioni in modo che ogni utente abbia una sola concessione per sede Amazon S3. Rivedi la configurazione di Amazon S3 Access Grants e rimuovi le concessioni ridondanti per lo stesso bucket in diversi gruppi di Active Directory.

Risolvi i problemi relativi al connettore SFTP

Questa sezione descrive le possibili soluzioni ai problemi con i connettori SFTP.

Argomenti

- [Risolvi i problemi relativi all'aggiunta di chiavi host affidabili per il connettore SFTP](#)
- [La negoziazione chiave fallisce](#)
- [Limitazione del connettore SFTP](#)
- [Ottimizzazione delle prestazioni del connettore SFTP](#)
- [Risolvi i problemi di connettività VPC](#)
- [Problemi vari del connettore SFTP](#)

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...==
```

La negoziazione chiave fallisce

Descrizione

Quando la negoziazione sullo scambio di chiavi fallisce, viene visualizzato un errore. 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

Assicuratevi 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 di sicurezza per AWS Transfer Family i connettori SFTP](#)

Limitazione del connettore SFTP

Descrizione

Quando si utilizzano i connettori SFTP per il trasferimento di file, si verificano errori come:

```
{"type": "ExecutionThrottled", "details": {}, "connectorId": "c-1234567890abcdef0"}
```

Oppure notate che i trasferimenti di file subiscono ritardi o falliscono a intermittenza durante le operazioni ad alto volume.

Causa

I connettori SFTP hanno quote di servizio che limitano il numero di trasferimenti simultanei di file e operazioni API. Quando questi limiti vengono superati, si verifica una limitazione per proteggere il servizio e garantire un utilizzo equo da parte di tutti i clienti.

Soluzione

Per risolvere i problemi relativi al connettore SFTP, provate le seguenti soluzioni:

1. Implementa la logica esponenziale di backoff e riprova nelle tue applicazioni. Ad esempio, create una funzione che ritenti automaticamente le operazioni non riuscite con tempi di attesa crescenti tra un tentativo e l'altro.
2. Implementa la limitazione della velocità nella tua applicazione:
 - Limita il numero di trasferimenti simultanei.
 - Aggiungi ritardi tra batch di trasferimenti.
3. Monitora l'utilizzo rispetto alle quote di servizio:
 - Utilizza le CloudWatch metriche per tenere traccia dell'utilizzo delle API.
 - Imposta allarmi per avvisarti quando ti avvicini ai limiti di quota.
4. Per le opzioni per scalare i connettori SFTP, consulta. [Ridimensionamento dei connettori SFTP](#)
5. Se la limitazione persiste e influisce sulle operazioni aziendali, richiedi un aumento della quota tramite la console Service Quotas.

Ottimizzazione delle prestazioni del connettore SFTP

Descrizione

I trasferimenti tramite connettore SFTP sono più lenti del previsto o si verificano prestazioni incoerenti.

Causa

Le prestazioni del connettore SFTP possono essere influenzate da vari fattori, tra cui le condizioni di rete, le dimensioni dei file, la configurazione del server remoto e i limiti di trasferimento simultaneo.

Soluzione

Per ottimizzare le prestazioni del connettore SFTP:

- Configura il tuo server SFTP remoto per prestazioni ottimali:
 - Aumenta il numero massimo di sessioni e trasferimenti per sessione
 - Ottimizza le dimensioni delle finestre TCP per connessioni ad alta latenza
 - Usa la compressione se supportata da entrambe le estremità
- Prendi in considerazione l'ottimizzazione della rete, posizionando il connettore Transfer Family in una regione vicina al server SFTP remoto.
- Implementa una strategia di monitoraggio per identificare gli ostacoli alle prestazioni:
 - Monitora la velocità di trasmissione e la latenza della rete
 - Analizza i log alla ricerca di schemi nei trasferimenti lenti

Risolvi i problemi di connettività VPC

Questa sezione descrive le soluzioni ai problemi più comuni con i connettori LATTICE-enabled VPC_SFTP.

Connettore bloccato nello stato IN SOSPESO

Descrizione

Il connettore VPC_ LATTICE-enabled SFTP rimane attivo per un periodo prolungato (più di 10 minuti). PENDING

Causa

Ciò può verificarsi a causa di ritardi nella risoluzione DNS, problemi di configurazione di Resource Gateway o problemi di associazione alla rete di servizi VPC Lattice.

Soluzione

[Contatta Contact Supporto AWS](#) per aiutarti ad analizzare la causa principale del problema.

Puoi anche provare la seguente soluzione alternativa.

1. Verifica che il tuo Resource Gateway sia in ACTIVE stato:

```
aws vpc-lattice get-resource-gateway --resource-gateway-  
identifier rgw-1234567890abcdef0
```

2. Verifica che la tua configurazione delle risorse sia correttamente configurata e attiva:

```
aws vpc-lattice get-resource-configuration --resource-configuration-  
identifier rcfg-1234567890abcdef0
```

3. Assicurati che il tuo Resource Gateway disponga di sottoreti in almeno due zone di disponibilità che supportano VPC Lattice.
4. Se il problema persiste, elimina e ricrea il connettore con la stessa configurazione.

Connettore in stato ERRATO

Descrizione

Il connettore VPC_ LATTICE-enabled SFTP mostra ERRORRED lo stato con i dettagli dell'errore.

Causa

Le cause più comuni includono un ARN di configurazione delle risorse non valido, indirizzi IP insufficienti nelle sottoreti VPC o tentativi di condivisione delle risorse tra regioni.

Soluzione

1. Controlla i dettagli dell'errore utilizzando: `describe-connector`

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

2. Verifica che l'ARN della configurazione delle risorse sia corretto e nella stessa regione del connettore.
3. Assicurati che le sottoreti VPC abbiano un numero sufficiente di indirizzi IP disponibili per il Resource Gateway.
4. Verifica che il tuo obiettivo di configurazione delle risorse (indirizzo IP o nome DNS) sia raggiungibile dal tuo VPC.

Errore relativo all'indirizzo IP pubblico non supportato

Descrizione

Viene visualizzato un errore quando si tenta di creare una configurazione delle risorse con un indirizzo IP pubblico: `ValidationException: IP address x.x.x.x is not in allowed ranges.`

Causa

Le configurazioni delle risorse per gli endpoint pubblici devono utilizzare nomi DNS, non indirizzi IP.

Soluzione

Usa il nome DNS pubblico del tuo server SFTP anziché il suo indirizzo IP durante la creazione della configurazione delle risorse:

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="my.sftp.server.com"} \  
  --port-ranges 22
```

Errore relativo alla zona di disponibilità non supportata

Descrizione

Viene visualizzato un errore durante la creazione di un Resource Gateway: Subnet subnet-xxx is not valid because it is not in a supported Availability Zone.

Causa

Non tutte le zone di disponibilità supportano VPC Lattice Cross-VPC Resource Access. Il messaggio di errore elenca le AZ supportate per la tua regione.

Soluzione

1. Crea sottoreti nelle zone di disponibilità supportate elencate nel messaggio di errore.
2. Aggiorna Resource Gateway per utilizzare solo le sottoreti delle AZ supportate.
3. Assicurati di avere almeno due sottoreti in diverse AZ supportate.

Timeout di connessione con connettori VPC_LATTICE

Descrizione

I trasferimenti di file tramite connettori VPC scadono o falliscono a intermittenza.

Causa

VPC Lattice ha limiti di connessione (350 connessioni per risorsa) e timeout di inattività (350 secondi per TCP).

Soluzione

1. Monitora le connessioni simultanee per rimanere entro il limite di 350 connessioni per risorsa.
2. Implementa il pooling e il riutilizzo delle connessioni nelle tue applicazioni.
3. Configura i valori di timeout appropriati nelle applicazioni client SFTP (meno di 350 secondi).
4. Valuta la possibilità di creare più configurazioni di risorse per lo stesso obiettivo per distribuire il carico.

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

- Verifica il tuo connettore: Vedi. [Prova 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: Vedi [Esempi 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 di connettività e trasferimento SFTP

Questa sezione descrive le possibili soluzioni per i problemi di connettività SFTP e trasferimento di file.

Argomenti

- [Risolvi i problemi di connettività SFTP](#)
- [Risolveti i problemi relativi al client SFTP](#)
- [Risolvi i problemi di caricamento dei file](#)
- [Risolvi i problemi relativi al connettore SFTP di tipo di uscita VPC](#)

Risolvi i problemi di connettività SFTP

Descrizione

Il client SFTP non è in grado di avviare la connessione. Questo problema può verificarsi in modo continuo o intermittente. Ad esempio, potreste vedere la seguente sequenza di eventi nei log di debug del client SFTP:

```
sftp -vvv username@1.1.1.1
.....
debug1: Local version string .....
kex_exchange_identification: read: Connection reset by peer
Connection reset by 1.1.1.1 port 22
Connection closed.
```

Causa

Esiste un caso limite in cui l'ACK TCP a zero byte (ACK senza dati), noto anche come handshake a tre vie, viene interrotto o ritardato.

Soluzione

Come soluzione alternativa, Transfer Family offre una soluzione che utilizza una configurazione diversa per risolvere questo problema, ma può causare problemi di compatibilità con i client più vecchi. Per questo motivo, questa soluzione è disponibile solo sulla porta 2223.

Nella procedura per creare un server Transfer Family in un VPC ([Crea un server in un cloud privato virtuale](#)), quando specificate un gruppo di sicurezza, configurate il traffico SSH per utilizzare la porta 2223.

Risolveti i problemi relativi al client SFTP

I messaggi SFTP lato client sono descritti in [Messaggi SFTP](#). Il modo migliore per risolvere i problemi relativi ai client SFTP consiste nel controllare i log del client SFTP e, se necessario, contattare l'amministratore di rete.

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

Risolvi i problemi relativi al connettore SFTP di tipo di uscita VPC

Se riscontri problemi con i connettori SFTP di tipo VPC in uscita, controlla quanto segue:

Lo stato del connettore è IN SOSPESO

Descrizione

Il connettore di tipo di uscita VPC rimane nello stato IN SOSPESO per diversi minuti dopo la creazione e TestConnection restituisce «Connettore non disponibile».

Causa

Il completamento della risoluzione DNS per i connettori VPC può richiedere diversi minuti dopo la creazione.

Soluzione

Attendi che lo stato del connettore diventi ATTIVO prima di tentare il trasferimento di file. Questo è un comportamento normale per i connettori di tipo VPC in uscita.

Timeout di connessione.

Descrizione

Il connettore di tipo di uscita VPC scade quando si tenta di connettersi al server SFTP.

Causa

I gruppi di sicurezza potrebbero non consentire il traffico sulla porta 22 tra le sottoreti Resource Gateway e il server SFTP di destinazione.

Soluzione

Verificate che i gruppi di sicurezza consentano il traffico sulla porta 22 tra le sottoreti Resource Gateway e il server SFTP di destinazione.

Errori di configurazione delle risorse

Descrizione

Il connettore di tipo di uscita VPC non riesce a connettersi a causa di problemi di configurazione delle risorse.

Causa

La configurazione delle risorse potrebbe indicare un indirizzo IP o un nome DNS errati oppure il Resource Gateway potrebbe non trovarsi nello stesso VPC del server SFTP (per endpoint privati).

Soluzione

Assicurati che la configurazione delle risorse punti all'indirizzo IP o al nome DNS corretti e che il Resource Gateway si trovi nello stesso VPC del server SFTP (per endpoint privati). Per ulteriori informazioni, consulta [Configurazione delle risorse](#) nella Guida per l'utente di Amazon VPC Lattice.

Problemi relativi agli endpoint pubblici

Descrizione

Il connettore di tipo di uscita VPC non può connettersi agli endpoint SFTP pubblici.

Causa

Per gli endpoint pubblici, è necessario utilizzare un nome DNS (non un indirizzo IP) nella configurazione delle risorse e il VPC deve disporre di un gateway NAT per l'accesso a Internet in uscita.

Soluzione

Assicurati di utilizzare un nome DNS, non un indirizzo IP, nella configurazione delle risorse. Verifica che il tuo VPC disponga di un gateway NAT per l'accesso a Internet in uscita.

Problemi relativi alla zona di disponibilità

Descrizione

Non è possibile creare un Resource Gateway a causa delle limitazioni della zona di disponibilità.

Causa

I Resource Gateway richiedono sottoreti in almeno 2 zone di disponibilità e non tutte le AZ supportano VPC Lattice.

Soluzione

Verifica le zone di disponibilità supportate per VPC Lattice nella tua regione e assicurati di avere sottoreti in almeno 2 AZ supportate.

Risolvi i problemi relativi ai provider di identità personalizzati

Questa sezione descrive le possibili soluzioni per i problemi relativi ai provider di identità personalizzati con Transfer Family.

Argomenti

- [Risolvi gli errori di integrazione dell'API Gateway](#)
- [Risoluzione dei problemi relativi ai timeout delle funzioni Lambda](#)
- [Risolvi i problemi di timeout Lambda coerenti](#)
- [Risolvi i problemi relativi alle eccezioni KeyError](#)

Risolvi gli errori di integrazione dell'API Gateway

Descrizione

Gli utenti non possono autenticarsi con il server Transfer Family e, durante il test del provider di identità, vengono visualizzati errori come:

```
{
  "Response": "",
  "StatusCode": 500,
  "Message": "Internal server error"
}
```

Causa

Gli errori di integrazione dell'API Gateway possono verificarsi a causa di:

- Configurazione API Gateway errata
- Gli errori della funzione Lambda non vengono gestiti correttamente
- Problemi di autorizzazione tra API Gateway e Lambda
- Risposte malformate dalla funzione Lambda

Soluzione

Per risolvere gli errori di integrazione dell'API Gateway:

1. Controlla i registri delle funzioni Lambda per informazioni dettagliate sugli errori:

- Nella CloudWatch console, vai a Log groups > //your-function-name aws/lambda
- Cerca i messaggi di errore o le tracce dello stack che indicano la causa principale

2. Verifica che la funzione Lambda restituisca risposte formattate correttamente:

```
{
  "Role": "arn:aws:iam::123456789012:role/TransferUserRole",
  "HomeDirectory": "/mybucket/home/username"
}
```

3. Abilita la CloudWatch registrazione dettagliata per API Gateway:

- Nella console API Gateway, seleziona la tua API e scegli Stages
- Seleziona il tuo stage e Logs/Tracing, in basso, abilita CloudWatch Logs
- Imposta il livello di registro su ERROR o INFO

4. Testa direttamente il tuo endpoint API Gateway:

```
curl -X POST https://your-api-id.execute-api.region.amazonaws.com/prod/servers/your-
server-id/users/username/config \
  -H "Content-Type: application/json" \
  -d '{"Password": "password"}'
```

5. Verifica le autorizzazioni tra API Gateway e Lambda:

- Assicurati che API Gateway sia autorizzato a richiamare la tua funzione Lambda
- Verifica che il ruolo di esecuzione per la tua funzione Lambda disponga delle autorizzazioni necessarie

Risoluzione dei problemi relativi ai timeout delle funzioni Lambda

Descrizione

Quando gli utenti tentano di autenticarsi con il server Transfer Family utilizzando un provider di identità personalizzato, subiscono lunghi ritardi seguiti da errori di autenticazione. Nei log Lambda, vengono visualizzati gli errori di timeout.

Causa

Le funzioni Lambda utilizzate per i provider di identità personalizzati hanno un timeout predefinito di 3 secondi. Se la logica di autenticazione impiega più tempo di questo timeout (ad esempio, quando si interrogano database esterni o si effettuano chiamate API a provider di identità di terze parti), la funzione scadrà e l'autenticazione avrà esito negativo.

Soluzione

Per risolvere i problemi di timeout Lambda:

1. Aumenta il timeout della funzione Lambda:

- Nella console Lambda, accedi alla tua funzione e seleziona la scheda Configurazione
- In Configurazione generale, fai clic su Modifica
- Aumenta il valore di timeout (si consigliano fino a 15 secondi per le funzioni di autenticazione)

2. Ottimizza il codice della funzione Lambda:

- Usa il pool di connessioni per le query del database
- Implementa la memorizzazione nella cache per i dati ad accesso frequente
- Riduci al minimo le chiamate API esterne durante l'autenticazione

3. Prendi in considerazione l'utilizzo di Lambda Provisioned Concurrency per eliminare gli avviamenti a freddo:

```
aws lambda put-provisioned-concurrency-config \
  --function-name my-authentication-function \
  --qualifier prod \
  --provisioned-concurrent-executions 5
```

4. Monitora le prestazioni Lambda utilizzando le CloudWatch metriche e configura allarmi per le soglie di durata

Risolvi i problemi di timeout Lambda coerenti

Descrizione

Gli utenti riscontrano timeout costanti quando utilizzano una funzione Lambda per l'autenticazione.

Causa

Lambda non riesce a raggiungere il AWS servizio corrispondente utilizzato per l'autenticazione (come DynamoDB, Secrets Manager o un altro provider di identità).

Soluzione

Verifica che le sottoreti possano raggiungere i servizi. AWS Oppure, se ti connetti a un provider di identità Internet (come Okta), verifica che la sottorete della funzione Lambda possa raggiungere Internet tramite un gateway NAT

Risolvi i problemi relativi alle eccezioni **KeyError**

Descrizione

Nelle voci del registro Transfer Family, si notano delle eccezioni KeyError «».

Causa

La causa più probabile è che l'utente o il `identity_provider` record non siano corretti o che manchino i campi obbligatori.

Soluzione

Esamina il ERRORS registro, che si trova nel gruppo di `/aws/transfer/your-server-id` log, per trovare indizi.

Risolvi i problemi relativi al flusso di lavoro

Questa sezione descrive le possibili soluzioni ai problemi relativi ai flussi di lavoro gestiti.

Argomenti

- [Risolvi i problemi relativi ai flussi di lavoro gestiti](#)
- [Risolvi i problemi di decrittografia del flusso di lavoro](#)

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](#)
- [Risolvi gli errori di copia del flusso di lavoro](#)

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 i dettagli, consulta [Real-time l'elaborazione dei dati di log con abbonamenti](#) e la [sintassi Filter and 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. Supporto AWS**](#)

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.

Risolvi 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 i problemi di crittografia dei destinatari anonimi](#)
- [Risolvi l'errore relativo al file di crittografia firmato](#)
- [Risolveti l'errore relativo a un algoritmo FIPS](#)

Risolvi i problemi di crittografia dei destinatari anonimi

Descrizione

Il flusso di lavoro di decrittografia non riesce durante l'elaborazione di determinati file crittografati, ma funziona con altri.

Causa

È possibile che i file siano stati crittografati senza specificare un destinatario (crittografia anonima), rendendo difficile per il flusso di lavoro determinare quale chiave utilizzare per la decrittografia.

Soluzione

Crittografa sempre i file con un destinatario non anonimo utilizzando il parametro. -r Esempio:

```
gpg -e -r user@example.com --openpgp file.txt
```

Per verificare se un file è stato crittografato con un destinatario specifico o in forma anonima, usa il comando: `--list-packets`

```
gpg --list-packets file.txt.gpg
```

Questo comando visualizza la struttura dei pacchetti del GPG-encrypted file senza decriptarne il contenuto. Cerca un output che includa informazioni sul destinatario, ad esempio:

```
:pubkey enc packet: version 3, algo 1, keyid 1A2B3C4D5E6F7G8H
```

Se vedi informazioni sull'ID della chiave, il file è stato crittografato per un destinatario specifico. Se mancano queste informazioni, il file potrebbe essere stato crittografato in forma anonima, il che può causare errori di decrittografia nei flussi di lavoro di Transfer Family.

Puoi anche usare questo comando per verificare:

- Quali algoritmi di crittografia sono stati utilizzati
- Metodi di compressione (se presenti)
- Timestamp di creazione

Per visualizzare l'elenco degli algoritmi di cifratura supportati per l'installazione di GPG, usa:

```
gpg --version
```

Queste informazioni possono aiutarti a garantire l'utilizzo di algoritmi di crittografia compatibili con i flussi di lavoro Transfer Family, specialmente quando è richiesta la conformità FIPS.

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 EFS

Questa sezione descrive le possibili soluzioni ai problemi con lo storage Amazon EFS.

Argomenti

- [Risolvi i problemi di Amazon EFS](#)

Risolvi i problemi di Amazon EFS

Questa sezione descrive le possibili soluzioni per i seguenti problemi di Amazon EFS.

Argomenti

- [Risoluzione dei problemi relativi agli utenti gestiti dal servizio Amazon EFS](#)
- [Risolvi i problemi relativi al profilo POSIX mancante](#)

- [Risoluzione dei problemi relativi alle directory logiche con Amazon EFS](#)

Risoluzione dei 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 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 Gestione dei segreti AWS, 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 di archiviazione e crittografia

Questa sezione descrive le possibili soluzioni ai problemi di archiviazione e crittografia.

Argomenti

- [Risolvi i problemi relativi alle politiche per i bucket Amazon S3 crittografati](#)
- [Risolvi i problemi relativi all'eccezione ResourceNotFound](#)

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 [Protezione e crittografia dei dati](#).

Risolvi i problemi relativi all'eccezione **ResourceNotFound**

Descrizione

Viene visualizzato un errore in cui la risorsa non può essere trovata. Ad esempio, se `corriUpdateServer`, 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 `ResourceNotFoundException` messaggio. 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 di monitoraggio e avviso

Questa sezione fornisce informazioni sulla risoluzione dei problemi di monitoraggio e avviso AWS Transfer Family, tra cui CloudWatch metriche mancanti o incomplete ed eventi mancanti. EventBridge

Argomenti

- [Risolvi i problemi relativi alle metriche mancanti o incomplete CloudWatch](#)
- [Risolvi i problemi relativi agli eventi mancanti EventBridge](#)

Risolvi i problemi relativi alle metriche mancanti o incomplete CloudWatch

Descrizione

CloudWatch le metriche per i server Transfer Family sono mancanti, incomplete o non si aggiornano come previsto.

Causa

Le metriche mancanti o incomplete possono essere causate da diversi fattori:

- Problemi di configurazione della registrazione
- Bassi livelli di attività che non generano metriche entro il periodo di tempo previsto
- Visualizzazione di metriche con dimensioni o intervalli di tempo errati

Soluzione

Per risolvere i problemi relativi a CloudWatch metriche mancanti o incomplete:

1. Assicurati che la registrazione sia configurata correttamente per il tuo server Transfer Family:
 - Nella console Transfer Family, verifica che la registrazione sia abilitata in Dettagli del server > Dettagli aggiuntivi > Ruolo di registrazione.
 - Molto che il ruolo di registrazione abbia le autorizzazioni e le relazioni di fiducia necessarie.
2. Durante la visualizzazione delle metriche nella console: CloudWatch
 - Utilizza le dimensioni corrette, ad esempio ServerIdper le metriche a livello di server
 - Modifica l'intervallo di tempo per assicurarti che copra i periodi di attività
 - Verifica di essere nella posizione corretta Regione AWS
3. Genera attività di test sul tuo server Transfer Family per garantire che le metriche vengano prodotte.

Risolvi i problemi relativi agli eventi mancanti EventBridge

Descrizione

Hai configurato EventBridge le regole di Amazon per acquisire gli eventi Transfer Family, ma gli eventi non vengono consegnati alle destinazioni target né attivano le azioni previste.

Causa

EventBridge Gli eventi mancanti possono essere causati da:

- Schemi di eventi configurati in modo errato
- Problemi di autorizzazione con gli obiettivi degli eventi
- Limiti o limitazione del servizio
- Eventi non generati a causa della configurazione del server

Soluzione

Per risolvere gli eventi mancanti EventBridge :

1. Verifica che lo schema degli eventi sia formattato correttamente per corrispondere agli eventi Transfer Family:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["Transfer State Change"],
  "detail": {
    "serverId": ["s-1234567890abcdef0"]
  }
}
```

2. Verifica che il target del tuo evento disponga delle autorizzazioni necessarie:

- Per gli obiettivi Lambda, assicurati che la politica delle risorse della funzione Lambda consenta di richiamarla EventBridge
- Per le destinazioni SQS, verifica che la politica di coda consenta l'invio di messaggi EventBridge
- Per le destinazioni SNS, conferma l'argomento «La policy consente EventBridge di pubblicare su di esso»

3. Verifica la tua regola generando eventi di esempio:

- Usa la EventBridge console per creare un evento di test che corrisponda al tuo schema
- Esegui azioni sul tuo server Transfer Family che dovrebbero generare eventi

4. Abilita le metriche delle EventBridge regole per monitorare le chiamate e gli errori delle regole:

```
aws events put-rule --name "TransferStateChangeRule" --event-pattern '{...}' --state
ENABLED --metrics-enabled
```

5. Controlla CloudWatch i log per eventuali messaggi di errore relativi agli errori di consegna degli eventi

Risolvi i problemi di trasferimento tra regioni

Questa sezione descrive le possibili soluzioni per i problemi relativi al trasferimento di file. Regioni AWS

Argomenti

- [Risolvi i problemi relativi alle autorizzazioni di trasferimento tra regioni](#)
- [Risolvi i problemi relativi alle prestazioni dei trasferimenti tra regioni](#)

Risolvi i problemi relativi alle autorizzazioni di trasferimento tra regioni

Descrizione

Quando si tenta di trasferire file tra bucket Amazon S3 in diverse regioni utilizzando i flussi di lavoro Transfer Family, si verificano errori come:

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "Access Denied (Service: Amazon S3; Status Code: 403; Error Code: AccessDenied)",
    "stepType": "COPY",
    "stepName": "cross_region_copy"
  }
}
```

Causa

Cross-region i trasferimenti richiedono autorizzazioni IAM specifiche sia per i bucket di origine che per quelli di destinazione. Il ruolo IAM utilizzato dal server o dal flusso di lavoro Transfer Family potrebbe non disporre di autorizzazioni sufficienti per accedere ai bucket in altre regioni.

Soluzione

Per risolvere i problemi relativi alle autorizzazioni di trasferimento tra regioni:

1. Assicurati che il tuo ruolo IAM disponga delle autorizzazioni sia per i bucket di origine che per quelli di destinazione:

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

```

        "s3:GetObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::source-bucket-name/*"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:::destination-bucket-name/*"
}
]
}

```

2. Se utilizzi la crittografia KMS, aggiungi le autorizzazioni per le chiavi KMS di origine e di destinazione:

```

{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [
        "arn:aws:kms:source-region:account-id:key/source-key-id",
        "arn:aws:kms:destination-region:account-id:key/destination-key-id"
    ]
}

```

3. Verifica che le policy bucket in entrambe le regioni consentano l'accesso dal ruolo IAM del tuo server Transfer Family
4. Per i trasferimenti tra account, assicurati che siano configurate le autorizzazioni appropriate su più account

Risolvi i problemi relativi alle prestazioni dei trasferimenti tra regioni

Descrizione

Cross-region i trasferimenti sono notevolmente più lenti del previsto o scadono durante i trasferimenti di file di grandi dimensioni.

Causa

Cross-region i trasferimenti implicano intrinsecamente una maggiore latenza e possono essere influenzati dalle condizioni di rete, dalle dimensioni dei file e dai limiti del servizio. File di grandi dimensioni o volumi elevati di file di piccole dimensioni possono comportare un peggioramento delle prestazioni.

Soluzione

Per migliorare le prestazioni di trasferimento tra regioni:

- Per file di grandi dimensioni, prendi in considerazione l'utilizzo di Amazon S3 Transfer Acceleration:

```
aws s3 cp --source-region us-east-1 --region us-west-2 \  
s3://source-bucket/large-file.zip s3://destination-bucket/large-file.zip \  
--acl bucket-owner-full-control --s3-accelerate
```

- Per più file di piccole dimensioni, raggruppalì insieme prima del trasferimento:
 - Usa la compressione per combinare più file
 - Usa le operazioni in batch di Amazon S3 per trasferimenti su larga scala
- Prendi in considerazione l'utilizzo di connettori SFTP Transfer Family con impostazioni di timeout appropriate per trasferimenti di grandi dimensioni
- Per i trasferimenti ricorrenti, prendi in considerazione la possibilità di replicare i dati utilizzando Amazon S3 Cross-Region Replication (CRR) anziché trasferimenti ad hoc
- Monitora le prestazioni di trasferimento utilizzando i CloudWatch parametri di Amazon per identificare i colli di bottiglia

Risolvi i problemi di distribuzione di Terraform

Questa sezione descrive le possibili soluzioni per i problemi relativi alla distribuzione delle risorse Transfer Family utilizzando Terraform. Per informazioni generali sui moduli Terraform per Transfer Family, vedere [Moduli Transfer Family Terraform](#).

Argomenti

- [Risolvi gli errori di creazione delle risorse Terraform](#)
- [Risolvi i problemi di gestione dello stato di Terraform](#)

Risolvi gli errori di creazione delle risorse Terraform

Descrizione

Quando si tenta di creare risorse Transfer Family utilizzando Terraform, si verificano errori come:

```
Error: error creating Transfer Server: InvalidRequestException: The request is not valid.  
Error: error creating Transfer User: InvalidRequestException: Unable to create the user because the server endpoint type is incompatible with the home directory type.
```

Causa

Questi errori si verificano in genere a causa di parametri di configurazione incompatibili o dipendenze mancanti nella configurazione di Terraform. Le cause più comuni includono:

- Tipi di endpoint e configurazioni di storage incompatibili
- Ruoli o policy IAM richiesti mancanti
- Specifiche errate delle politiche di sicurezza
- Problemi di configurazione degli endpoint VPC

Soluzione

Per risolvere i problemi di implementazione di Terraform:

- Assicurati che la tua configurazione Terraform utilizzi combinazioni di parametri compatibili:
 - Per gli endpoint pubblici, assicurati di utilizzare Amazon S3 per lo storage.
 - Per gli endpoint VPC, verifica la corretta configurazione del VPC e del gruppo di sicurezza.
- Utilizza dipendenze esplicite con l'attributo `depends_on` per garantire che le risorse vengano create nell'ordine corretto.
- Verifica che tutti i ruoli IAM abbiano le relazioni di fiducia e le autorizzazioni necessarie.
- Utilizza l'ultima versione del AWS provider per Terraform per garantire la compatibilità con tutte le funzionalità di Transfer Family.
- Per implementazioni complesse e casi d'uso semplici, prendi in considerazione l'utilizzo dei moduli Transfer Family Terraform ufficiali disponibili all'indirizzo. GitHub <https://github.com/aws-ia/terraform-aws-transfer-family> Questi moduli forniscono esempi completi che coprono casi d'uso semplici e complessi per i clienti, seguono le AWS migliori pratiche e possono semplificare

l'implementazione per i clienti che necessitano di assistenza con la configurazione dell'infrastruttura come codice (IaC).

Risolvi i problemi di gestione dello stato di Terraform

Descrizione

Dopo aver apportato modifiche alle risorse Transfer Family al di fuori di Terraform (tramite console o AWS CLI), si verificano variazioni di stato o errori durante l'esecuzione `terraform plan` o `terraform apply`.

Causa

Terraform mantiene un file di stato che tiene traccia delle risorse che gestisce. Quando vengono apportate modifiche al di fuori di Terraform, il file di stato non è sincronizzato con le risorse effettive, causando errori o comportamenti imprevisti durante le successive operazioni di Terraform.

Soluzione

Per risolvere i problemi di gestione dello stato di Terraform con le risorse Transfer Family:

1. Utilizzalo `terraform import` per portare le risorse esistenti sotto la gestione di Terraform:

```
terraform import <transfer_family_server.example> s-<server-id>  
terraform import <transfer_family_server.example> s-<server-id>/username
```

2. Utilizzare `terraform refresh` per aggiornare il file di stato con l'attuale infrastruttura del mondo reale
3. Per le risorse che non possono essere importate o che presentano problemi di stato complessi, prendi in considerazione l'idea `terraform state rm` di rimuoverle dal file di stato, quindi ricreale con Terraform
4. Implementa una politica per gestire le risorse di Transfer Family esclusivamente tramite Terraform per prevenire future derive statali
5. Utilizza l'archiviazione a stato remoto con blocco per evitare modifiche simultanee quando lavori in team

Risolvi i problemi di integrazione del Web Application Firewall

Questa sezione descrive le possibili soluzioni per i problemi relativi all'integrazione AWS WAF con Transfer Family.

Argomenti

- [Risolvi i problemi del blocco del traffico legittimo da parte di WAF](#)
- [Risolvi i problemi di integrazione WAF con provider di identità personalizzati](#)

Risolvi i problemi del blocco del traffico legittimo da parte di WAF

Descrizione

Dopo la configurazione AWS WAF con l'endpoint Transfer Family, gli utenti legittimi non sono in grado di connettersi o riscontrano errori di connessione intermittenti. Potresti vedere le risposte HTTP 403 (Forbidden) nei tuoi log.

Causa

AWS WAF Le tue regole potrebbero essere troppo restrittive o configurate in modo errato, causando falsi positivi che bloccano il traffico legittimo. Le cause più comuni includono:

- IP-based regole che bloccano inavvertitamente le reti aziendali o le VPN
- Rate-based regole con soglie troppo basse per i normali schemi di traffico
- Gruppi di regole gestiti eccessivamente aggressivi per il tuo caso d'uso

Soluzione

Per risolvere i problemi relativi ai falsi positivi:

1. Abilita AWS WAF la registrazione per identificare quali regole attivano i blocchi. Per istruzioni, consulta [Registrazione del traffico ACL AWS WAF web](#).
2. Esamina i log per identificare gli schemi nelle richieste bloccate.
3. Modifica le tue regole in questo modo:
 - Aggiungere indirizzi IP o intervalli a una lista consentita
 - Aumento dei limiti di velocità per le regole basate sulle tariffe

- Impostazione di regole specifiche sulla modalità Count anziché sulla modalità Block per monitorare senza bloccare
 - Creazione di eccezioni per regole specifiche utilizzando le esclusioni dei gruppi di regole
4. Verifica la configurazione aggiornata con un campione rappresentativo di traffico legittimo prima della distribuzione completa.

Risolvi i problemi di integrazione WAF con provider di identità personalizzati

Descrizione

Dopo la configurazione AWS WAF con il server Transfer Family che utilizza un provider di identità personalizzato, l'autenticazione fallisce o gli utenti riscontrano problemi di autenticazione intermittenti.

Causa

Quando si utilizza un provider di identità personalizzato con API Gateway, AWS WAF le regole possono interferire con le chiamate API tra Transfer Family e il provider di identità. Ciò può accadere perché AWS WAF sta ispezionando e potenzialmente bloccando il traffico API in base ai relativi set di regole.

Soluzione

Per risolvere i problemi relativi AWS WAF ai provider di identità personalizzati:

- Assicurati che la AWS WAF configurazione includa eccezioni per gli endpoint API Gateway utilizzati dal tuo provider di identità personalizzato.
- Aggiungi il responsabile del servizio Transfer Family (transfer.amazonaws.com) a una lista consentita nelle tue regole. AWS WAF
- Se utilizzi gruppi di regole gestiti, esaminali per individuare le regole che potrebbero influire sui flussi di autenticazione delle API e valuta la possibilità di disabilitare tali regole specifiche.
- Testa il tuo provider di identità utilizzando direttamente l'operazione `TestIdentityProvider` API per verificare che funzioni correttamente senza AWS WAF interferenze.

Risolvi i problemi relativi agli utenti gestiti dal servizio

Questa sezione descrive le possibili soluzioni ai problemi con gli utenti gestiti dal servizio.

Argomenti

- [Risolvi i problemi relativi agli utenti gestiti dal servizio](#)

Risolvi i problemi relativi agli utenti gestiti dal servizio

Questa sezione descrive le possibili soluzioni per i seguenti problemi.

Argomenti

- [Risolvi i problemi relativi al corpo della chiave pubblica per un periodo troppo lungo](#)
- [Risoluzione dei problemi: impossibile aggiungere la chiave pubblica SSH](#)

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 RSA-based, puoi convertirla in formato PEM. Ad esempio, Ubuntu fornisce uno strumento di conversione qui: <https://manpages.ubuntu.com/manpages/jammy/en/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 SSH2-formatted pubblica e che AWS Transfer Family non supporti le chiavi SSH2-formatted pubbliche per gli utenti gestiti dal servizio.

Soluzione

È necessario convertire la chiave in formato OpenSSH. Questo processo è descritto in [Conversione di una chiave SSH2 in formato chiave pubblica SSH](#)

Risolvi i problemi relativi a AS2

Questa sezione descrive le possibili soluzioni ai problemi relativi ai trasferimenti AS2.

Argomenti

- [Risolvi i problemi relativi a AS2](#)
- [Problemi relativi ai certificati AS2](#)
- [Problemi di ricezione MDN AS2](#)
- [Problemi di monitoraggio della scadenza dei certificati](#)

Risolvi i problemi relativi a AS2

[Codici di errore AS2](#), i messaggi e i suggerimenti per la risoluzione dei problemi per i server abilitati all'Applicability Statement 2 (AS2) sono descritti nella sezione Codici di errore AS2 di questa guida.

Problemi relativi ai certificati AS2

Descrizione

Stai riscontrando errori relativi ai certificati con i trasferimenti AS2.

Causa

Le cause più comuni includono certificati scaduti, formati di certificati errati o catene di certificati non corrispondenti.

Soluzione

Prova le seguenti soluzioni:

- Verifica che i tuoi certificati non siano scaduti
- Assicurati che i certificati siano nel formato corretto (PEM per) AWS Transfer Family
- Verifica che la catena di certificati sia completa e valida
- Verifica che i certificati di firma e di crittografia corrispondano tra i partner commerciali
- Ruota i certificati ben prima della scadenza per evitare interruzioni

Problemi di ricezione MDN AS2

Descrizione

Non stai ricevendo le notifiche di disposizione dei messaggi (mDNS) previste per i trasferimenti AS2.

Causa

I problemi di MDN possono verificarsi a causa di problemi di connettività di rete, configurazioni errate degli endpoint o mancate corrispondenze del formato MDN.

Soluzione

Prendi in considerazione queste soluzioni:

- Verifica che l'URL MDN sia configurato e accessibile correttamente
- Verifica la connettività di rete tra il server AS2 e l'endpoint MDN
- Assicurati che entrambi i partner commerciali siano configurati per lo stesso tipo di MDN (sincrono o asincrono)
- Controlla i log AS2 per eventuali errori relativi all'elaborazione MDN
- Se utilizzi mDNS sincrono, verifica che i timeout siano impostati in modo appropriato

Problemi di monitoraggio della scadenza dei certificati

Questa sezione fornisce soluzioni per problemi comuni relativi al monitoraggio della scadenza dei certificati e alla DaysUntilExpiry metrica.

DaysUntilExpiry metrica non visualizzata

Problema: la DaysUntilExpiry metrica non è visibile in Amazon CloudWatch dopo l'importazione di un certificato.

Soluzione::

- Attendi fino a 24 ore dopo l'importazione del certificato. Può essere necessario fino a un giorno intero prima che Transfer Family emetta la metrica sul tuo account.
- Assicurati di cercare nell' AWS area corretta e nel AWS/Transfer namespace in CloudWatch

Gli allarmi di scadenza dei certificati non si attivano

Problema: gli CloudWatch allarmi relativi alla scadenza dei certificati non si attivano quando previsto.

Soluzione::

- Verifica che l'allarme sia configurato con la Maximum statistica e un periodo di 1 giorno.
- Verifica che il confronto delle soglie sia impostato Less than or equal to sul numero di giorni desiderato.
- Assicurati che Treat missing data as good (not breaching) sia selezionato nella configurazione dell'allarme.
- Verifica che le dimensioni dell'allarme corrispondano a quelle del certificato CertificateId e della descrizione (se fornita).
- Verifica che le azioni di allarme (argomenti SNS, notifiche e-mail) siano configurate e attive correttamente.

AWS Transfer Family Riferimento API

La guida di riferimento API completa per Transfer Family è disponibile su [AWS Transfer Family API Reference](#).

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)

Server, utenti e 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`.

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 [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](#).

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: 19 novembre 2025

Modifica	Descrizione	Data
Supporto endpoint VPC per le app web Transfer Family	AWS Transfer Family le app Web ora supportano gli endpoint ospitati in VPC, consentendoti di ospitare l'endpoint dell'app Web all'interno di un cloud privato virtuale per il trasferimento di dati privati da e verso Amazon S3 senza attraversare la rete Internet pubblica. Per informazioni dettagliate, vedi Crea un'app web Transfer Family in un VPC .	19 novembre 2025
Supporto IPv6	AWS Transfer Family ora supporta endpoint dual-stack (IPv4 e IPv6) per endpoint pubblici SFTP, endpoint per connettori SFTP e AS2 ed endpoint API VPC-internal . SFTP/FTPS/FTP/AS2 Per informazioni dettagliate, vedi Supporto IPv6 per i server Transfer Family .	30 giugno 2025
Miglioramenti all'esperienza utente dei connettori SFTP	• Possibilità di impostare connessioni simultanee in	9 aprile 2025

Modifica	Descrizione	Data
	modalità self-service per i connettori • Capacità di fornire una chiave privata SSH in formato OpenSSH utilizzata per l'autenticazione delle connessioni • Capacità di scoprire la chiave host pubblica dei server remoti utilizzando i relativi connettori SFTP Per informazioni dettagliate, vedi Crea un connettore SFTP con uscita gestita dal servizio.	
Capacità dei connettori SFTP di eliminare, rinominare e spostare file sul server SFTP remoto	È ora possibile organizzare i file archiviati su server SFTP remoti eliminando, rinominando o spostando i file sorgente in posizioni di archiviazione dopo che sono stati copiati dal server remoto. Per informazioni dettagliate, vedi Sposta o rinomina file o directory sul server SFTP remoto.	7 aprile 2025

Modifica	Descrizione	Data
Support per app AWS Transfer Family Web	AWS Transfer Family le app Web sono una nuova risorsa che i clienti possono utilizzare e per creare un'interfaccia semplice per accedere ai propri dati in Amazon S3 tramite un browser Web. Per informazioni dettagliate, vedi App web Transfer Family .	1 dicembre 2024
API Reference è stato spostato in una guida separata	Per migliorare l'esperienza del cliente, l'API Reference è ora pubblicato separatamente dalla guida per l'utente. Per il riferimento separato all'API, consulta Welcome to the AWS Transfer Family API .	31 luglio 2024
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, consultare Elenca il contenuto di una directory remota .	23 aprile 2024

Modifica	Descrizione	Data
Possibilità di utilizzare il certificato TLS autofirmato di un partner commerciale con 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 di sicurezza per AWS Transfer Family i connettori SFTP .	5 aprile 2024
Integrazione con Amazon EventBridge	AWS Transfer Family ora pubblica automaticamente gli eventi su Amazon EventBridge per tutte le operazioni di trasferimento di file. Per informazioni dettagliate, vedi Gestione Transfer Family degli eventi tramite Amazon EventBridge .	8 febbraio 2024

Modifica	Descrizione	Data
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 i server AWS Transfer Family .	5 febbraio 2024
Support per indirizzi IP statici per connettori SFTP e AS2	Transfer Family ora fornisce indirizzi IP statici per connettori SFTP e AS2. Ciò consente la connessione con server SFTP remoti protetti da controlli di elenchi di indirizzi IP consentiti. Per AS2, stiamo introducendo gli indirizzi IP statici per le risposte MDN asincrone dai server AS2.	16 gennaio 2024
La guida per l'utente è stata riorganizzata per allinearla 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

Modifica	Descrizione	Data
Miglioramenti alla mappatura delle directory logiche Ottimizzazione delle prestazioni 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
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 Utilizzo dei connettori SFTP .	25 luglio 2023

Modifica	Descrizione	Data
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 server AWS Transfer Family .	24 giugno 2023
Support per diversi metodi di autenticazione	Transfer Family supporta l'autenticazione tramite password, public/private key pair o entrambi. È disponibile per i server che utilizzano il protocollo SFTP e un provider di identità personalizzato. Per ulteriori informazioni, consulta Crea un SFTP-enabled server .	17 maggio 2023

Modifica	Descrizione	Data
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 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 ulteriori informazioni, consultare e Genera 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'esterno 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 SFTP-enabled server , Creare un FTPS-enabled server o Crea un FTP-enabled server .	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 tuo provider di identità .	16 novembre 2021

Modifica	Descrizione	Data
Support per flussi di lavoro di trasferimento gestito di file	I flussi di lavoro di trasferimento file gestito forniscono astrazioni di elaborazione post-caricamento per le attività più comuni che attualmente 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 di AWS Directory Service per Microsoft Active Directory .	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 (Bahrein). 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 Family la 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 i server AWS Transfer Family .	12 agosto 2020

Modifica	Descrizione	Data
Supporto per gli endpoint Federal Information Processing Standard (FIPS)	FIPS-enabled gli endpoint sono ora disponibili in Nord America. Regioni AWS Per le regioni disponibili, consulta gli AWS Transfer Family endpoint e le quote in . Riferimenti generali di AWS Per abilitare FIPS per un endpoint SFTP-enabled server, vedere. Crea un SFTP-enabled server Per abilitare FIPS per un endpoint FTPS-enabled server, vedere. Creare un FTPS-enabled server Per abilitare FIPS per un endpoint FTP-enabled server, vedere. Crea un FTP-enabled server	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, consulta Gestione 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 SFTP-enabled server , Creare un FTPS-enabled server o Crea un FTP-enabled server .	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, consentendo 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 e 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 informazioni su configurazione client, configurazione utente e monitoraggio attività.	25 Novembre 2018

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.