Guida per l'utente

AWS Terminale di trasferimento dati

AWS Terminale di trasferimento dati: Guida per l'utente

Table of Contents

Che cos'è il terminale di trasferimento dati?

AWS Data Transfer Terminal è una postazione fisica predisposta per la rete in cui puoi portare i tuoi dispositivi di archiviazione dati per un trasferimento rapido dei dati da e verso il tuo servizio. Cloud AWS Carica i dati acquisiti in remoto per facilitare l'accesso ai dati acquisiti in remoto.

Pianifica una prenotazione presso una delle nostre strutture fisiche del Terminale di trasferimento dati dal AWS Management Console, arriva all'orario previsto e carica i dati sui tuoi Cloud AWS servizi con i tuoi dispositivi. Una volta completata la prenotazione programmata e dopo la partenza, la struttura viene nuovamente messa in sicurezza e pronta per la prossima prenotazione programmata.

> **Note**
>
> AWS Al momento, Data Transfer Terminal è disponibile solo per i clienti AWS Enterprise.

Per accedere al Data Transfer Terminal:

- AWS Console del terminale di trasferimento dati: https://console.aws.amazon.com/datatransferterminal
- Servizi del terminale di trasferimento dati: l'ubicazione delle strutture del terminale di trasferimento dati viene fornita una volta effettuata una prenotazione nella console. Per ulteriori informazioni, consulta Effettua un trasferimento di dati.

Funzionalità

L'utilizzo di AWS Data Transfer Terminal semplifica l'invio dei dati Cloud AWS al servizio da postazioni remote. Di seguito sono riportati alcuni dei vantaggi di Data Transfer Terminal per le esigenze di caricamento remoto dei dati:

Sicuro, privato ed esclusivo

Ogni struttura del Data Transfer Terminal è un luogo privato e sicuro in cui effettuare trasferimenti di dati di grandi dimensioni tra il dispositivo di archiviazione dati e i AWS servizi tramite una connessione di rete veloce.

Una console di prenotazione dedicata

Aggiungi personale approvato al tuo team di trasferimento e pianifica una prenotazione del Data Transfer Terminal utilizzando la console AWS Data Transfer Terminal.

Connessioni di rete in fibra ottica

Ogni struttura del Data Transfer Terminal include due connessioni in fibra ottica () da 100 Gigabit (GbpsLR4) per caricamenti rapidi dei dati e ridondanza.

Controllo dei dispositivi di archiviazione dei dati

Non è necessario spedire il dispositivo Snowball e attendere che i dati vengano caricati sui Cloud AWS servizi. Puoi controllare i dispositivi fisici di archiviazione dei dati durante l'intero processo di trasferimento dei dati, trasferendo i dati dove servono più velocemente.

Concetti chiave

L'utilizzo di AWS Data Transfer Terminal richiede che il titolare del processo pianifichi una prenotazione per consentire a uno specialista di trasferimento dati di accedere a una struttura del Terminale di trasferimento dati. Fai riferimento alle seguenti sezioni per saperne di più sulla terminologia del Data Transfer Terminal.

Argomenti

- Squadra di trasferimento
- Personale
- Strutture

Squadra di trasferimento

Un team di trasferimento è un gruppo di personale determinato da un Account AWS proprietario che può essere selezionato per condurre i trasferimenti di dati per conto dell'organizzazione. La configurazione di un team di trasferimento include l'assegnazione di un nome al team di trasferimento e la specificazione del personale per il team. Consigliamo gruppi di quattro o meno specialisti del trasferimento dei dati per una singola prenotazione.

Per ulteriori informazioni, consulta Pianifica una prenotazione del Terminale di trasferimento dati.

Personale

Il personale si riferisce alle persone che possono effettuare e gestire le prenotazioni o possono accedere e utilizzare le strutture del Terminale di trasferimento dati. Il personale può essere titolare del processo o specialista del trasferimento dei dati o entrambi.

Proprietario del processo

Il proprietario del processo è un Account AWS proprietario che può aggiungere, modificare e rimuovere personale dal proprio account AWS Data Transfer Terminal.

Specialista in trasferimento dati

Uno specialista del trasferimento dati è una persona che può rivolgersi alle strutture del Terminale di trasferimento dati per le transazioni di caricamento dei dati. Questo personale deve essere autorizzato dal titolare del processo e aggiunto all'account del Terminale di trasferimento AWS dati. Per accedere a una struttura del Terminale di trasferimento dati, sarà richiesto un documento d'identità rilasciato dal governo.

Strutture

Le strutture del Data Transfer Terminal sono hub di dati, di proprietà congiunta e gestiti da uno o più fornitori di servizi. Ogni struttura richiede che gli specialisti del trasferimento dei dati forniscano un documento d'identità rilasciato dal governo che deve corrispondere ai registri delle prenotazioni per accedere alla suite Data Transfer Terminal.

Considerazioni sulla pianificazione

Le prenotazioni possono essere effettuate nella console del Data Transfer Terminal per una durata da una a sei ore, per qualsiasi giorno della settimana, durante tutto l'anno. Le prenotazioni individuali possono essere programmate consecutivamente, con un intervallo minimo di un'ora tra le prenotazioni. Tutte le prenotazioni devono essere effettuate con almeno 24 ore di anticipo.

La quantità di tempo necessaria per effettuare il trasferimento dei dati varia a seconda della velocità delle prestazioni di caricamento. Considerate i seguenti fattori che influiscono sulle prestazioni di caricamento quando pianificate e programmate la prenotazione del Data Transfer Terminal.

Apparecchiature

Alcune apparecchiature possono includere impostazioni che possono influire sulle prestazioni di caricamento. Fai riferimento alle specifiche della tua attrezzatura per le velocità di caricamento consigliate.

Condizioni di rete

I periodi di intenso traffico di rete influiranno sulla velocità di caricamento dei dati e devono essere presi in considerazione quando si seleziona un orario per la sessione di trasferimento dei dati. La pianificazione della sessione di trasferimento dei dati nelle ore non di punta o durante i periodi di minore attività di rete può migliorare la velocità di caricamento.

Dimensioni del trasferimento dei dati

La connettività di rete del Data Transfer Terminal è progettata per trasferimenti di dati di grandi dimensioni. Tuttavia, la dimensione dei dati trasferiti influirà sulla durata della sessione.

Casi d'uso

Sebbene qualsiasi cliente AWS Enterprise possa accedere al sistema Data Transfer Terminal, alcuni scenari di utilizzo potrebbero trarne maggiori vantaggi.

Guida autonoma e sistemi avanzati di assistenza alla guida (AD/ADAS): i produttori di apparecchiature originali (OEM) e i fornitori generano grandi set di dati dalle loro flotte di veicoli autonomi che operano e raccolgono dati in numerose aree metropolitane del Nord America, Europa e ASEAN. Con Data Transfer Terminal, i dati raccolti da questi veicoli della flotta possono essere caricati sul Cloud AWS servizio e utilizzati per addestrare modelli AD/ADAS.

Media e intrattenimento: gli studi e altri creatori di contenuti generano spesso file audio e video digitali (AV) in località remote. È importante che questi file AV vengano caricati tempestivamente sul cloud in modo che i team di produzione e montaggio geograficamente distribuiti possano avviare flussi di lavoro in parallelo e in tempo reale. Utilizzando Data Transfer Terminal per caricare i dati in remoto, i tempi di produzione possono essere abbreviati, il che si traduce in una riduzione dei costi di produzione.

Mappe, fotogrammetria e immagini 3D: le organizzazioni che utilizzano applicazioni di mappatura o di immagini raccolgono dati in postazioni remote e devono caricare questi file visivi per l'analisi o la formazione. Cloud AWS Data Transfer Terminal riduce al minimo il tempo che intercorre tra la

raccolta e l'analisi di questi set di dati di grandi dimensioni, il che aiuta a conservare i dati geospaziali up-to-date per conducenti, agricoltori e altri utenti di tali informazioni.

Servizi correlati

Quanto segue Servizi AWS offre un'esperienza ottimale durante l'utilizzo di Data Transfer Terminal.

Servizio AWS	Descrizione
AWS Snowball Edge	AWS Data Transfer Terminal completa i prodotti Snowball fornendo una posizione per un caricamento più rapido AWS sul cloud, riducendo al minimo i tempi di attesa per accedere ai dati.
Amazon S3	Porta il tuo dispositivo a un terminale di trasferimento dati per caricare i dati in modo rapido e sicuro sul tuo servizio Amazon S3.

Requisiti tecnici per l'utilizzo del Terminale di trasferimento dati

Prima di programmare una prenotazione presso un terminale di trasferimento dati, è necessario assicurarsi di disporre delle apparecchiature e delle configurazioni necessarie per connettersi alla rete. Fai riferimento alle seguenti linee guida per una connettività e un'esperienza di rete ottimali.

Apparecchiature

È necessario portare dispositivi portatili per la connettività, tra cui monitor, tastiera, mouse e computer o laptop, alla struttura del Data Transfer Terminal per la prenotazione programmata.

L'hardware deve essere in grado di funzionare con connessioni in fibra ottica (L4)

> **Note**
>
> Come best practice per la sicurezza dei dati, assicurati che i tuoi dati siano crittografati e protetti sui dispositivi di archiviazione che porti al Data Transfer Terminal e che applichi politiche di crittografia dei dati durante l'utilizzo della funzionalità Data Transfer Terminal. Per ulteriori informazioni, consulta Sicurezza del terminale di trasferimento AWS dati

Requisiti di rete

Assicurati che il dispositivo, il server o l'appliance (laptop) di caricamento sia pronto per la connessione alla rete e che supporti DHCP. Per un'esperienza di caricamento dei dati ottimale, è necessario disporre di quanto segue:

- Un ricetrasmettitore QSFP ottico 100G QSFP28 LR4 (100GBASE-LR4), compatibile con i connettori NIC e LC per le connessioni via cavo in fibra fornite nella struttura Data Transfer Terminal.
- Configurazione automatica dell'indirizzo IP DHCP abilitato. I server DNS vengono assegnati automaticamente tramite DHCP.
- Up-to-date software e driver NIC.

Ottimizzazione delle prestazioni

Per massimizzare la velocità di trasmissione durante l'utilizzo del AWS Data Transfer Terminal, prendete in considerazione i seguenti consigli.

- Hardware consigliato:
  - Scheda di interfaccia di rete da 100 Gbps
  - CPU a 16 core
  - 128 GB DI RAM
  - più unità SSD NVME in un array RAID
- Utilizza la libreria AWS Common Runtime (AWS CRT) per i caricamenti utilizzando o SDK. AWS Command Line Interface AWS

  Ottimizza le impostazioni di trasferimento di Amazon S3 configurando i parametri seguenti. Imposta questi valori nella `s3` chiave di primo livello nel file di AWS configurazione, posizione predefinita. `~/.aws/config`

  ```
  [default]
  s3 =
      preferred_transfer_client = crt
      target_bandwidth = 100Gb/s
      max_concurrent_requests = 20
      multipart_chunksize = 16MB
  ```

  Tieni presente che tutti i valori di configurazione di Amazon S3 sono rientrati e annidati sotto la chiave di primo livello. `s3`

  - Facoltativo: puoi impostare i valori precedenti a livello di codice utilizzando il comando. `aws configure set` Ad esempio, per impostare i valori precedenti per il profilo predefinito, è possibile eseguire invece i seguenti comandi:

    ```
    aws configure set default.s3.preferred_transfer_client crt
    aws configure set default.s3.target_bandwidth 100Gb/s
    aws configure set default.s3.max_concurrent_requests 20
    aws configure set default.s3.multipart_chunksize 16MB
    ```

- Per impostare a livello di codice questi valori per un profilo diverso da quello predefinito, fornite il `--profile` flag. Ad esempio, per impostare la configurazione per un profilo denominato`test-profile`, esegui un comando come nell'esempio seguente.

```
aws configure set s3.max_concurrent_requests 20 --profile test-profile
```

- Abilita BBR (Linux) sul dispositivo per una migliore velocità di trasmissione.

```
sysctl -w net.core.default_qdisc=fq
sysctl -w net.ipv4.tcp_congestion_control=bbr
```

Ulteriori informazioni

Per ulteriori informazioni sulle configurazioni di Amazon S3 da riga di AWS comando per ottimizzare la connettività e le prestazioni di rete, consulta le seguenti risorse.

- AWS Configurazione CLI di Amazon S3 nel riferimento ai comandi AWS CLI
- Usa un client Amazon S3 performante AWS : client basato su CRT nell'Amazon S3Amazon SDK for Java AppStream
- Come posso ottimizzare le prestazioni quando utilizzo AWS CLI per caricare file di grandi dimensioni su Amazon S3? nel AWS Knowledge Center

Nozioni di base

Inizia a effettuare trasferimenti di dati in remoto verso i tuoi Cloud AWS servizi effettuando una prenotazione presso una delle strutture del Data Transfer Terminal. Per iniziare, avrai bisogno di apparecchiature supportate dalla struttura Data Transfer Terminal e di un account AWS Enterprise.

Consulta la Requisiti tecnici per l'utilizzo del Terminale di trasferimento dati sezione di questa guida prima di programmare una prenotazione per un terminale di trasferimento dati per assicurarti di disporre di apparecchiature con le configurazioni ottimali per il trasferimento dei dati. Non tutti i dispositivi di archiviazione dati e le apparecchiature di connessione di rete sono compatibili con le connessioni di rete in fibra ottica disponibili nelle suite.

Quando ti iscrivi AWS, il tuo Account AWS viene automaticamente registrato a tutti i servizi in AWS, incluso Data Transfer Terminal. Ti vengono addebitati solo i servizi che utilizzi.

Per configurare Data Transfer Terminal, segui i passaggi nelle seguenti sezioni.

Quando ti registri AWS e configuri Data Transfer Terminal, puoi facoltativamente modificare la lingua di visualizzazione in. AWS Management Console Per ulteriori informazioni, consulta Modifica della lingua della AWS Management Console nella Guida introduttiva di AWS Management Console .

Una volta che hai un, Account AWS puoi accedere al Data Transfer Terminal. Per ulteriori informazioni sulla configurazione e l'utilizzo di AWS Data Transfer Terminal, consultaPianifica una prenotazione del Terminale di trasferimento dati.

Registrati per un Account AWS

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

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Parte della procedura di registrazione prevede la ricezione di una telefonata o di un messaggio di testo e l'immissione di un codice di verifica sulla tastiera del telefono.

   Quando ti iscrivi a Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come 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.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Pianifica una prenotazione del Terminale di trasferimento dati

Per iniziare a utilizzare AWS Data Transfer Terminal, è necessario disporre di un account Account AWS e accedere alla console del Data Transfer Terminal all'indirizzo /datatransferterminal. https://console.aws.amazon.com Dopo aver effettuato l'accesso alla console Data Transfer Terminal, puoi vedere le prenotazioni esistenti o crearne una nuova. Per programmare una prenotazione, devi fare quanto segue:

1. Crea un team di trasferimento. Dovrai creare un gruppo designato di utenti per creare una prenotazione e accedere alla struttura del Terminale di trasferimento dati per effettuare un trasferimento di dati. Per ulteriori informazioni su questo argomento, vedereCrea un team di trasferimento.
2. Una volta creato il team, dovrai aggiungervi del personale. Per ulteriori informazioni sull'aggiunta di personale al team Transfer, consultaAggiungi personale.
3. Il proprietario del processo può pianificare il trasferimento dei dati con i team dell'account. Per ulteriori informazioni su come programmare la prenotazione, consultaSpecificare i dettagli della prenotazione.
4. Assicurati che i dettagli della prenotazione siano corretti prima di inviare la richiesta. Una volta inviata, una richiesta di prenotazione non può essere modificata per almeno 24 ore. Per ulteriori informazioni, consulta Rivedi e conferma la tua prenotazione.

Una volta elaborata e confermata la prenotazione, il team addetto al trasferimento sarà in grado di accedere alla struttura del Data Transfer Terminal all'orario previsto. Per ulteriori informazioni, consulta Effettua un trasferimento di dati presso la struttura Data Transfer Terminal.

Crea un team di trasferimento

Per accedere a una struttura del Data Transfer Terminal dovrai programmare una prenotazione nel AWS Management Console. Accedi Account AWS al tuo per accedere alla console del Data Transfer Terminal e completa i seguenti passaggi per programmare la tua prenotazione.

1. Dalla home page del Data Transfer Terminal, seleziona il pulsante Inizia.
2. Se non hai già un team di Transfer configurato nel tuo account, il pulsante Crea prenotazione verrà disabilitato. Per iniziare, dovrai creare e assegnare un nome a un team di trasferimento.

a. Seleziona il pulsante Crea squadra di trasferimento.

b. Dai un nome alla squadra.

   - Il nome deve avere una lunghezza compresa tra due e 64 caratteri, iniziando con una lettera o un numero.
   - Usa solo lettere, numeri, punti e trattini. I caratteri speciali non vengono riconosciuti.
   - Non includere informazioni identificative sensibili.

c. Crea una descrizione del team Transfer.

   - Fornisci una descrizione che aiuti a identificare il team, ad esempio descrivendo lo scopo del team per un periodo di tempo, una campagna o un progetto specifici.

d. Seleziona il pulsante Crea team Transfer.

   Tornerai alla pagina Trasferisci squadra e la squadra appena creata apparirà nella sezione Trasferisci squadre.

Aggiornamento dei team di Transfer sul tuo account Data Transfer Terminal

Per creare un nuovo team di Transfer, consulta la Pianifica una prenotazione del Terminale di trasferimento dati sezione di questa guida.

Per modificare o rimuovere un team di trasferimento, procedi come segue:

1. Nella pagina Trasferisci squadre, seleziona il team di trasferimento che desideri modificare.
2. Per modificare il nome e la descrizione del team di trasferimento, seleziona il pulsante Modifica.
3. Per aggiungere o rimuovere personale, seleziona la scheda Personale e completa i passaggi descritti nella sezione Come posso modificare, aggiungere o rimuovere personale dal mio account? sezione di questa FAQ.
4. Per aggiungere o annullare una prenotazione per il team di trasferimento selezionato, consulta la Aggiornamento del personale sul tuo account Data Transfer Terminal sezione di questa FAQ.

Aggiungi personale

Aggiungi i proprietari dei processi e gli specialisti del trasferimento dei dati al tuo team di trasferimento per configurare il trasferimento dei dati e accedere alla struttura del Data Transfer Terminal. Per aggiungere personale al tuo team di Transfer, procedi come segue:

1. Nella pagina Trasferisci squadre, seleziona la carta Trasferisci squadra desiderata tra quelle elencate nella sezione Trasferisci squadre. Apparirà la pagina di riepilogo della squadra che si trasferisce.
2. Scegli la scheda Personale, quindi il pulsante Registra persona per aggiungere personale al team di trasferimento.
3. Completa i campi con le informazioni necessarie sulla persona che stai aggiungendo al team di trasferimento nella pagina Registra personale.

    a. Alias personale: crea un alias univoco per identificare la persona.

        - L'alias viene utilizzato per identificare il personale proteggendone al contempo l'identità.
        - Può contenere fino a 64 caratteri e includere lettere, numeri e trattini.
        - I caratteri speciali non sono consentiti.

    b. Nome: fornisci il nome della persona così come appare sul documento d'identità rilasciato dal governo.

    c. Cognome: fornisci il cognome o il cognome della persona così come appare sul documento di identità rilasciato dal governo.

    d. Indirizzo e-mail: includi un indirizzo e-mail valido per consentire alla persona di ricevere le informazioni sulla prenotazione e le istruzioni per accedere alla struttura del Terminale di trasferimento dati.
4. Seleziona il pulsante Registra persona per completare l'aggiunta della persona al tuo team di Transfer.

Aggiornamento del personale sul tuo account Data Transfer Terminal

La modifica del personale esistente sul tuo account nella console del Data Transfer Terminal non è attualmente supportata. AWS Al momento, i proprietari di Data Transfer Terminal Process possono solo aggiungere o eliminare personale.

Per rimuovere il personale dal tuo account Data Transfer Terminal, procedi come segue:

1. Nella pagina Trasferimento team, seleziona il team di trasferimento associato al personale che desideri rimuovere.
2. Nella pagina di riepilogo del team di trasferimento selezionato, seleziona la scheda Personale.
3. Fai clic sul pulsante di opzione accanto all'alias che desideri rimuovere. Tieni presente che potrai vedere l'alias della persona solo quando elimini il suo profilo.
4. Seleziona il pulsante Elimina. Apparirà un avviso per confermare l'azione prevista per il personale selezionato. Fai clic sul pulsante Elimina per continuare. Nella parte superiore della console verrà visualizzato un banner che conferma che il personale è stato eliminato con successo.

Specificare i dettagli della prenotazione

Le seguenti istruzioni illustrano come programmare la prenotazione del Data Transfer Terminal nel AWS Management Console. Per informazioni sull'utilizzo della funzione Data Transfer Terminal, vedereEffettua un trasferimento di dati.

1. Seleziona il pulsante Effettua prenotazione nella scheda Prenotazioni imminenti.
2. Compila i campi nella pagina Specificare i dettagli della prenotazione.

    a. Selezione della squadra di trasferimento: La squadra di trasferimento selezionata come impostazione predefinita appare per prima. Se desideri scegliere una squadra diversa, fai clic sulla freccia a discesa per selezionarla dall'elenco delle squadre disponibili per il trasferimento.

    b. Titolare del processo: seleziona l'alias del personale a cui desideri affidare la gestione della prenotazione.

    - È consentito effettuare una prenotazione con un solo proprietario del processo, che deve essere un membro del personale autorizzato del processo. Account AWS

      Il Titolare del processo può essere incluso tra gli specialisti del trasferimento dei dati anche per eseguire l'attività di trasferimento dei dati.

    c. Specialista del trasferimento dati: seleziona il personale a cui desideri che abbia accesso alla struttura del Terminale di trasferimento dati per completare l'attività di trasferimento dei dati. È possibile selezionare più di un personale, se necessario.

    - La migliore pratica è limitare il team di trasferimento a non più di quattro (4) specialisti del trasferimento dei dati.

d. Informazioni sul terminale di trasferimento dati: specifica la funzione del terminale di trasferimento dati, la data desiderata e l'ora specifica per la sessione di trasferimento dati.

   i. Funzione del terminale di trasferimento dati: fai clic sulla freccia a discesa per selezionare una struttura del terminale di trasferimento dati.

   > **Note**
   >
   > Al momento della prenotazione verranno fornite solo le descrizioni delle strutture. Ulteriori informazioni sulla posizione verranno fornite nell'e-mail di conferma della prenotazione.

   ii. Data e ora del Terminale di trasferimento dati: fai clic sul campo Cerca una data e un'ora per la tua prenotazione per visualizzare il calendario e programmare la prenotazione.

   - Le prenotazioni devono essere effettuate con almeno 24 ore di anticipo e non più di sei (6) mesi prima e possono avere una durata massima di sei (6) ore. Una singola prenotazione può durare più di un giorno per tenere conto degli scenari con pernottamento, se necessario.
   - L'orario è indicato utilizzando un orologio a 24 ore e può essere prenotato solo in intervalli di un'ora intera.
   - Per effettuare prenotazioni consecutive, è necessario creare prenotazioni separate con almeno un'ora tra ogni sessione di trasferimento dati.
   - Per ulteriori informazioni, consulta Considerazioni sulla pianificazione.

3. Conferma che i dettagli della prenotazione siano corretti, quindi seleziona il pulsante Crea per continuare. Verrai reindirizzato alla pagina di conferma, che fornisce un riepilogo della tua prenotazione.

Rivedi e conferma la tua prenotazione

Dopo aver specificato i dettagli della prenotazione, seleziona il pulsante Avanti per continuare a visualizzare la pagina di panoramica. Controlla i dettagli della tua richiesta di prenotazione del Data Transfer Terminal nella pagina Rivedi e crea.

- Se sei soddisfatto della richiesta, seleziona il pulsante Crea.

- Se devi modificare la tua prenotazione, seleziona il pulsante Precedente.

Una volta inviata la richiesta di prenotazione, il proprietario del processo riceverà un'email di conferma che la richiesta è stata ricevuta ed è in corso di elaborazione. Una volta approvata la richiesta, un'altra e-mail confermerà la prenotazione e fornirà le istruzioni per localizzare e accedere alla struttura del Data Transfer Terminal. Per informazioni sull'accesso alla funzione Data Transfer Terminal, vedereEffettua un trasferimento di dati.

Apportare modifiche alla prenotazione

È previsto un periodo di elaborazione di 24 ore prima di poter apportare modifiche alla richiesta di prenotazione del Data Transfer Terminal.

Dopo il periodo di elaborazione, per visualizzare, modificare o eliminare la tua prenotazione, vai alla pagina Transfer teams nella console.

1. Individua e seleziona la prenotazione desiderata sulla scheda del team.
2. Fai clic sul menu Azioni e seleziona l'azione desiderata.
   - Visualizza: la selezione dell'opzione di visualizzazione consente di visualizzare i dettagli della prenotazione, tra cui data, ora, luogo e personale assegnato.
   - Modifica: puoi modificare i dettagli della prenotazione, tra cui data, ora, luogo e personale assegnato. Tieni presente che le modifiche devono essere apportate 24 ore prima della data di prenotazione desiderata e che le revisioni non vengono accettate e applicate immediatamente. Il proprietario del processo riceverà la conferma della richiesta aggiornata.
   - Elimina: l'opzione di cancellazione consente di cancellare la prenotazione. La richiesta di cancellazione deve essere effettuata almeno 24 ore prima della data di prenotazione prevista. Il proprietario del processo riceverà la conferma della prenotazione annullata quando la richiesta sarà approvata.

Effettua un trasferimento di dati presso la struttura Data Transfer Terminal

Il Data Transfer Terminal è una sede sicura e di proprietà condivisa che fornisce un accesso sicuro alla AWS rete. Per accedere alla struttura del Data Transfer Terminal, assicurati di avere un'e-mail di conferma con la descrizione della posizione e le istruzioni di accesso. Fai riferimento agli argomenti seguenti per ulteriori informazioni sull'accesso e sull'utilizzo della funzione Data Transfer Terminal.

Argomenti

Cosa portare

Gli specialisti del trasferimento dati devono portare gli elementi necessari per eseguire il trasferimento dei dati, ad esempio un computer portatile, unità flash, unità a stato solido (SSDs) e AWS Snowball Edge. Assicuratevi che le vostre apparecchiature siano ottimizzate per utilizzare i cavi di rete in fibra presso la struttura del Data Transfer Terminal. Per ulteriori informazioni sulle apparecchiature e sulle configurazioni ottimali, vedereRequisiti tecnici per l'utilizzo del Terminale di trasferimento dati.

L'utente è responsabile dell'installazione, dell'uso e della rimozione delle apparecchiature e degli articoli che l'accompagnatore e gli specialisti del trasferimento dei dati portano nella struttura del Terminale di trasferimento dei dati. Tutto ciò che viene portato nella suite deve essere rimosso al momento della partenza. AWS Data Transfer Terminal non è responsabile per gli oggetti dimenticati o smarriti.

Indirizzo fisico della struttura del Data Transfer Terminal

L'indirizzo fisico della struttura del Terminale di trasferimento dati non verrà fornito. Invece, il proprietario del processo e gli specialisti del trasferimento dei dati specificati nella prenotazione riceveranno un'e-mail con il nome pubblico ricercabile della struttura del Terminale di trasferimento dati. AWS Data Transfer Terminal utilizza lo stesso sistema di identificazione della posizione AWS

Direct Connect in modo da poter cercare il nome pubblico su Internet per localizzare la struttura del Terminale di trasferimento dati. Se non disponi di un'e-mail con queste informazioni, conferma con l'account manager del Terminale di trasferimento AWS dati di essere incluso nel team di Transfer e che le informazioni e-mail sono corrette.

Accesso all'edificio

Per accedere alla struttura del Terminale di trasferimento dati, ogni specialista del trasferimento dati deve fornire un documento di identità o un documento d'identità rilasciato dal governo. Una volta ammessi all'edificio, i servizi di sicurezza vi accompagneranno alla suite Data Transfer Terminal.

Apparecchiature previste nella suite Data Transfer Terminal.

Ogni struttura del Data Transfer Terminal deve avere solo due (2) cavi in fibra ottica, un tavolo o una scrivania e sedie. Se ci sono altre apparecchiature o oggetti nella stanza, segnalalo Supportoimmediatamente.

Risoluzione dei problemi di connessione di rete

Se riscontri problemi di connessione alla rete durante l'utilizzo di AWS Data Transfer Terminal, ad esempio l'impossibilità di connetterti a Internet o se la connessione è lenta, prendi in considerazione i seguenti suggerimenti per la risoluzione dei problemi.

Argomenti

Problemi di connessione delle apparecchiature

Se hai difficoltà a stabilire una connessione fisica mentre sei nella suite Data Transfer Terminal, considera quanto segue:

- Ogni struttura del Data Transfer Terminal avrà due (2) cavi in fibra LC monomodali. Se uno o entrambi questi cavi sono mancanti, contatta immediatamente il servizio di AWS assistenza.
- Se un cavo in fibra ottica non funziona, prova prima ad arrotolarlo. Se non riesci ancora a connetterti con il primo cavo, prova a usare l'altro cavo.

Se non riesci ancora a utilizzare i cavi per la connessione, contatta immediatamente l'AWS assistenza.

Risoluzione dei problemi relativi alla connettività

Se riesci a connettere l'apparecchiatura ma non riesci a connetterti alla rete, prova i seguenti suggerimenti per la risoluzione dei problemi.

- Verifica che la configurazione dell'apparecchiatura soddisfi i requisiti di rete specificati. Per ulteriori informazioni, consulta Requisiti tecnici per l'utilizzo del Terminale di trasferimento dati
- Passa all'altro cavo in fibra ottica da collegare.
- Riavvia il dispositivo mantenendo collegati i cavi in fibra ottica.
- Esegui la diagnostica di rete di base sul dispositivo per garantire quanto segue:
  - DHCP è abilitato

- Un indirizzo IP viene assegnato all'interfaccia di rete connessa
- I server DNS sono configurati
- L'orologio di sistema è sincronizzato con NTP

Se non riesci ancora a connetterti, contatta l'AWS assistenza e fornisci loro i seguenti output a seconda del sistema operativo (OS) in esecuzione sul tuo dispositivo.

Linux/Unix

- Ottieni l'indirizzo IP e le informazioni di routing in un terminale o in un'interfaccia a riga di comando (CLI). Verificate che all'interfaccia di rete sia assegnato un indirizzo IP e che nella tabella delle rotte venga aggiunta una route predefinita con un indirizzo gateway predefinito.

```
ip address show
ip route show
```

  - In alternativa, se non `iproute2` è installato sul dispositivo e `ip` i comandi non sono disponibili, utilizzate i seguenti comandi:

```
ifconfig
netstat -rn
```

- Raccogli informazioni sul server DNS. Questo dovrebbe mostrare due indirizzi IP che iniziano con la `nameserver` parola chiave.

```
cat /etc/resolv.conf
```

- Raccogli i risultati dei test di connettività di base. Sostituisci il `default_gateway_address` con l'indirizzo IP del gateway predefinito assegnato.

```
ping -c 5 <default_gateway_address>
ping -c 5 s3.amazonaws.com
traceroute s3.amazonaws.com
```

- Raccogli l'output del test di connettività HTTPS. Il comando seguente dovrebbe mostrare una `HTTP 200 OK` risposta da Amazon S3.

```
curl -i https://s3.amazonaws.com/ping
```

Windows

- Ottieni l'indirizzo IP, il routing e le informazioni sul server DNS nel prompt dei comandi. Verificate che all'interfaccia di rete sia assegnato un indirizzo IP, che siano assegnati due server DNS e che nella tabella di routing venga aggiunta una route predefinita con un indirizzo gateway predefinito.

```
ipconfig /all
route print
```

- Raccogli l'output dei test di connettività di base nel prompt dei comandi. Sostituisci il `default_gateway_address` con l'indirizzo IP del gateway predefinito assegnato.

```
ping <default_gateway_address>
ping s3.amazonaws.com
tracert s3.amazonaws.com
```

- Raccogli l'output del test di connettività HTTPS in PowerShell. Il comando seguente dovrebbe mostrare una `HTTP 200 OK` risposta.

```
Invoke-WebRequest -Uri "https://s3.amazonaws.com/ping"
```

Throughput di rete

La velocità di trasmissione della rete, che misura l'effettiva velocità di trasferimento dei dati in una rete, può essere influenzata da vari fattori. Quanto segue può influire sulla velocità di trasferimento dei dati:

- Hardware: i componenti hardware del dispositivo possono ridurre la velocità di connessione durante il caricamento dei dati. La CPU e i dischi utilizzati nel dispositivo potrebbero raggiungere i limiti di prestazioni. Prendi in considerazione l'utilizzo di NVME SSDs in un array RAID. Assicurati di utilizzare la libreria AWS CRT per migliorare le prestazioni e ridurre l'utilizzo della CPU.
- Sovraccarico di crittografia: le trasmissioni sicure, come HTTPS, aumentano i tempi di elaborazione a causa del sovraccarico di crittografia.
- Latenza: la latenza si riferisce al tempo impiegato da un pacchetto di dati per viaggiare dall'origine alla destinazione. È possibile osservare un'elevata latenza durante il caricamento su un bucket Amazon S3 in un'area geografica diversa, il che può comportare ritardi nel trasferimento dei dati

e una riduzione del throughput. La migliore pratica consiste nell'effettuare trasferimenti di dati all'interno della stessa regione, quando possibile.

- Perdita di pacchetti: i pacchetti persi richiedono la ritrasmissione, rallentando il trasferimento dei dati.

Sicurezza del terminale di trasferimento AWS dati

AWS Data Transfer Terminal offre un ambiente sicuro per effettuare trasferimenti di dati da e verso Cloud AWS. Come qualsiasi altra connessione fisica in fibra di rete, la connessione Data Transfer Terminal non fornisce la crittografia predefinita. Pertanto, sarà tua responsabilità applicare le migliori pratiche di crittografia dei dati per garantire che il trasferimento dei dati sia sicuro.

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità che si applicano al Terminale di trasferimento AWS dati, vedere AWS Servizi nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Data Transfer Terminal. I seguenti argomenti mostrano come proteggere i dati durante l'utilizzo del servizio Data Transfer Terminal. Imparerai anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse del tuo Data Transfer Terminal.

Argomenti

- Sicurezza dell'infrastruttura nel terminale di trasferimento AWS dati

Protezione dei dati nel AWS Data Transfer Terminal

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei AWS dati nel Data Transfer Terminal. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. 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. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Data Transfer Terminal o altro Servizi AWS utilizzando la console, l'API o.

AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati

AWS Data Transfer Terminal fornisce l'accesso a una connessione di rete ad alta velocità che consente di trasferire in modo sicuro i dati tra sistemi di storage autogestiti e AWS servizi di archiviazione. Il modo in cui i dati di archiviazione vengono crittografati durante il transito dipende in parte dalle politiche abilitate sui dispositivi e dai servizi a cui vengono trasferiti i dati. La gestione dei dati e la relativa crittografia in transito sono responsabilità dell'individuo che utilizza Data Transfer Terminal.

Crittografia a riposo

AWS Data Transfer Terminal crittografa tutti i dati inattivi.

Data Transfer Terminal acquisisce solo i dati necessari per le prenotazioni, inclusi nome e cognome e indirizzi e-mail delle persone specificate per partecipare e programmare la prenotazione. Lo scopo di questa raccolta di dati è confermare i dettagli della prenotazione e garantire l'accesso alla camera per eseguire il trasferimento dei dati. Il backup di queste informazioni transazionali non viene eseguito per più di 35 giorni, tuttavia, le informazioni sull' AWS account vengono conservate per 10 anni.

Crittografia in transito

AWS Data Transfer Terminal non crittografa i dati in transito. I dati si encrypted-in-transit verificano quando interagisci con gli endpoint dell'API Data Transfer Terminal per configurare i team di Transfer, aggiungere personale e pianificare le prenotazioni nella console. Nell'ambito del modello di responsabilità AWS condivisa, puoi scegliere come connetterti Servizi AWS tramite Data Transfer Terminal. Ti consigliamo vivamente di scegliere di connetterti Servizi AWS utilizzando sistemi forti encryption-in-transit, come TLS 1.2 e 1.3.

Ad esempio, utilizza solo connessioni crittografate su HTTPS (TLS) utilizzando la `aws:SecureTransport`condizione nelle policy relative ai bucket di Amazon S3, come illustrato nella policy del bucket riportata di seguito.

```
{
```

```
 "Version": "2012-10-17",
    "Statement": [{
        "Sid": "RestrictToTLSRequestsOnly",
        "Action": "s3:",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        },
        "Principal": "*"
    }]
}
```

Per ulteriori informazioni sulla crittografia dei dati in transito con altri Servizi AWS, ad esempio Amazon S3, consulta la sezione Protezione dei dati con crittografia lato server nella Amazon S3 User Guide.

Gestione delle chiavi

AWS Data Transfer Terminal non supporta direttamente le chiavi gestite dal Cliente. Utilizza l'assistenza con chiavi gestite dal cliente disponibile per i AWS servizi a cui ti connetti durante la prenotazione del Terminale di trasferimento dati. Scopri di più sulle chiavi gestite dal cliente e su come crittografare i dati archiviati nella sezione sulle chiavi AWS KMS della AWS Key Management Service Developer Guide.

Riservatezza del traffico Internet

L'accesso alla console del Data Transfer Terminal avviene tramite il servizio pubblicato. APIs Le risorse del Data Transfer Terminal sono indipendenti dal cloud privato virtuale (VPC).

Gestione delle identità e degli accessi per Data Transfer Terminal

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 del Data Transfer Terminal. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Data Transfer Terminal.

Utente del servizio: se utilizzi il servizio Data Transfer Terminal per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità del Data Transfer Terminal per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Data Transfer Terminal, consultaRisoluzione dei problemi relativi all'identità e all'accesso al AWS Data Transfer Terminal.

Amministratore del servizio: se sei responsabile delle risorse del Data Transfer Terminal presso la tua azienda, probabilmente hai pieno accesso a Data Transfer Terminal. È tuo compito determinare a quali funzionalità e risorse del Data Transfer Terminal devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Data Transfer Terminal, consultaCome funziona Data Transfer Terminal con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso al Data Transfer Terminal. Per visualizzare esempi di policy basate sull'identità di Data Transfer Terminal che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Data Transfer Terminal AWS

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA)AWS in IAM nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per

effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
- Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore

IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di

Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.

- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come funziona Data Transfer Terminal con IAM

Prima di utilizzare IAM per gestire l'accesso al Data Transfer Terminal, scopri quali funzionalità IAM sono disponibili per l'uso con Data Transfer Terminal.

Funzionalità IAM	Supporto per Data Transfer Terminal
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	No
Credenziali temporanee	Sì
Autorizzazioni del principale	No

Funzionalità IAM	Supporto per Data Transfer Terminal
☻Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una visione di alto livello di come Data Transfer Terminal e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Data Transfer Terminal

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per Data Transfer Terminal

Per visualizzare esempi di politiche basate sull'identità del Data Transfer Terminal, vedere. Esempi di policy basate sull'identità per Data Transfer Terminal AWS

Politiche basate sulle risorse all'interno di Data Transfer Terminal

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi

possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per il terminale di trasferimento dati

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale 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 a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni del terminale di trasferimento dati, vedere Azioni definite da AWS Data Transfer Terminal nel riferimento di autorizzazione del servizio.

Le azioni politiche in Data Transfer Terminal utilizzano il seguente prefisso prima dell'azione:

```
datatransferterminal
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
```

```
      "datatransferterminal:action1",
      "datatransferterminal:action2"
         ]
```

Per visualizzare esempi di politiche basate sull'identità di Data Transfer Terminal, consulta. Esempi di policy basate sull'identità per Data Transfer Terminal AWS

Risorse politiche per Data Transfer Terminal

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse del Data Transfer Terminal e relativi ARNs, consulta Risorse definite da AWS Data Transfer Terminal nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ciascuna risorsa, vedere Azioni definite dal terminale di trasferimento AWS dati.

Per visualizzare esempi di politiche basate sull'identità di Data Transfer Terminal, consulta. Esempi di policy basate sull'identità per Data Transfer Terminal AWS

Chiavi relative alle condizioni delle policy per Data Transfer Terminal

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. 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.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco delle chiavi di condizione del Data Transfer Terminal, consulta Condition Keys for AWS Data Transfer Terminal nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta Azioni definite dal terminale di trasferimento AWS dati.

Per visualizzare esempi di politiche basate sull'identità di Data Transfer Terminal, consulta. Esempi di policy basate sull'identità per Data Transfer Terminal AWS

ACLs in Data Transfer Terminal

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con terminale di trasferimento dati

Supporta ABAC (tag nelle politiche): No

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Data Transfer Terminal

Supporta le credenziali temporanee: sì

Alcuni Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per Data Transfer Terminal

Supporta l'inoltro delle sessioni di accesso (FAS): no

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Data Transfer Terminal

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità del Data Transfer Terminal. Modifica i ruoli di servizio solo quando Data Transfer Terminal fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Data Transfer Terminal

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati in Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked

role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Data Transfer Terminal AWS

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse del Data Transfer Terminal. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da, incluso il formato di ARNs per ogni tipo di risorsa, consulta Actions, Resources and Condition Keys for AWS Data Transfer Terminal nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Data Transfer Terminal
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse del Data Transfer Terminal nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Data Transfer Terminal

Per accedere alla console AWS Data Transfer Terminal, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse del Data Transfer Terminal presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console del Terminale di trasferimento dati, collega anche il Terminale di trasferimento dati *ConsoleAccess* o la politica *ReadOnly* AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso al AWS Data Transfer Terminal

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Data Transfer Terminal e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Data Transfer Terminal
- Voglio consentire a persone esterne a me di accedere Account AWS alle risorse del mio Data Transfer Terminal

Non sono autorizzato a eseguire un'azione in Data Transfer Terminal

Se non riesci a visualizzare o pianificare le prenotazioni nella console AWS Data Transfer Terminal, potresti non disporre delle autorizzazioni richieste. Contatta l'amministratore del tuo account per configurare una policy di identità IAM che ti garantisca l'accesso e le autorizzazioni appropriate.

Voglio consentire a persone esterne a me di accedere Account AWS alle risorse del mio Data Transfer Terminal

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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Data Transfer Terminal supporta queste funzionalità, consulta. Come funziona Data Transfer Terminal con IAM
- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, 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 IAM.

Riferimenti all'API Data Transfer Terminal: azioni e risorse

Durante la creazione di policy AWS Identity and Access Management (IAM), questa pagina può aiutarti a comprendere la relazione tra le operazioni dell'API AWS Data Transfer Terminal, le azioni corrispondenti per le quali puoi concedere le autorizzazioni e AWS le risorse per le quali puoi concedere le autorizzazioni.

In generale, ecco come aggiungere le autorizzazioni di Data Transfer Terminal alla tua policy:

- Specificate un'azione nell'`Action`elemento. Il valore include un `datatransferterminal:` prefisso e il nome dell'operazione API. Ad esempio, `datatransferterminal:CreateTask`.
- Specificate una AWS risorsa correlata all'azione nell'`Resource`elemento.

Puoi anche utilizzare le chiavi di AWS condizione nelle politiche del tuo Data Transfer Terminal. Per un elenco completo delle AWS chiavi, consulta Available keys nella IAM User Guide.

Operazioni dell'API Data Transfer Terminal e azioni corrispondenti

CreateTransferTeam

Operazione: `datatransferterminal:CreateTransferTeam`

Risorsa:None

GetTransferTeam

Operazione: `datatransferterminal:GetTransferTeam`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

UpdateTransferTeam

Operazione: `datatransferterminal:UpdateTransferTeam`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

DeleteTransferTeam

Operazione: `datatransferterminal:DeleteTransferTeam`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

ListTransferTeams

Operazione: `datatransferterminal:ListTransferTeams`

Risorsa:None

RegisterPerson

Operazione: `datatransferterminal:RegisterPerson`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

GetPerson

Operazione: `datatransferterminal:GetPerson`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId/person/$PersonId`

Azione dipendente: `datatransferterminal:GetTransferTeam`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

DeregisterPerson

Operazione: `datatransferterminal:DeregisterPerson`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId/person/$PersonId`

Azione dipendente: `datatransferterminal:GetTransferTeam`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

ListPersons

Operazione: `datatransferterminal:ListPersons`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

CreateReservation

Operazione: `datatransferterminal:CreateReservation`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

Azione dipendente: `datatransferterminal:GetTransferTeam`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

Azione dipendente: `datatransferterminal:GetPerson`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId/person/$PersonId`

Azione dipendente: `datatransferterminal:GetFacility`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:::facility/$FacilityId`

GetReservation

Operazione: `datatransferterminal:GetReservation`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId/reservation/$ReservationId`

Azione dipendente: `datatransferterminal:GetTransferTeam`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

UpdateReservation

Operazione: `datatransferterminal:UpdateReservation`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId/reservation/$ReservationId`

Azione dipendente: `datatransferterminal:GetTransferTeam`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

Azione dipendente: `datatransferterminal:GetPerson`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId/person/$PersonId`

DeleteReservation

Operazione: `datatransferterminal:DeleteReservation`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId/person/$PersonId`

Azione dipendente: `datatransferterminal:GetTransferTeam`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

ListReservations

Operazione: `datatransferterminal:ListReservations`

Risorsa:`arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

ListFacilities

Operazione: `datatransferterminal:ListFacilities`

Risorsa:None

GetFacility

Operazione: `datatransferterminal:GetFacility`

Risorsa:`arn:aws::$Partition:datatransferterminal:::facility/$FacilityId`

GetFacilityAvailability

Operazione: `datatransferterminal:GetFacilityAvailability`

Risorsa:`arn:aws::$Partition:datatransferterminal:::facility/$FacilityId/availability`

Azione dipendente: `datatransferterminal:GetFacility`

Risorsa dipendente: `arn:aws::$Partition:datatransferterminal:::facility/$FacilityId/availability`

Convalida della conformità per AWS Data Transfer Terminal

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of

Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).

- Evaluating Resources with Rules nella AWS Config Developer Guide: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza nel terminale di trasferimento AWS dati

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS 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, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

AWS Data Transfer Terminal è disponibile in tutto il mondo. È possibile connettersi a qualsiasi Regione AWS dispositivo accessibile da Internet.

Registrazione e monitoraggio nel terminale di trasferimento dati

AWS Data Transfer Terminal è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Data Transfer Terminal. CloudTrail acquisisce tutte le chiamate API per Data Transfer Terminal come eventi. Le chiamate

acquisite includono chiamate dalla console Data Transfer Terminal e chiamate di codice alle operazioni dell'API Data Transfer Terminal. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Data Transfer Terminal. 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 la richiesta che è stata effettuata a Data Transfer Terminal, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e altri dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni sul terminale di trasferimento dati in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività nel Terminale di trasferimento dati, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo Account AWS, compresi gli eventi per Data Transfer Terminal, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo 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 le azioni del Data Transfer Terminal vengono registrate CloudTrail e sono documentate nella Riferimenti all'API Data Transfer Terminal: azioni e risorse sezione di questa guida.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- 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.

Comprensione delle voci dei file di registro del Data Transfer Terminal

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Sicurezza dell'infrastruttura nel terminale di trasferimento AWS dati

In quanto servizio gestito, AWS Data Transfer Terminal è protetto dalle procedure di sicurezza di rete AWS globali descritte nel white paper Amazon Web Services: Overview of Security Processes.

Utilizzi chiamate API AWS pubblicate per accedere a Data Transfer Terminal attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.0 o versioni successive. È consigliabile TLS 1.2 o versioni successive. I client devono, inoltre, supportare le suite di cifratura con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Cronologia dei documenti per la Guida per l'utente del terminale di trasferimento dati

La tabella seguente descrive le modifiche importanti in ogni versione della AWS Data Transfer Terminal User Guide. Per ricevere notifiche sugli aggiornamenti della documentazione, puoi sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	Data di lancio della documentazione originale.	dicembre 2024
Aggiorna il layout	Aggiornamenti al layout del documento e modifiche minori alla verbosità e al contenuto.	Gennaio 2025

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.