Guida di riferimento

AWS Gestione dell'account

AWS Gestione dell'account: Guida di riferimento

Table of Contents

Benvenuto nella Guida di riferimento per la gestione degli AWS account

Account AWSsono una parte fondamentale dell'accesso ai AWS servizi.

An Account AWS svolge due funzioni di base:

- Contenitore: An Account AWS è il contenitore di base per tutte le AWS risorse che crei come AWS cliente. Ad esempio, un bucket Amazon Simple Storage Service (Amazon S3), un database Amazon Relational Database Service (Amazon RDS) e un'istanza Amazon Elastic Compute Cloud (Amazon EC2) sono tutte risorse. Ogni risorsa è identificata in modo univoco da un Amazon Resource Name (ARN) che include l'ID dell'account che contiene o possiede la risorsa.
- Limite di sicurezza: An Account AWS è anche il limite di sicurezza di base per le tue risorse. AWS Le risorse che crei nel tuo account sono disponibili per gli utenti che dispongono delle credenziali per il tuo account.

  Tra le risorse principali che puoi creare nel tuo account ci sono le identità, come utenti e ruoli. Le identità hanno credenziali che qualcuno può utilizzare per accedere (autenticarsi). AWS Le identità hanno anche politiche di autorizzazione che specificano cosa può fare un utente (autorizzazione) con le risorse dell'account.

  Come procedura consigliata in materia di sicurezza, richiedi agli utenti di utilizzare credenziali temporanee durante l'accesso. AWS Per fornire credenziali temporanee, puoi utilizzare la federazione e un provider di identità, ad esempio AWS IAM Identity Center(IAM Identity Center). Se la tua azienda utilizza già un provider di identità, utilizzalo con la federazione per semplificare il modo in cui fornisci l'accesso alle risorse del tuoAccount AWS.

  Per informazioni sulle best practice di sicurezza, consulta la sezione Best practice di sicurezza in IAM nella IAM User Guide.

Argomenti

Ho bisogno di piùAccount AWS?

Account AWSfunge da confine fondamentale per la sicurezza inAWS. Servono come contenitore di risorse che fornisce un utile livello di isolamento. La capacità di isolare risorse e utenti è un requisito fondamentale per creare un ambiente sicuro e ben gestito.

Separazione delle risorse in separateAccount AWSaiuta a supportare i seguenti principi nel tuo ambiente cloud:

- Controllo di sicurezza— Diverse applicazioni possono avere profili di sicurezza diversi, che richiedono diversi criteri di controllo e meccanismi intorno a loro. Ad esempio, è molto più facile parlare con un auditor ed essere in grado di indicare un singoloAccount AWSche ospita tutti gli elementi del tuo carico di lavoro soggetti aPayment Card Industry (Payment Card Industry) Standard di sicurezza.
- ISOLATION— UnAccount AWSè un'unità di protezione di sicurezza. I rischi potenziali e le minacce alla sicurezza dovrebbero essere contenuti all'interno di unAccount AWSsenza intaccare gli altri. Potrebbero esserci diverse esigenze di sicurezza a causa dei diversi team o dei diversi profili di sicurezza.
- Molti team— Diversi team hanno le loro responsabilità e le loro esigenze di risorse diverse. È possibile impedire ai team di interferire tra di loro spostandoli in modo separatoAccount AWS.
- Isolamento dei dati— Oltre a isolare i team, è importante isolare i data store su un account. Ciò può contribuire a limitare il numero di persone che possono accedere e gestire quel data store. Ciò aiuta a contenere l'esposizione a dati altamente privati e quindi può aiutare nel rispetto dellaRegolamento generale sulla protezione dei dati dell'Unione europea (GDPR).
- Processo aziendale— Business unit o prodotti diversi possono avere scopi e processi completamente diversi. con piùAccount AWS, è possibile supportare le esigenze specifiche di una business unit.
- Fatturazione— Un account è l'unico modo vero per separare gli articoli a livello di fatturazione. Più account aiutano a separare gli articoli a livello di fatturazione tra business unit, team funzionali o singoli utenti. Puoi comunque consolidare tutte le tue fatture a un singolo pagatore (utilizzandoAWS Organizationse fatturazione consolidata) pur avendo gli elementi riga separati daAccount AWS.
- Allocazione di quote–AWSle quote di servizio vengono applicate separatamente per ciascunaAccount AWS. Separazione dei carichi di lavoro in diversiAccount AWSimpedisce loro di consumare quote l'una per l'altra.

Tutte le raccomandazioni e le procedure descritte in questo documento sono conformi alAWSFramework Well-Architected. Questo framework ha lo scopo di aiutarti a progettare un'infrastruttura cloud flessibile, resiliente e scalabile. Anche quando si inizia in piccole dimensioni, si consiglia di procedere nel rispetto di questa guida nel quadro. Ciò può aiutarti a scalare il tuo ambiente in modo sicuro e senza influire sulle operazioni in corso man mano che cresci.

Gestione di piùAccount AWS

Prima di iniziare ad aggiungere più account, è necessario sviluppare un piano per gestirli. Per questo, consigliamo di utilizzareAWS Organizations, che è gratuitoAWSservizio per gestire tutto ilAccount AWSnella tua organizzazione.

AWSoffre ancheAWS Control Tower, che aggiunge strati diAWSautomazione gestita per le Organizations e la integra automaticamente con altriAWSservizi comeAWS CloudTrail,AWS Config, Amazon CloudWatch,AWS Service Cataloge altri. Questi servizi possono comportare costi aggiuntivi. Per ulteriori informazioni, consulta Prezzi di AWS Control Tower.

Guida introduttiva: sei un AWS utente alle prime armi?

Se sei il primo utente diAWS, il primo passo è iscriverti a unAccount AWS. Quando ti registri, AWS crea un account Account AWS con i dettagli che fornisci e ti assegna l'account. Dopo aver creato il tuoAccount AWS, accedi come utente root, attiva l'autenticazione a più fattori (MFA) per l'utente root e assegna l'accesso amministrativo a un utente.

Fasi

- Prerequisiti
- Fase 1: Crea il tuo Account AWS
- Passaggio 2: attiva l'MFA per il tuo utente root
- Fase 3: Creare un utente amministratore
- Argomenti correlati

Prerequisiti

Per iscriverti a unAccount AWS, hai bisogno delle seguenti informazioni:

- Un nome account: il nome dell'account viene visualizzato in diversi punti, ad esempio sulla fattura, e in console come la dashboard di Billing and Cost Management e la console. AWS Organizations

Ti consigliamo di utilizzare un modo standard per denominare i tuoi account in modo da poter assegnare ai tuoi account nomi facili da riconoscere. Per gli account aziendali, prendi in considerazione l'utilizzo di uno standard di denominazione come organizzazione - scopo - ambiente (ad esempio, AnyCompany- audit - prod). Per gli account personali, prendete in considerazione l'utilizzo di uno standard di denominazione come nome - cognome - scopo (ad esempio,). paulo-santos-testaccount

Per informazioni sulla modifica del nome di un account, vedi Come posso cambiare il nome sul mio Account AWS account? .

- Indirizzo: se il tuo indirizzo di contatto è in India, l'accordo utente per il tuo account è con Amazon Internet Services Private Limited (AISPL), un AWS venditore locale in India. È necessario fornire il CVV come parte del processo di verifica. Potrebbe inoltre essere necessario inserire una password monouso, a seconda della banca. AISPL addebita al tuo metodo di pagamento 2 INR come parte del processo di verifica. AISPL rimborserà i 2 INR dopo il completamento della verifica.
- Un indirizzo e-mail: l'indirizzo e-mail viene utilizzato come nome di accesso per l'utente root ed è necessario per il ripristino dell'account. Devi essere in grado di ricevere messaggi di posta elettronica inviati a questo indirizzo. Prima di poter eseguire determinate attività, è necessario verificare di avere accesso ai messaggi di posta elettronica inviati a questo indirizzo.

> **Important**
>
> Se questo account è destinato a un'azienda, utilizza una lista di distribuzione aziendale sicura (ad esempio`it.admins@example.com`) in modo che la società possa continuare ad accedervi Account AWS anche quando un dipendente cambia posizione o lascia l'azienda. Poiché l'indirizzo e-mail può essere utilizzato per reimpostare le credenziali dell'utente root dell'account, proteggi l'accesso a questa lista di distribuzione o a questo indirizzo.

- Un numero di telefono: questo numero può essere utilizzato per confermare la proprietà del tuo account. Devi essere in grado di ricevere chiamate a questo numero di telefono.

> **Important**
>
> Se questo account è destinato a un'azienda, utilizza un numero di telefono aziendale in modo che l'azienda possa continuare ad accedervi Account AWS anche quando un dipendente cambia posizione o lascia l'azienda.

Fase 1: Crea il tuo Account AWS

1. Nel tuo browser, apri la AWShome page.
2. Scegli Crea un Account AWS.

   > **Note**
   >
   > Se hai effettuato l'accesso di AWS recente, scegli Accedi. Se l'opzione Crea un nuovo Account AWS non è visibile, scegli prima Accedi a un altro account, quindi scegli Crea un nuovo Account AWS.

3. Inserisci le informazioni del tuo account, quindi scegli Verifica indirizzo email. Questo invierà un codice di verifica all'indirizzo email specificato.
4. Inserisci il codice di verifica, quindi scegli Verifica.
5. Inserisci una password sicura per il tuo utente root, confermala, quindi scegli Continua. AWSrichiede che la password soddisfi le seguenti condizioni:

   - Deve avere un minimo di 8 caratteri e un massimo di 128 caratteri.
   - Deve includere almeno tre dei seguenti tipi di caratteri: maiuscole, minuscole, numeri e i simboli ! @ # $ % ^ & * () <> [] {} | _+-=.
   - Non può coincidere con il nome o l'indirizzo e-mail dell'Account AWS.

6. Scegli Business o Personal. La differenza tra queste opzioni è rappresentata dalle informazioni che ti chiediamo. Entrambi i tipi di account hanno le stesse caratteristiche e funzioni.
7. Inserisci le tue informazioni aziendali o personali. Consulta i consigli nella sezione Prerequisiti relativi all'indirizzo e-mail e al numero di telefono.
8. Leggi e accetta il Contratto con il AWS cliente. Assicurati di leggere e comprendere i termini del Contratto con il AWS cliente.
9. Scegli Continue (Continua). A questo punto, riceverai un messaggio e-mail per confermare che il tuo Account AWS è pronto per l'uso. Puoi accedere al tuo nuovo account utilizzando l'indirizzo e-mail e la password che hai fornito durante la registrazione. Tuttavia, non puoi utilizzare alcun AWS servizio finché non avrai completato l'attivazione del tuo account.
10. Inserisci le informazioni sul tuo metodo di pagamento. Se desideri utilizzare un indirizzo diverso per la fatturazione, scegli Usa un nuovo indirizzo.
11. Scegli Verify and Continue (Verifica e continua).

12. Inserisci il codice del tuo paese o regione dall'elenco, quindi inserisci un numero di telefono al quale essere contattato nei prossimi minuti. Inserisci il codice CAPTCHA e invia.
13. Quando il sistema automatico ti contatta, inserisci il PIN che ricevi e poi invialo.
14. Seleziona il tuo AWS Support piano. Per una descrizione dei piani disponibili, consulta Confronta AWS Support i piani.
15. Scegli Iscrizione completa. Viene visualizzata una pagina di conferma che indica che il tuo account è in fase di attivazione.
16. Controlla la tua posta elettronica e la cartella spam per un messaggio e-mail che conferma l'attivazione dell'account. L'attivazione richiede in genere alcuni minuti, ma a volte può richiedere fino a 24 ore.

    Dopo aver ricevuto il messaggio di attivazione, avrai pieno accesso a tutti i AWS servizi.

> **Note**
>
> Se riscontri problemi con l'attivazione dell'account, consultathe section called “Problemi relativi alla creazione dell'account”.

Passaggio 2: attiva l'MFA per il tuo utente root

Ti consigliamo vivamente di attivare l'MFA per il tuo utente root. La MFA riduce drasticamente il rischio che qualcuno acceda al tuo account senza la tua autorizzazione.

1. Accedi alla AWS Management Console come proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email dell'Account AWS. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso con l'utente root, consulta Accedere AWS Management Console come utente root nella Guida per l'utente di AWSaccesso.
2. Attiva l'MFA per il tuo utente root.

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

Fase 3: Creare un utente amministratore

Poiché non è possibile limitare ciò che un utente root può fare, si consiglia vivamente di non utilizzare l'utente root per attività che non richiedano esplicitamente l'utente root. Assegna invece l'accesso amministrativo a un utente amministrativo in IAM Identity Center e accedi come tale utente amministrativo per eseguire le tue attività amministrative quotidiane.

Per istruzioni, consulta Configurare Account AWS l'accesso per un utente amministrativo di IAM Identity Center nella Guida per l'utente di IAM Identity Center.

Argomenti correlati

- Per informazioni sulla protezione delle credenziali dell'utente root, consulta Securing the credentials for the root user nella IAM User Guide.
- Per un elenco delle attività che richiedono l'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Utilizzo di Utente root dell'account AWS

> **Important**
>
> Chiunque disponga delle credenziali dell'utente root per il tuo Account AWS ha accesso illimitato a tutte le risorse nel tuo account, incluse le informazioni di fatturazione.

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWS e le risorse nell'account. Tale identità è detta utente root Account AWS ed è possibile accedervi 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 Tasks that require root user credentials (Attività che richiedono le credenziali dell'utente root) nella Guida per l'utente IAM.

Per evitare di utilizzare l'utente root per le attività quotidiane, scopri come configurare un utente amministrativo in AWS IAM Identity Center. Per ulteriori consigli sulla sicurezza degli utenti root, consulta le migliori pratiche per gli utenti root per il tuo Account AWS.

È possibile modificare o reimpostare la password dell'utente root e creare o eliminare le chiavi di accesso (ID delle chiavi di accesso e chiavi di accesso segrete) per l'utente root. Per informazioni sull'accesso con l'utente root, consulta Accedere AWS Management Console come utente root nella Guida per l'utente di AWS accesso.

Gestisci il tuoAccount AWS

Questa sezione include argomenti che descrivono come gestire i tuoiAccount AWS.

> **Note**
>
> Se il tuoAccount AWSè stato creato in India utilizzandoAmazon Internet Services Private Limited(AISPL), ci sono considerazioni aggiuntive. Per ulteriori informazioni, consulta Gestisci gli account in India.

Argomenti

Crea uno standalone Account AWS

Questo argomento descrive come creare una versione autonoma Account AWS non gestita da. AWS Organizations Se desideri creare un account che faccia parte di un'organizzazione gestita daAWS Organizations, consulta Creazione di un account membro nella tua organizzazione nella Guida per l'AWS Organizationsutente.

Queste istruzioni servono per creare un account Account AWS al di fuori dell'India. Per creare un account in India, vediCrea unAccount AWScon AISPL.

AWS Management Console

Per creare un Account AWS

1. Apri la home page di Amazon Web Services.
2. Scegli Crea un Account AWS.

> **Note**
>
> Se hai effettuato l'accesso di AWS recente, questa opzione potrebbe non essere disponibile. Scegli invece Accedi alla console. Quindi, se l'opzione Crea una nuova Account AWS immagine non è visibile, scegli prima Accedi a un altro account, quindi scegli Crea un nuovo Account AWS.

3. Inserisci le informazioni del tuo account, quindi scegli Verifica indirizzo email. Questo invierà un codice di verifica all'indirizzo email specificato.

> **Important**
>
> A causa della natura critica dell'utente root dell'account, ti consigliamo vivamente di utilizzare un indirizzo e-mail a cui possa accedere un gruppo, anziché solo un individuo. In questo modo, se la persona che si è registrata Account AWS lascia l'azienda, Account AWS può comunque essere utilizzato perché l'indirizzo e-mail è ancora accessibile.
> Se perdi l'accesso all'indirizzo e-mail associato aAccount AWS, non potrai recuperare l'accesso all'account in caso di smarrimento della password.

4. Inserisci il codice di verifica, quindi scegli Verifica.
5. Inserisci una password sicura per il tuo utente root, confermala, quindi scegli Continua. AWSrichiede che la password soddisfi le seguenti condizioni:
   - Deve avere un minimo di 8 caratteri e un massimo di 128 caratteri.
   - Deve includere almeno tre dei seguenti tipi di caratteri: maiuscole, minuscole, numeri e i simboli ! @ # $ % ^ & * () <> [] {} | _+-=.
   - Non può coincidere con il nome o l'indirizzo e-mail dell'Account AWS.
6. Scegli Business o Personal. Gli account personali e gli account aziendali hanno le stesse caratteristiche e funzioni.

7. Inserisci le tue informazioni aziendali o personali.

   > **Important**
   >
   > Per le aziendeAccount AWS, è consigliabile inserire:
   >
   > - Un numero di telefono aziendale anziché un numero di telefono personale.
   > - Un indirizzo e-mail con un nome di dominio appartenente alla società o all'organizzazione che utilizzerà l'account.
   >
   > La configurazione dell'utente root dell'account con un indirizzo e-mail individuale o un numero di telefono personale può rendere l'account non sicuro.

8. Leggi e accetta il Contratto con il AWScliente. Assicurati di leggere e comprendere i termini del Contratto con il AWS cliente.
9. Scegli Continua. A questo punto, riceverai un messaggio e-mail per confermare che il tuo Account AWS è pronto per l'uso. Puoi accedere al tuo nuovo account utilizzando l'indirizzo e-mail e la password che hai fornito durante la registrazione. Tuttavia, non puoi utilizzare alcun AWS servizio finché non avrai completato l'attivazione del tuo account.
10. Inserisci le informazioni sul metodo di pagamento, quindi scegli Verifica e continua. Se desideri utilizzare un indirizzo di fatturazione diverso per i dati di AWS fatturazione, scegli Usa un nuovo indirizzo.

    Non puoi procedere con la procedura di registrazione finché non aggiungi un metodo di pagamento valido.
11. Inserisci il codice del tuo paese o regione dall'elenco, quindi inserisci un numero di telefono a cui potrai essere contattato nei prossimi minuti.
12. Inserisci il codice visualizzato nel CAPTCHA, quindi invia.
13. Quando il sistema automatico ti contatta, inserisci il PIN che ricevi e poi invialo.
14. Seleziona uno dei AWS Support piani disponibili. Per una descrizione dei piani di Support disponibili e dei relativi vantaggi, consulta Confronta AWS Support i piani.
15. Scegli Iscrizione completa. Viene visualizzata una pagina di conferma che indica che il tuo account è in fase di attivazione.

16. Controlla la tua posta elettronica e la cartella spam per un messaggio e-mail che conferma l'attivazione dell'account. L'attivazione richiede in genere alcuni minuti, ma a volte può richiedere fino a 24 ore.

    Dopo aver ricevuto il messaggio di attivazione, avrai pieno accesso a tutti i AWS servizi.

AWS CLI & SDKs

È possibile creare account membro in un'organizzazione gestita AWS Organizations eseguendo l'CreateAccountoperazione mentre si è connessi all'account di gestione dell'organizzazione.

Non puoi creare un account autonomo Account AWS al di fuori di un'organizzazione utilizzando un'operazione AWS Command Line Interface (AWS CLI) o AWS API.

Visualizza gli Account AWS identificatori

AWS assegna a ciascuno i seguenti identificatori univoci: Account AWS

Account AWS ID

Un numero di 12 cifre, ad esempio 012345678901, che identifica in modo univoco un. Account AWSMolte AWS risorse includono l'ID dell'account nei rispettivi Amazon Resource Names (ARN). La parte dell'ID account distingue le risorse in un account dalle risorse in un altro account. Se sei un utente AWS Identity and Access Management (IAM), puoi accedere AWS Management Console utilizzando l'ID dell'account o l'alias dell'account. Sebbene gli ID account, come qualsiasi informazione identificativa, debbano essere utilizzati e condivisi con attenzione, non sono considerati informazioni segrete, sensibili o riservate.

ID utente canonico

Un identificatore alfanumerico, ad esempio una forma `79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be` offuscata dell'ID. Account AWS Puoi utilizzare questo ID per identificare e concedere Account AWS l'accesso tra account diversi a bucket e oggetti utilizzando Amazon Simple Storage Service (Amazon S3). Puoi recuperare l'ID utente canonico per te Account AWS come utente root o utente IAM.

È necessario autenticarsi con AWS per visualizzare questi identificatori.

> **Warning**
>
> Non fornite AWS le vostre credenziali (incluse password e chiavi di accesso) a terze parti che necessitano dei vostri Account AWS identificatori per condividere risorse con voi. AWS In questo modo daresti loro lo stesso accesso a Account AWS quello che hai tu.

Trova il tuo Account AWS ID

Puoi trovare l' Account AWS ID utilizzando il AWS Management Console o il AWS Command Line Interface (AWS CLI). Nella console, la posizione dell'ID dell'account dipende dal fatto che tu abbia effettuato l'accesso come utente root o come utente IAM. L'ID dell'account è lo stesso indipendentemente dal fatto che tu abbia effettuato l'accesso come utente root o come utente IAM.

Come trovare l'ID del tuo account come utente root

AWS Management Console

Per trovare il tuo Account AWS ID dopo aver effettuato l'accesso come utente root

> **Autorizzazioni minime**
>
> Per eseguire le seguenti operazioni, devi disporre come minimo delle seguenti autorizzazioni IAM:
>
> - Quando accedi come utente root, non hai bisogno di alcuna autorizzazione IAM.

1. Nella barra di navigazione in alto a destra, scegli il nome o il numero del tuo account, quindi scegli Credenziali di sicurezza.

   > **Tip**
   >
   > Se non vedi l'opzione Credenziali di sicurezza, potresti aver effettuato l'accesso come utente federato con un ruolo IAM, anziché come utente IAM. In questo caso, cerca la voce Account e il numero ID dell'account accanto ad essa.

2. Nella sezione Dettagli dell'account, il numero di conto viene visualizzato accanto a Account AWS ID.

AWS CLI & SDKs

Per trovare il tuo Account AWS ID, utilizza il AWS CLI

> **Autorizzazioni minime**
>
> Per eseguire le seguenti operazioni, devi disporre come minimo delle seguenti autorizzazioni IAM:
>
> - Quando esegui il comando come utente root, non hai bisogno di alcuna autorizzazione IAM.

Utilizza il comando get-caller-identity come riportato di seguito.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Trova l'ID del tuo account come utente IAM

AWS Management Console

Per trovare il tuo Account AWS ID dopo aver effettuato l'accesso come utente IAM

> **Autorizzazioni minime**
>
> Per eseguire le seguenti operazioni, devi disporre come minimo delle seguenti autorizzazioni IAM:
>
> - `account:GetAccountInformation`

1. Seleziona il nome utente in alto a destra nella barra di navigazione e scegli Security credentials (Credenziali di sicurezza).

> **Tip**
>
> Se non vedi l'opzione Security credentials, potresti aver effettuato l'accesso come utente federato con un ruolo IAM, anziché come utente IAM. In questo caso, cerca la voce Account e il numero ID dell'account accanto ad essa.

2. Nella parte superiore della pagina, sotto Dettagli dell'account, il numero di conto viene visualizzato accanto a Account AWS ID.

AWS CLI & SDKs

Per trovare il tuo Account AWS ID, utilizza il AWS CLI

> **Autorizzazioni minime**
>
> Per eseguire le seguenti operazioni, devi disporre come minimo delle seguenti autorizzazioni IAM:
>
> - Quando esegui il comando come utente o ruolo IAM, devi avere:
>   - `sts:GetCallerIdentity`

Utilizza il comando get-caller-identity come riportato di seguito.

```
$ aws sts get-caller-identity \
    --query Account \
    --output text
123456789012
```

Trova l'ID utente canonico per il tuo Account AWS

Puoi trovare l'ID utente canonico da Account AWS utilizzare o il. AWS Management Console AWS CLIL'ID utente canonico di an Account AWS è specifico per quell'account. Puoi recuperare l'ID utente canonico per il tuo Account AWS utente root, un utente federato o un utente IAM.

Trova l'ID canonico come utente root o utente IAM

AWS Management Console

Per trovare l'ID utente canonico per il tuo account quando accedi alla console come utente root o utente IAM

> **Autorizzazioni minime**
>
> Per eseguire le seguenti operazioni, devi disporre come minimo delle seguenti autorizzazioni IAM:
>
> - Quando esegui il comando come utente root, non hai bisogno di alcuna autorizzazione IAM.
> - Quando accedi come utente IAM, devi avere:
>   - `account:GetAccountInformation`

1. Accedi AWS Management Console come utente root o utente IAM.
2. Nella barra di navigazione in alto a destra, scegli il nome o il numero del tuo account, quindi scegli Credenziali di sicurezza.

   > **Tip**
   >
   > Se non vedi l'opzione Credenziali di sicurezza, potresti aver effettuato l'accesso come utente federato con un ruolo IAM, anziché come utente IAM. In questo caso, cerca la voce Account e il numero ID dell'account accanto ad essa.

3. Nella sezione Dettagli dell'account, l'ID utente canonico viene visualizzato accanto all'ID utente canonico. Puoi usare il tuo ID utente canonico per configurare le liste di controllo degli accessi (ACL) di Amazon S3.

AWS CLI & SDKs

Per trovare l'ID utente canonico, utilizza il AWS CLI

Lo stesso AWS CLI comando API funziona per gli Utente root dell'account AWSutenti IAM o i ruoli IAM.

Usa il comando list-buckets come segue.

```
$ aws s3api list-buckets \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Trova l'ID canonico come utente federato con un ruolo IAM

AWS Management Console

Per trovare l'ID canonico del tuo account quando accedi alla console come utente federato con un ruolo IAM

> **Autorizzazioni minime**
>
> - È necessario disporre dell'autorizzazione per elencare e visualizzare un bucket Amazon S3.

1. Accedi AWS Management Console come utente federato con un ruolo IAM.
2. Nella console Amazon S3, scegli il nome di un bucket per visualizzare i dettagli relativi a un bucket.
3. Scegli la scheda Permissions (Autorizzazioni).
4. Nella sezione Elenco di controllo degli accessi, sotto Bucket owner, viene visualizzato l'ID canonico del tuo. Account AWS

AWS CLI & SDKs

Per trovare l'ID utente canonico, utilizza il AWS CLI

Lo stesso AWS CLI comando API funziona per gli Utente root dell'account AWSutenti IAM o i ruoli IAM.

Usa il comando list-buckets come segue.

```
$ aws s3api list-buckets \
    --query Owner.ID \
```

```
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Aggiorna il Account AWS nome, l'indirizzo email o la password per l'utente root

Per modificare Account AWS il nome o modificare la password o l'indirizzo e-mail dell'utente root, procedi nel seguente modo. Questo indirizzo e-mail e la password sono le credenziali che utilizzi per accedere come. Utente root dell'account AWS

> **Note**
>
> Le modifiche a an Account AWS possono richiedere fino a quattro ore per propagarsi ovunque.

AWS Management Console

Per modificare il Account AWS nome, la password dell'utente root o l'indirizzo e-mail dell'utente root

> **Autorizzazioni minime**
>
> Per eseguire le seguenti operazioni, devi disporre come minimo delle seguenti autorizzazioni IAM:
>
> - È necessario accedere come Utente root dell'account AWS, il che non richiede autorizzazioni IAM aggiuntive. Non è possibile eseguire questi passaggi come utente o ruolo IAM.

1. Usa Account AWS il tuo indirizzo email e la password per accedere AWS Management Consolecome tuoi Utente root dell'account AWS.
2. Nell'angolo in alto a destra della console, scegli il nome o il numero dell'account, quindi Account.
3. Nella pagina Account, accanto a Impostazioni account, scegli Modifica. Ti viene richiesto di effettuare nuovamente l'autenticazione per motivi di sicurezza.

> **Note**
>
> Se non vedi l'opzione Modifica, è probabile che tu non abbia effettuato l'accesso come utente root dell'account. Non è possibile modificare le impostazioni dell'account dopo aver effettuato l'accesso come utente o ruolo IAM.

4. Nella pagina Aggiorna le impostazioni dell'account, scegli Modifica accanto al campo che desideri aggiornare.

   a. Per Nome: nella pagina Aggiorna il nome dell'account, in Nuovo nome account, inserisci il nuovo nome dell'account, quindi scegli Salva modifiche.

   > **Note**
   >
   > Se non riesci a modificare il Account AWS nome, controlla se esiste una policy di controllo del servizio (SCP) AWS Organizations che limita l'accesso `account` o è impostata per negare l'azione. `iam:UpdateAccountName`

   b. Per e-mail: nella pagina Aggiorna il tuo indirizzo e-mail, compila i campi per Nuovo indirizzo e-mail, Conferma nuovo indirizzo e-mail e conferma la password corrente. Quindi, scegli Save changes (Salva modifiche). Un codice di verifica viene inviato al tuo nuovo indirizzo email dano`-reply@verify.signin.aws`. Nella pagina Verifica il nuovo indirizzo email, sotto Codice di verifica, inserisci il codice che hai ricevuto via email, quindi scegli Salva modifiche.

   > **Note**
   >
   > L'arrivo del codice di verifica può richiedere fino a 5 minuti. Se non vedi l'email nella tua casella di posta, controlla le cartelle spam e posta indesiderata.

   c. Per la password: nella pagina Aggiorna la password, compila i campi Password attuale, Nuova password e Conferma nuova password. Quindi, scegli Save changes (Salva modifiche). Per ulteriori indicazioni, comprese le migliori pratiche per l'impostazione delle password degli utenti root, consulta Change the password for the Utente root dell'account AWS nella IAM User Guide.

5. Dopo avere apportato tutte le modifiche, scegli Done (Fine).

AWS CLI & SDKs

Questa attività non è supportata in AWS CLI o da un'operazione API di uno degli AWS SDK. È possibile eseguire questa attività solo utilizzando. AWS Management Console

Comprendere le modalità operative delle API

Le operazioni API che funzionano con unAccount AWSgli attributi di funzionano sempre in una delle due modalità operative:

- Contesto autonomo— questa modalità viene utilizzata quando un utente o un ruolo in un account accede o modifica un attributo di account nelstesso account. La modalità contesto standalone viene utilizzata automaticamente quando siDon'tincludere il kit`AccountId`parametro quando si chiama uno degli Account ManagementAWS CLIoAWSOperazioni SDK.
- Contesto delle Organizations— questa modalità viene utilizzata quando un utente o un ruolo in un account in un'organizzazione accede o modifica un attributo di account in un account membro diverso nella stessa organizzazione. La modalità contesto dell'organizzazione viene utilizzata automaticamente quando sifareincludere il kit`AccountId`parametro quando si chiama uno degli Account ManagementAWS CLIoAWSFunzionamento SDK. È possibile richiamare le operazioni in questa modalità solo dall'account di gestione dell'organizzazione o dall'account amministratore delegato per Gestione account.

LaAWS CLIeAWSLe operazioni SDK possono funzionare sia nel contesto autonomo che in quello dell'organizzazione.

- Se tuDon'tincludere il kit`AccountId`parametro, quindi l'operazione viene eseguita nel contesto autonomo e applica automaticamente la richiesta all'account utilizzato per effettuare la richiesta. Questo è vero se l'account è membro di un'organizzazione.
- Se includi il file`AccountId`parametro, quindi l'operazione viene eseguita nel contesto dell'organizzazione e l'operazione funziona sull'account Organizations specificato.
  - Se l'account che chiama l'operazione è l'account di gestione o l'account amministratore delegato per il servizio Gestione account, è possibile specificare qualsiasi account membro di tale organizzazione nella casella`AccountId`parametro per aggiornare l'account specificato.
  - L'unico account di un'organizzazione che può chiamare una delle operazioni di contatto alternative e specificare il proprio numero di conto nella`AccountId`parametro è l'account

specificato comeaccount amministratore delegatoper il servizio di gestione degli account. Qualsiasi altro account, incluso l'account di gestione, riceve un`AccessDenied`eccezione.

- Se esegui un'operazione in modalità standalone, devi avere il permesso di eseguire l'operazione con una policy IAM che includa un`Resource`elemento di uno dei due`"*"`per consentire tutte le risorse o unARN che utilizza la sintassi per un account autonomo.
- Se esegui un'operazione in modalità organizzazioni, devi avere il permesso di eseguire l'operazione con una policy IAM che includa un`Resource`elemento di uno dei due`"*"`per consentire tutte le risorse o unARN che utilizza la sintassi per un account membro di un'organizzazione.

Concessione delle autorizzazioni per l'aggiornamento degli attributi

Come con la maggior parteAWSoperazioni, concedi le autorizzazioni per aggiungere, aggiornare o eliminare gli attributi dell'account perAccount AWSutilizzandoPolicy delle autorizzazioni IAM. Quando alleghi una policy di autorizzazione IAM (utente o ruolo) (utente o ruolo) (utente o ruolo), specifica le operazioni autorizzate per l'entità (utente o ruolo) (utente o ruolo), nonché le condizioni in cui possono essere eseguite.

Di seguito sono riportate alcune considerazioni specifiche sulla gestione degli account per la creazione di una politica di autorizzazioni.

Formato Amazon Resource Name perAccount AWS

- LaAmazon Resource Name (ARN)per unAccount AWSche puoi includere nel`resource`elemento di una dichiarazione politica è costruito in modo diverso a seconda che l'account a cui si desidera fare riferimento sia un account autonomo o un account appartenente a un'organizzazione. Consulta la sezione precedenteComprendere le modalità operative delle API.
  - Un ARN dell'account per un account autonomo:

    ```
    arn:aws:account::{AccountId}:account
    ```

    È necessario utilizzare questo formato quando si esegue un'operazione sugli attributi dell'account in modalità standalone escludendo il`AccountID`Parametro .
  - Un ARN account per un account membro di un'organizzazione:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

È necessario utilizzare questo formato quando si esegue un'operazione di attributi di account in modalità organizzazione includendo il`AccountID`Parametro .

Chiavi di contesto per le policy IAM

Il servizio di gestione degli account fornisce anche diversiChiavi di condizione specifiche per il servizio Account Managementche forniscono un controllo dettagliato sulle autorizzazioni concesse.

`account:AccountResourceOrgPaths`

La chiave di contesto`account:AccountResourceOrgPaths`consente di specificare un percorso attraverso la gerarchia dell'organizzazione verso una specifica unità organizzativa (OU). Solo gli account membro contenuti in tale unità organizzativa soddisfano la condizione. Il seguente frammento di codice di esempio limita l'applicazione del criterio solo agli account che si trovano in una delle due unità organizzative specificate.

Poiché`account:AccountResourceOrgPaths`è un tipo di stringa multivalore, è necessario utilizzare il`ForAnyValue`o`ForAllValues`operatori di stringa multivalore. Inoltre, si noti che il prefisso sulla chiave condizionale è`account`, anche se si fa riferimento a percorsi verso le unità organizzative in un'organizzazione.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgPaths": [
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
            "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
        ]
    }
}
```

`account:AccountResourceOrgTags`

La chiave di contesto`account:AccountResourceOrgTags`consente di fare riferimento ai tag che possono essere allegati a un account in un'organizzazione. Un tag è una coppia di stringhe chiave/valore che puoi utilizzare per classificare ed etichettare le risorse nel tuo account. Per ulteriori informazioni sul tagging, consultaEditor di tagnellaAWS Resource GroupsGuida per l'utente di. Per informazioni sull'utilizzo di tag come parte di una strategia di controllo degli accessi basata sugli

attributi, consultaChe cos'è ABAC per?AWSnellaIAM User Guide. Il seguente frammento di codice di esempio limita l'applicazione del criterio solo agli account di un'organizzazione che hanno il tag con la chiave.`projecte` un valore di entrambi`blue`e`red`.

Poiché`account:AccountResourceOrgTags`è un tipo di stringa multivalore, è necessario utilizzare il`ForAnyValue`e`ForAllValues`operatori di stringa multivalore. Inoltre, si noti che il prefisso sulla chiave condizionale è`account`, anche se fai riferimento ai tag sull'account membro di un'organizzazione.

```
"Condition": {
    "ForAnyValue:StringLike": {
        "account:AccountResourceOrgTags/project": [
            "blue",
            "red"
        ]
    }
}
```

> **Note**
>
> È possibile allegare tag solo a un account di un'organizzazione. Non è possibile allegare tag a uno standaloneAccount AWS.

Aggiorna il tuoAccount AWSinformazioni di contatto

È possibile memorizzare le informazioni di contatto relative alcontatto dell'account principaleper il tuoAccount AWS. Puoi anche aggiungere o modificare le informazioni di contatto per quanto seguecontatti di account alternativi:

- Fatturazione— Il contatto alternativo per la fatturazione riceverà notifiche relative alla fatturazione, come le notifiche sulla disponibilità delle fatture.
- Operazioni— Il contatto per le operazioni alternative riceverà notifiche relative alle operazioni.
- Sicurezza— Il contatto di sicurezza alternativo riceverà notifiche relative alla sicurezza, comprese le notifiche dalAWSSquadra contro gli abusi.

Argomenti

- Aggiorna i contatti alternativi per il tuo Account AWS

- Aggiorna il contatto principale per il tuo Account AWS

Aggiorna i contatti alternativi per il tuo Account AWS

I contatti alternativi consentono di AWS contattare fino a tre contatti alternativi associati all'account. Un contatto alternativo non deve necessariamente essere una persona specifica. È invece possibile aggiungere una lista di distribuzione e-mail se si dispone di un team per la gestione di problemi relativi alla fatturazione, alle operazioni e alla sicurezza. Questi si aggiungono all'indirizzo e-mail associato all'utente root dell'account. Il contatto principale dell'account continuerà a ricevere tutte le comunicazioni e-mail inviate all'indirizzo e-mail dell'account root.

È possibile specificare solo uno dei seguenti tipi di contatto associati a un account.

- Contatto di fatturazione
- Contatto operativo
- Contatto di sicurezza

Puoi aggiungere o modificare contatti alternativi in modo diverso, a seconda che gli account siano autonomi o facciano parte di un'organizzazione:

- Autonomo Account AWS: Account AWS se non sei associato a un'organizzazione, puoi aggiornare i tuoi contatti alternativi utilizzando la Console di AWS gestione o tramite AWS CLI e SDK. Per informazioni su come eseguire questa operazione, consulta Aggiornare i contatti alternativi autonomi. Account AWS
- Account AWS all'interno di un'organizzazione: per gli account membro che fanno parte di un' AWS organizzazione, un utente dell'account di gestione o dell'account amministratore delegato può aggiornare centralmente qualsiasi account membro dell'organizzazione dalla AWS Organizations console o in modo programmatico tramite la CLI AWS e gli SDK. Per informazioni su come eseguire questa operazione, consulta Aggiornare i contatti Account AWS alternativi nell'organizzazione.

Argomenti

- Requisiti relativi al numero di telefono e all'indirizzo e-mail
- Aggiorna i contatti alternativi per renderli autonomi Account AWS
- Aggiorna i contatti alternativi per tutti i Account AWS membri dell'organizzazione

- account: chiave AlternateContactTypes contestuale

Requisiti relativi al numero di telefono e all'indirizzo e-mail

Prima di procedere con l'aggiornamento delle informazioni di contatto alternative del tuo account, ti consigliamo di esaminare innanzitutto i seguenti requisiti per l'immissione di numeri di telefono e indirizzi e-mail.

- I numeri di telefono possono contenere solo numeri, spazi bianchi e i seguenti caratteri:». `+-()`
- Gli indirizzi e-mail possono contenere fino a 254 caratteri e includere i seguenti caratteri speciali nella parte locale dell'indirizzo e-mail oltre a quelli alfanumerici standard: ». `+=.#|!&-_`

Aggiorna i contatti alternativi per renderli autonomi Account AWS

Per aggiungere o modificare i contatti alternativi per una versione autonoma Account AWS, effettuate le operazioni descritte nella procedura seguente. La AWS Management Console procedura seguente funziona sempre solo in un contesto autonomo. È possibile utilizzare il AWS Management Console per accedere o modificare solo i contatti alternativi dell'account utilizzato per chiamare l'operazione.

AWS Management Console

Per aggiungere o modificare i contatti alternativi per un account indipendente Account AWS

> **Autorizzazioni minime**
>
> Per eseguire le seguenti operazioni, devi disporre come minimo delle seguenti autorizzazioni IAM:
>
> - `account:GetAlternateContact`(per visualizzare i dettagli di contatto alternativi)
> - `account:PutAlternateContact`(per impostare o aggiornare un contatto alternativo)
> - `account:DeleteAlternateContact`(per eliminare un contatto alternativo)

1. Accedi AWS Management Consolecome utente o ruolo IAM con le autorizzazioni minime.
2. Scegli il nome del tuo account in alto a destra nella finestra, quindi scegli Account.

3. Nella pagina Account, scorri verso il basso fino a Contatti alternativi e, a destra del titolo, scegli Modifica.

> **Note**
>
> Se non vedi l'opzione Modifica, è probabile che tu non abbia effettuato l'accesso come utente root del tuo account o come utente che dispone delle autorizzazioni minime specificate sopra.

4. Modifica i valori nei campi disponibili.

> **Important**
>
> Per le aziende Account AWS, è consigliabile inserire il numero di telefono e l'indirizzo e-mail dell'azienda anziché quelli di una persona fisica.

5. Dopo aver apportato tutte le modifiche, scegli Aggiorna.

AWS CLI & SDKs

Puoi recuperare, aggiornare o eliminare le informazioni di contatto alternative utilizzando AWS CLI i seguenti comandi o le relative operazioni equivalenti all' AWS SDK:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Note**
>
> - Per eseguire queste operazioni dall'account di gestione o da un account amministratore delegato di un'organizzazione utilizzando gli account dei membri, è necessario abilitare l'accesso affidabile per il servizio Account.

Autorizzazioni minime

Per ogni operazione, è necessario disporre dell'autorizzazione corrispondente a tale operazione:

- `GetAlternateContact`(per visualizzare i dettagli di contatto alternativi)
- `PutAlternateContact`(per impostare o aggiornare un contatto alternativo)
- `DeleteAlternateContact`(per eliminare un contatto alternativo)

Se utilizzi queste autorizzazioni individuali, puoi concedere ad alcuni utenti la possibilità di leggere solo le informazioni di contatto e concedere ad altri la possibilità di leggere e scrivere.

Example

L'esempio seguente recupera l'attuale contatto alternativo di Billing per l'account del chiamante.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

L'esempio seguente imposta un nuovo contatto alternativo Operations per l'account del chiamante.

```
$ aws account put-alternate-contact \
    --alternate-contact-type=OPERATIONS \
```

```
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Se ha esito positivo, questo comando non produrrà alcun output.

Example

> **Note**
>
> Se si eseguono più `PutAlternateContact` operazioni sullo stesso Account AWS tipo di contatto, la prima aggiunge il nuovo contatto e tutte le chiamate successive allo stesso Account AWS tipo di contatto aggiornano il contatto esistente.

Example

L'esempio seguente elimina il contatto alternativo di sicurezza per l'account del chiamante.

```
$ aws account delete-alternate-contact \
    --alternate-contact-type=SECURITY
```

Se ha esito positivo, questo comando non produrrà alcun output.

> **Note**
>
> Se si tenta di eliminare lo stesso contatto più di una volta, il primo riesce inavvertitamente. Tutti i tentativi successivi generano un'`ResourceNotFound`eccezione.

Aggiorna i contatti alternativi per tutti i Account AWS membri dell'organizzazione

Per aggiungere o modificare i dati di contatto alternativi per qualsiasi Account AWS membro dell'organizzazione, procedi nel seguente modo.

Requisiti

Per aggiornare i contatti alternativi con la AWS Organizations console, è necessario eseguire alcune impostazioni preliminari:

- L'organizzazione deve abilitare tutte le funzionalità per gestire le impostazioni degli account dei membri. Ciò consente il controllo amministrativo sugli account dei membri. Questa impostazione è predefinita al momento della creazione dell'organizzazione. Se la tua organizzazione è impostata solo sulla fatturazione consolidata e desideri abilitare tutte le funzionalità, vedi Abilitazione di tutte le funzionalità nell'organizzazione.
- È necessario abilitare l'accesso affidabile per il servizio di gestione degli AWS account. Per configurarlo, vedi Abilitazione dell'accesso affidabile per la gestione AWS dell'account.

> **Note**
>
> Le politiche AWS Organizations `AWSOrganizationsReadOnlyAccess` gestite `AWSOrganizationsFullAccess` sono state aggiornate per fornire l'autorizzazione ad accedere alle API di gestione dell' AWS account in modo da poter accedere ai dati dell'account dalla AWS Organizations console. Per visualizzare le policy gestite aggiornate, vedere Updates to Organizations AWS managed policy.

AWS Management Console

Per aggiungere o modificare i contatti alternativi per tutti i membri Account AWS dell'organizzazione

1. Accedi alla AWS Organizations console con le credenziali dell'account di gestione dell'organizzazione.
2. Da Account AWS, seleziona l'account che desideri aggiornare.
3. Scegli Informazioni di contatto e, in Contatti alternativi, individua il tipo di contatto: contatto di fatturazione, contatto di sicurezza o contatto operativo.
4. Per aggiungere un nuovo contatto, seleziona Aggiungi o per aggiornare un contatto esistente seleziona Modifica.
5. Modifica i valori nei campi disponibili.

> **Important**
>
> Per le aziende Account AWS, è consigliabile inserire il numero di telefono e l'indirizzo e-mail dell'azienda anziché uno appartenente a una persona.

6. Dopo aver apportato tutte le modifiche, scegli Aggiorna.

AWS CLI & SDKs

Puoi recuperare, aggiornare o eliminare le informazioni di contatto alternative utilizzando AWS CLI i seguenti comandi o le relative operazioni equivalenti all' AWS SDK:

- GetAlternateContact
- PutAlternateContact
- DeleteAlternateContact

> **Note**
>
> - Per eseguire queste operazioni dall'account di gestione o da un account amministratore delegato di un'organizzazione utilizzando gli account dei membri, è necessario abilitare l'accesso affidabile per il servizio Account.
> - Non puoi accedere a un account in un'organizzazione diversa da quella che stai utilizzando per chiamare l'operazione.

> **Autorizzazioni minime**
>
> Per ogni operazione, devi disporre dell'autorizzazione corrispondente a tale operazione:
>
> - `GetAlternateContact`(per visualizzare i dettagli di contatto alternativi)
> - `PutAlternateContact`(per impostare o aggiornare un contatto alternativo)
> - `DeleteAlternateContact`(per eliminare un contatto alternativo)
>
> Se utilizzi queste autorizzazioni individuali, puoi concedere ad alcuni utenti la possibilità di leggere solo le informazioni di contatto e concedere ad altri la possibilità di leggere e scrivere.

Example

L'esempio seguente recupera l'attuale contatto alternativo di Billing per l'account del chiamante in un'organizzazione. Le credenziali utilizzate devono provenire dall'account di gestione dell'organizzazione o dall'account amministratore delegato di Account Management.

```
$ aws account get-alternate-contact \
    --alternate-contact-type=BILLING \
    --account-id 123456789012
{
    "AlternateContact": {
        "AlternateContactType": "BILLING",
        "EmailAddress": "saanvi.sarkar@amazon.com",
        "Name": "Saanvi Sarkar",
        "PhoneNumber": "+1(206)555-0123",
        "Title": "CFO"
    }
}
```

Example

L'esempio seguente imposta il contatto alternativo Operations per l'account membro specificato in un'organizzazione. Le credenziali utilizzate devono provenire dall'account di gestione dell'organizzazione o dall'account amministratore delegato di Account Management.

```
$ aws account put-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=OPERATIONS \
    --email-address=mateo_jackson@amazon.com \
    --name="Mateo Jackson" \
    --phone-number="+1(206)555-1234" \
    --title="Operations Manager"
```

Se ha esito positivo, questo comando non produrrà alcun output.

> **Note**
>
> Se si eseguono più `PutAlternateContact` operazioni sullo stesso Account AWS tipo di contatto, la prima aggiunge il nuovo contatto e tutte le chiamate successive allo stesso Account AWS tipo di contatto aggiornano il contatto esistente.

Example

L'esempio seguente elimina il contatto alternativo di sicurezza per l'account membro specificato in un'organizzazione. Le credenziali utilizzate devono provenire dall'account di gestione dell'organizzazione o dall'account amministratore delegato di Account Management.

```
$ aws account delete-alternate-contact \
    --account-id 123456789012 \
    --alternate-contact-type=SECURITY
```

Se ha esito positivo, questo comando non produrrà alcun output.

Example

> **Note**
>
> Se si tenta di eliminare lo stesso contatto più di una volta, il primo riesce inavvertitamente. Tutti i tentativi successivi generano un'`ResourceNotFound`eccezione.

account: chiave AlternateContactTypes contestuale

Puoi utilizzare la chiave di contesto `account:AlternateContactTypes` per specificare quale dei tre tipi di fatturazione è consentito (o negato) dalla policy IAM. Ad esempio, il seguente esempio di policy di autorizzazione IAM utilizza questa chiave di condizione per consentire ai responsabili collegati di recuperare, ma non modificare, solo il contatto `BILLING` alternativo per un account specifico in un'organizzazione.

Poiché `account:AlternateContactTypes` si tratta di un tipo di stringa multivalore, è necessario utilizzare gli operatori di stringa o multivalore. `ForAnyValueForAllValues`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "account:GetAlternateContact",
            "Resource": [
```

```
                "arn:aws:account::123456789012:account/o-aa111bb222/111111111111"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "account:AlternateContactTypes": [
                        "BILLING"
                    ]
                }
            }
        }
    ]
}
```

Aggiorna il contatto principale per il tuo Account AWS

Puoi aggiornare le informazioni di contatto principali associate al tuo account, inclusi il nome completo del contatto, la ragione sociale, l'indirizzo postale, il numero di telefono e l'indirizzo del sito web.

Puoi modificare il contatto principale dell'account in modo diverso, a seconda che gli account siano autonomi o facciano parte di un'organizzazione:

- Autonomo Account AWS: Account AWS se non sei associato a un'organizzazione, puoi aggiornare il contatto principale del tuo account utilizzando la console di AWS gestione o tramite AWS CLI e SDK. Per informazioni su come eseguire questa operazione, consulta Aggiornare il contatto principale autonomo Account AWS.
- Account AWSall'interno di un'organizzazione: per gli account membro che fanno parte di un'AWSorganizzazione, un utente dell'account di gestione o dell'account amministratore delegato può aggiornare centralmente qualsiasi account membro dell'organizzazione dalla AWS Organizations console o in modo programmatico tramite la CLI AWS e gli SDK. Per informazioni su come eseguire questa operazione, consulta Aggiornare il contatto Account AWS principale nell'organizzazione.

Argomenti

Requisiti relativi al numero di telefono e all'indirizzo e-mail

Prima di procedere con l'aggiornamento delle informazioni di contatto principali del tuo account, ti consigliamo di esaminare innanzitutto i seguenti requisiti per l'immissione di numeri di telefono e indirizzi e-mail.

- I numeri di telefono possono contenere solo numeri, spazi bianchi e i seguenti caratteri:»». +-( )
- I numeri di telefono devono iniziare con un + prefisso internazionale e non devono avere zeri iniziali o spazi aggiuntivi dopo il prefisso internazionale. Ad esempio, +1 (USA/Canada) o +44 (Regno Unito).
- I numeri di telefono devono includere i trattini "-" tra il prefisso, il prefisso di scambio e il prefisso locale. Ad esempio, +1 202-555-0179.

> **Note**
>
> I numeri di telefono immessi senza trattini possono comportare l'impossibilità di ricevere chiamate durante il processo di verifica del numero di telefono durante la reimpostazione di un dispositivo MFA per l'utente root. Per ulteriori informazioni, vedi Come posso resettare il mio dispositivo MFA con account utente AWS root? .

- Per motivi di sicurezza, i numeri di telefono devono essere in grado di ricevere SMS daAWS. I numeri verdi non saranno accettati poiché la maggior parte non supporta gli SMS.
- Per le aziendeAccount AWS, è consigliabile inserire il numero di telefono e l'indirizzo e-mail dell'azienda anziché quelli di una persona fisica. La configurazione dell'utente root dell'account con l'indirizzo e-mail o il numero di telefono di una persona può rendere difficile il ripristino dell'account se quella persona lascia l'azienda.

Aggiorna il contatto principale per uno standalone Account AWS

Per modificare i dati di contatto principali per un account indipendenteAccount AWS, procedi nel seguente modo. La AWS Management Console procedura seguente funziona sempre solo in un contesto autonomo. È possibile utilizzare il AWS Management Console per accedere o modificare solo le informazioni di contatto principali dell'account utilizzato per chiamare l'operazione.

AWS Management Console

Per modificare il contatto principale in modo autonomo Account AWS

> **Autorizzazioni minime**
>
> Per eseguire le seguenti operazioni, devi disporre come minimo delle seguenti autorizzazioni IAM:
>
> - `account:GetContactInformation`(per visualizzare i dettagli di contatto principali)
> - `account:PutContactInformation`(per aggiornare i dati di contatto principali)

1. Accedi AWS Management Consolecome utente o ruolo IAM con le autorizzazioni minime.
2. Scegli il nome del tuo account in alto a destra nella finestra, quindi scegli Account.
3. Scorri verso il basso fino alla sezione Informazioni di contatto e accanto ad essa scegli Modifica.
4. Modifica i valori nei campi disponibili.
5. Dopo aver apportato tutte le modifiche, scegli Aggiorna.

AWS CLI & SDKs

Puoi recuperare, aggiornare o eliminare le informazioni di contatto principali utilizzando AWS CLI i seguenti comandi o le relative operazioni equivalenti all'AWSSDK:

- GetContactInformation
- PutContactInformation

> **Note**
>
> - Per eseguire queste operazioni dall'account di gestione o da un account amministratore delegato di un'organizzazione utilizzando gli account dei membri, è necessario abilitare l'accesso affidabile per il servizio Account.

Autorizzazioni minime

Per ogni operazione, è necessario disporre dell'autorizzazione corrispondente a tale operazione:

- `account:GetContactInformation`
- `account:PutContactInformation`

Se utilizzi queste autorizzazioni individuali, puoi concedere ad alcuni utenti la possibilità di leggere solo le informazioni di contatto e concedere ad altri la possibilità di leggere e scrivere.

Example

L'esempio seguente recupera le informazioni di contatto principali correnti per l'account del chiamante.

```
$ aws account get-contact-information
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

L'esempio seguente imposta nuove informazioni di contatto principali per l'account del chiamante.

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
 Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
```

```
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Se ha esito positivo, questo comando non produrrà alcun output.

Aggiorna il contatto principale per qualsiasi membro Account AWS della tua organizzazione

Per modificare i dati di contatto principali Account AWS di qualsiasi membro dell'organizzazione, procedi nel seguente modo.

Requisiti aggiuntivi

Per aggiornare il contatto principale con la AWS Organizations console, è necessario eseguire alcune impostazioni preliminari:

- L'organizzazione deve abilitare tutte le funzionalità per gestire le impostazioni degli account dei membri. Ciò consente il controllo amministrativo sugli account dei membri. Questa impostazione è predefinita al momento della creazione dell'organizzazione. Se la tua organizzazione è impostata solo sulla fatturazione consolidata e desideri abilitare tutte le funzionalità, vedi Abilitazione di tutte le funzionalità nell'organizzazione.
- È necessario abilitare l'accesso affidabile per il servizio di gestione degli AWS account. Per configurarlo, vedi Abilitazione dell'accesso affidabile per la gestione AWS dell'account.

AWS Management Console

Per modificare il contatto principale per qualsiasi Account AWS membro dell'organizzazione

1. Accedi alla AWS Organizationsconsole con le credenziali dell'account di gestione dell'organizzazione.
2. Da Account AWS, seleziona l'account che desideri aggiornare.
3. Scegli Informazioni di contatto e individua il contatto principale,
4. Seleziona Edit (Modifica).
5. Modifica i valori nei campi disponibili.
6. Dopo aver apportato tutte le modifiche, scegli Aggiorna.

AWS CLI & SDKs

Puoi recuperare, aggiornare o eliminare le informazioni di contatto principali utilizzando AWS CLI i seguenti comandi o le relative operazioni equivalenti all'AWSSDK:

- GetContactInformation
- PutContactInformation

> **Note**
>
> - Per eseguire queste operazioni dall'account di gestione o da un account amministratore delegato di un'organizzazione utilizzando gli account dei membri, è necessario abilitare l'accesso affidabile per il servizio Account.
> - Non puoi accedere a un account in un'organizzazione diversa da quella che stai utilizzando per chiamare l'operazione.

> **Autorizzazioni minime**
>
> Per ogni operazione, devi disporre dell'autorizzazione corrispondente a tale operazione:
>
> - `account:GetContactInformation`
> - `account:PutContactInformation`
>
> Se utilizzi queste autorizzazioni individuali, puoi concedere ad alcuni utenti la possibilità di leggere solo le informazioni di contatto e concedere ad altri la possibilità di leggere e scrivere.

Example

L'esempio seguente recupera le informazioni di contatto principali correnti per l'account membro specificato in un'organizzazione. Le credenziali utilizzate devono provenire dall'account di gestione dell'organizzazione o dall'account amministratore delegato di Account Management.

```
$ aws account get-contact-information --account-id 123456789012
```

```
{
    "ContactInformation": {
        "AddressLine1": "123 Any Street",
        "City": "Seattle",
        "CompanyName": "Example Corp, Inc.",
        "CountryCode": "US",
        "DistrictOrCounty": "King",
        "FullName": "Saanvi Sarkar",
        "PhoneNumber": "+15555550100",
        "PostalCode": "98101",
        "StateOrRegion": "WA",
        "WebsiteUrl": "https://www.examplecorp.com"
    }
}
```

Example

L'esempio seguente imposta le informazioni di contatto principali per l'account membro specificato in un'organizzazione. Le credenziali utilizzate devono provenire dall'account di gestione dell'organizzazione o dall'account amministratore delegato di Account Management.

```
$ aws account put-contact-information --account-id 123456789012 \
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",
 "CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":
 "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
 "StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Se ha esito positivo, questo comando non produrrà alcun output.

Aggiorna le domande relative alle sfide di sicurezza

Le domande relative ai problemi di sicurezza sono un metodo di verifica utilizzato in precedenza per verificare un'identità negli scenari di ripristino dell'account. Sono meno sicure rispetto alle forme di verifica più moderne, come l'autenticazione a più fattori (MFA). Se al momento hai domande relative ai problemi di sicurezza attive sul tuo AWS Support accountAccount AWS, puoi utilizzarle per autenticarti come proprietario dell'account.

Important

A partire dal 5 gennaio 2024, non AWS saranno più supportate le domande relative ai problemi di sicurezza per gli account che non le hanno già abilitate e utilizzate. Ciò rimuoverà l'opzione per aggiungere nuove domande relative alla sicurezza dalla pagina Account delAWS Management Console. Se hai già impostato domande relative ai problemi di sicurezza o le hai già impostate nell'account di gestione della tua AWS organizzazione, puoi continuare a usarle. Dopo il 6 gennaio 2025, non AWS supporterà più le domande relative ai problemi di sicurezza per tutti i clienti rimanenti. Ti consigliamo invece di aggiungere l'MFA. Per ulteriori informazioni, consulta AWSAccounts (Interrompe l'uso delle domande relative ai problemi di sicurezza).

Per modificare le domande esistenti relative ai problemi di sicurezza e fornire le risposte, esegui i passaggi indicati nella procedura seguente.

AWS Management Console

Per modificare le domande relative alle sfide di sicurezza relative a Account AWS

Autorizzazioni minime

Per eseguire le seguenti operazioni, devi disporre come minimo delle seguenti autorizzazioni IAM:

- `account:GetChallengeQuestions`(per vedere le domande relative alle sfide di sicurezza)
- `account:PutChallangeQuestions`(per impostare o aggiornare le domande relative alla sfida di sicurezza)

1. Accedi a o AWS Management Consolecome utente Utente root dell'account AWS o ruolo IAM con le autorizzazioni minime.
2. Scegli il nome del tuo account in alto a destra nella finestra, quindi scegli Account.
3. Scorri verso il basso fino alla sezione Domande relative alla sfida di sicurezza e scegli Modifica.

> **Note**
>
> Se non vedi l'opzione Modifica, è probabile che tu non abbia effettuato l'accesso come utente root del tuo account o come utente che dispone delle autorizzazioni minime specificate sopra.

4. Modifica i valori nei campi disponibili. Puoi selezionare una delle domande fornite e inserire la risposta appropriata.
5. Dopo aver completato le modifiche, scegli Aggiorna.

AWS CLI & SDKs

Questa attività non è supportata nella AWS CLI o da un'operazione API di uno degli SDK AWS. È possibile eseguire questa attività solo utilizzando la AWS Management Console.

Specificate quali possono essere utilizzati dal Regioni AWS vostro account

An Regione AWSè una posizione fisica nel mondo in cui abbiamo più zone di disponibilità. Le zone di disponibilità sono costituite da uno o più data AWS center discreti, ciascuno con alimentazione, rete e connettività ridondanti, ospitati in strutture separate. Ciò significa che ciascuna Regione AWS è fisicamente isolata e indipendente dalle altre regioni. Le regioni forniscono la tolleranza ai guasti, la stabilità e la resilienza e possono anche ridurre la latenza. Per una mappa delle regioni disponibili e future, vedi Regioni e zone di disponibilità.

Le risorse create in una regione non esistono in nessun'altra regione a meno che non si utilizzi esplicitamente una funzionalità di replica offerta da un AWS servizio. Ad esempio, Amazon S3 e Amazon EC2 supportano la replica tra regioni. Alcuni servizi, come AWS Identity and Access Management (IAM), non dispongono di risorse regionali.

Il tuo account determina le regioni per te disponibili.

- An Account AWS fornisce più regioni in modo da poter lanciare AWS risorse in località che soddisfano i tuoi requisiti. Ad esempio, potresti voler lanciare istanze Amazon EC2 in Europa per essere più vicino ai tuoi clienti europei o per soddisfare i requisiti legali.

- Un account AWS GovCloud (Stati Uniti occidentali) fornisce l'accesso alla regione AWS GovCloud (Stati Uniti occidentali) e alla regione AWS GovCloud (Stati Uniti orientali). Per ulteriori informazioni, consulta AWS GovCloud (US).
- Un account Amazon AWS (Cina) consente l'accesso solo alle regioni di Pechino e Ningxia. Per ulteriori informazioni, consulta Amazon Web Services in Cina.

Per un elenco dei nomi delle regioni e dei codici corrispondenti, consulta Endpoint regionali nella Guida AWS generale di riferimento. Per un elenco dei AWS servizi supportati in ogni regione (senza endpoint), consulta l'Elenco dei servizi AWS regionali.

> **Important**
>
> AWS consiglia di utilizzare gli endpoint regionali AWS Security Token Service (AWS STS) anziché l'endpoint globale per ridurre la latenza. I token di sessione degli AWS STS endpoint regionali sono validi in tutte le regioni. AWS Se utilizzi AWS STS endpoint regionali, non è necessario apportare modifiche. Tuttavia, i token di sessione dell' AWS STS endpoint globale (https://sts.amazonaws.com) sono validi solo se abilitati o se sono abilitati per impostazione predefinita. Regioni AWS Se intendi abilitare una nuova regione per il tuo account, puoi utilizzare i token di sessione dagli AWS STS endpoint regionali o attivare l'endpoint globale AWS STS per emettere token di sessione validi in tutti. Regioni AWS I token di sessione validi in tutte le regioni sono più grandi. Se memorizzi token di sessione, questi token più grandi potrebbero influire sui tuoi sistemi. Per ulteriori informazioni su come gli AWS STS endpoint funzionano con AWS le regioni, vedi Gestione AWS STS in una regione. AWS

Argomenti

Considerazioni prima di abilitare e disabilitare le regioni

Prima di abilitare o disabilitare una regione, è importante considerare quanto segue:

- Le aree introdotte prima del 20 marzo 2019 sono abilitate per impostazione predefinita: AWS inizialmente abilitate, tutte nuove Regioni AWS per impostazione predefinita, il che significa che

puoi iniziare a creare e gestire risorse in queste aree immediatamente. Non è possibile abilitare o disabilitare una regione abilitata per impostazione predefinita. Oggi, quando si AWS aggiunge una regione, la nuova regione è disabilitata per impostazione predefinita. Se desideri che i tuoi utenti siano in grado di creare e gestire risorse in una nuova regione, devi prima abilitare quella regione. Le seguenti regioni sono disabilitate per impostazione predefinita.

Nome	Codice
Africa (Città del Capo)	`af-south-1`
Asia Pacifico (Hong Kong)	`ap-east-1`
Asia Pacific (Hyderabad)	`ap-south-2`
Asia Pacifico (Giacarta)	`ap-southeast-3`
Asia Pacifico (Melbourne)	`ap-southeast-4`
Canada (Calgary)	`ca-west-1`
Europa (Milano)	`eu-south-1`
Europa (Spagna)	`eu-south-2`
Europa (Zurigo)	`eu-central-2`
Israele (Tel Aviv)	`il-central-1`
Medio Oriente (Bahrein)	`me-south-1`
Medio Oriente (Emirati Arabi Uniti)	`me-central-1`

- Puoi utilizzare le autorizzazioni IAM per controllare l'accesso alle regioni: AWS Identity and Access Management (IAM) include quattro autorizzazioni che consentono di controllare quali utenti possono abilitare, disabilitare, ottenere ed elencare le regioni. Per ulteriori informazioni, consulta AWS: Consente l'attivazione e la disabilitazione Regioni AWS nella Guida per l'utente IAM. Puoi anche utilizzare il tasto `aws:RequestedRegion`condition per controllare l'accesso a Servizi AWS in un Regione AWS.
- L'attivazione di una regione è gratuita: l'abilitazione di una regione è gratuita. Ti vengono addebitati solo i costi delle risorse che crei nella nuova regione.

- La disabilitazione di una regione disabilita l'accesso IAM alle risorse nella regione: se disabiliti una regione che contiene ancora AWS risorse, come le istanze Amazon Elastic Compute Cloud (Amazon EC2), perdi l'accesso IAM alle risorse in quella regione. Ad esempio, non puoi utilizzare il per visualizzare o AWS Management Console modificare la configurazione di alcuna istanza EC2 in una regione disattivata.
- Gli addebiti per le risorse attive continuano se disabiliti una regione: se disabiliti una regione che contiene ancora AWS risorse, gli addebiti per tali risorse (se presenti) continuano ad essere addebitati alla tariffa standard. Ad esempio, se disabiliti una regione che contiene istanze Amazon EC2, devi ancora pagare i costi per tali istanze anche se queste non sono accessibili.
- La disabilitazione di una regione non è sempre immediatamente visibile: i servizi e le console potrebbero essere temporaneamente visibili dopo aver disabilitato una regione. La disabilitazione di una regione può richiedere da alcuni minuti a diverse ore per avere effetto.
- L'abilitazione di una regione richiede da alcuni minuti a diverse ore in alcuni casi: quando abiliti una regione, AWS esegue azioni per preparare l'account in quella regione, come la distribuzione delle risorse IAM nella regione. Questo processo richiede alcuni minuti per la maggior parte degli account, ma a volte può richiedere diverse ore. Non è possibile utilizzare la regione finché il processo viene completato.
- Le organizzazioni possono avere 50 richieste region-opt aperte in un determinato momento all'interno di un' AWS organizzazione: l'account di gestione può in qualsiasi momento avere 50 richieste aperte in attesa di completamento per la propria organizzazione. Una richiesta equivale all'attivazione o alla disabilitazione di una particolare regione per un account.
- Un singolo account può avere 6 richieste di opzione regionale in corso in un dato momento: una richiesta equivale all'attivazione o alla disabilitazione di una particolare regione per un account.
- EventBridge Integrazione con Amazon: i clienti possono iscriversi alle notifiche di aggiornamento dello stato di region-opt in. EventBridge Verrà creata una EventBridge notifica per ogni modifica di stato, che consentirà ai clienti di automatizzare i flussi di lavoro.
- Stato espressivo di opzione regionale: a causa della natura asincrona dell'abilitazione/disabilitazione di un'area opt-in, esistono quattro potenziali stati per una richiesta di opzione regionale:
  - `ENABLING`
  - `DISABLING`
  - `ENABLED`
  - `DISABLED`

Non è possibile annullare un opt-in o un opt-out quando si trova in uno dei due stati. `ENABLING` `DISABLING` Altrimenti, `ConflictException` verrà lanciato un. Una richiesta region-opt completata (abilitata/disabilitata) dipende dalla fornitura dei principali servizi sottostanti. AWS Potrebbero esserci alcuni AWS servizi che non saranno immediatamente utilizzabili nonostante lo stato. `ENABLED`

- Integrazione completa con AWS Organizations: un account di gestione può modificare o leggere region-opt per qualsiasi account membro di quell' AWS organizzazione. Un account membro è anche in grado di leggere/scrivere lo stato della propria regione.

Abilita o disabilita una regione per gli account autonomi

Per aggiornare le Account AWS regioni a cui hai accesso, esegui i passaggi indicati nella procedura seguente. La AWS Management Console procedura riportata di seguito funziona sempre solo in un contesto autonomo. È possibile utilizzare il AWS Management Console per visualizzare o aggiornare solo le regioni disponibili nell'account utilizzato per chiamare l'operazione.

AWS Management Console

Per abilitare o disabilitare una regione per una versione autonoma Account AWS

> **Autorizzazioni minime**
>
> Per eseguire i passaggi della procedura seguente, un utente o un ruolo IAM deve disporre delle seguenti autorizzazioni:
>
> - `account:ListRegions`(necessario per visualizzare l'elenco Regioni AWS e se sono attualmente abilitati o disabilitati).
> - `account:EnableRegion`
> - `account:DisableRegion`

1. Accedi a o AWS Management Consolecome utente Utente root dell'account AWS o ruolo IAM con le autorizzazioni minime.
2. Scegli il nome del tuo account in alto a destra nella finestra, quindi scegli Account.
3. Nella pagina Account, scorri verso il basso fino alla sezione Regioni AWS.

> **Note**
>
> È possibile che ti venga richiesto di approvare l'accesso a queste informazioni. AWS invia una richiesta all'indirizzo e-mail associato all'account e al numero di telefono di contatto principale. Scegli il link nella richiesta per aprirlo nel tuo browser e approva l'accesso.

4. Accanto Regione AWS a ciascuna opzione nella colonna Azione, scegli Abilita o Disabilita, a seconda che tu voglia che gli utenti del tuo account siano in grado di creare e accedere alle risorse in quella regione.
5. Se richiesto, conferma la scelta.
6. Dopo aver apportato tutte le modifiche, scegli Aggiorna.

AWS CLI & SDKs

Puoi abilitare, disabilitare, leggere ed elencare lo stato delle opzioni regionali utilizzando AWS CLI i seguenti comandi o le relative operazioni equivalenti all' AWS SDK:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **Autorizzazioni minime**
>
> Per eseguire i seguenti passaggi, è necessario disporre dell'autorizzazione corrispondente a tale operazione:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Se si utilizzano queste autorizzazioni individuali, è possibile concedere ad alcuni utenti la possibilità di leggere solo le informazioni sulle opzioni regionali e concedere ad altri la possibilità di leggere e scrivere.

L'esempio seguente abilita una regione per l'account membro specificato in un'organizzazione. Le credenziali utilizzate devono provenire dall'account di gestione dell'organizzazione o dall'account amministratore delegato di Account Management.

Tieni presente che puoi anche disabilitare una regione usando lo stesso comando e sostituendola `enable-region` con. `disable-region`

```
aws account enable-region --region-name af-south-1
```

Se ha esito positivo, questo comando non produrrà alcun output.

L'operazione è asincrona. Il comando seguente ti permetterà di vedere lo stato più recente della richiesta.

```
aws account get-region-opt-status --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Abilita o disabilita una regione nella tua organizzazione

Per aggiornare le regioni abilitate per gli account membro della tua AWS Organizations, procedi nel seguente modo.

> **Note**
>
> Le politiche AWS Organizations `AWSOrganizationsReadOnlyAccess` gestite `AWSOrganizationsFullAccess` vengono aggiornate per consentire l'accesso alle API di gestione degli AWS account in modo da poter accedere ai dati dell'account dalla AWS Organizations console. Per visualizzare le policy gestite aggiornate, vedere Updates to Organizations AWS managed policy.

> **Note**
>
> Prima di poter eseguire queste operazioni dall'account di gestione o da un account amministratore delegato di un'organizzazione da utilizzare con gli account dei membri, è necessario:
>
> - Abilita tutte le funzionalità dell'organizzazione per gestire le impostazioni degli account dei membri. Ciò consente il controllo amministrativo sugli account dei membri. Questa impostazione è predefinita al momento della creazione dell'organizzazione. Se la tua organizzazione è impostata solo sulla fatturazione consolidata e desideri abilitare tutte le funzionalità, vedi Abilitazione di tutte le funzionalità nell'organizzazione.
> - Abilita l'accesso affidabile per il servizio di gestione degli AWS account. Per configurarlo, consultaAbilitare l'accesso affidabile per la gestione degli AWS account.

AWS Management Console

Per abilitare o disabilitare una regione nell'organizzazione

1. Accedi alla AWS Organizations console con le credenziali dell'account di gestione dell'organizzazione.
2. Nella Account AWSpagina, seleziona l'account che desideri aggiornare.
3. Scegli la scheda Impostazioni dell'account.
4. In Regioni, seleziona la regione che desideri abilitare o disabilitare.
5. Scegli Azioni, quindi scegli l'opzione Abilita o Disabilita.
6. Se avete scelto l'opzione Abilita, controllate il testo visualizzato, quindi scegliete Abilita regione.
7. Se avete scelto l'opzione Disabilita, esaminate il testo visualizzato, digitate disabilita per confermare, quindi scegliete Disabilita regione.

AWS CLI & SDKs

Puoi abilitare, disabilitare, leggere ed elencare lo stato di optazione regionale per gli account dei membri dell'organizzazione utilizzando i seguenti AWS CLI comandi o le relative operazioni equivalenti all' AWS SDK:

- `EnableRegion`

- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

> **Autorizzazioni minime**
>
> Per eseguire i seguenti passaggi, è necessario disporre dell'autorizzazione corrispondente a tale operazione:
>
> - `account:EnableRegion`
> - `account:DisableRegion`
> - `account:GetRegionOptStatus`
> - `account:ListRegions`

Se si utilizzano queste autorizzazioni individuali, è possibile concedere ad alcuni utenti la possibilità di leggere solo le informazioni sulle opzioni regionali e concedere ad altri la possibilità di leggere e scrivere.

L'esempio seguente abilita una regione per l'account membro specificato in un'organizzazione. Le credenziali utilizzate devono provenire dall'account di gestione dell'organizzazione o dall'account amministratore delegato di Account Management.

Tieni presente che puoi anche disabilitare una regione usando lo stesso comando e sostituendola `enable-region` con. `disable-region`

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

Se ha esito positivo, questo comando non produrrà alcun output.

> **Note**
>
> Un'organizzazione può avere solo fino a 20 richieste regionali alla volta. Altrimenti, riceverai un`TooManyRequestsException`.

L'operazione è asincrona. Il comando seguente ti permetterà di vedere lo stato più recente della richiesta.

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
  {
    "RegionName": "af-south-1",
    "RegionOptStatus": "ENABLING"
  }
```

Crea o aggiorna il tuo Account AWS alias

Se desideri che l'URL dei tuoi utenti IAM contenga il nome della tua azienda (o un altro easy-to-remember identificatore) anziché l'Account AWSID, puoi creare un alias dell'account.

Per informazioni su come creare o aggiornare un alias di account, consulta Creating, delete and listing an Account AWS alias nella IAM User Guide.

Fatturazione di unaAccount AWS

Per le procedure e le attività relative alla fatturazione correlate al tuoAccount AWS, consulta i seguenti argomenti nellaAWS Billing and Cost ManagementGuida per l'utente di:

- Modifica della valuta utilizzata per il pagamento delle fatture
- Aggiornamento ed eliminazione di numeri di registrazione fiscale
- Abilitazione dell'ereditarietà delle impostazioni fiscali

Gestisci gli account in India

Se ti iscrivi a un nuovoAccount AWSe scegli India come indirizzo di contatto, il tuo contratto d'uso è conAmazon Internet Services Private Limited(AISPL), un localeAWSil venditore in India.AISPL gestisce la fatturazione e il totale della fattura è indicato in rupie indiane (INR) anziché in dollari statunitensi (USD). Dopo aver creato un account con AISPL non puoi cambiare il Paese nelle informazioni di contatto.

Se ne hai già unoAccount AWScon un indirizzo indiano, il tuo account è conAWSo AISPL, a seconda di quando hai aperto l'account. Per sapere se il tuo account è conAWSo AISPL, vediDetermining

which company your account is with. Se sei un cliente AWS, puoi continuare a usare il tuo Account AWS. Puoi anche scegliere di avere entrambiAccount AWSe un account AISPL, sebbene non possano essere consolidati nello stessoAWSorganizzazione. Per informazioni sulla gestione di unAccount AWS, vediGestisci il tuoAccount AWS.

Se il tuo account è con AISPL, segui le procedure riportate in questo argomento per gestire il tuo account. Questo argomento spiega come creare un account AISPL, modificare le informazioni sul tuo account AISPL e aggiungere o modificare il tuo Permanent Account Number (PAN).

Come parte della procedura di verifica della carta di credito durante la registrazione, AISPL addebita 2 INR sulla tua carta, che ti verranno rimborsati da AISPL al termine della verifica. La verifica potrebbe includere il reindirizzamento al sito della tua banca.

Argomenti

Determina a quale azienda appartiene il tuo account

I servizi AWS vengono forniti da AWS e AISPL. Utilizza questa procedura per stabilire il rivenditore con il quale hai registrato il tuo account.

AWS Management Console

Per determinare la società con cui hai registrato l'account

> **Autorizzazioni minime**
>
> Per eseguire i seguenti passaggi, devi disporre almeno delle seguenti autorizzazioni IAM:
>
> - Questa procedura non richiede autorizzazioni speciali.

1. Apri la AWS Management Console all'indirizzo AWS Management Console.
2. Nel piè di pagina in fondo alla pagina, guarda l'avviso di copyright. Se il copyright indica di Amazon Web Services, allora il tuo account è registrato con AWS. Se il copyright è di Amazon Internet Services Private Ltd., allora il tuo account è registrato con AISPL.

AWS CLI & SDKs

Questa attività non è supportata nelAWS CLIo tramite un'operazione API da uno deiAWSSDK. È possibile eseguire questa operazione solo utilizzandoAWS Management Console.

Crea unAccount AWScon AISPL

AISPL è un venditore locale diAWSin India. Utilizza la seguente procedura per registrare un account con AISPL se il tuo indirizzo di contatto è in India.

AWS Management Console

Per registrare un account con AISPL

> **Autorizzazioni minime**
>
> Per eseguire i seguenti passaggi, devi disporre almeno delle seguenti autorizzazioni IAM:
>
> - Perché questa operazione si verifica prima di avere unAccount AWS, questa operazione non richiedeAWSautorizzazioni.

1. Apri ilAWS Management Console, quindi scegliAccedi alla console.
2. SulAccedipagina, inserisci l'indirizzo email che desideri utilizzare.
3. Nel campo dell'indirizzo e-mail, seleziona I am a new user (Nuovo utente), quindi scegli Sign in using our secure server (Accedi utilizzando il nostro server sicuro).
4. Per ognuno dei campi delle credenziali di accesso, inserisci le tue informazioni, quindi scegliCrea un account.
5. Per ognuno dei campi delle informazioni di contatto, inserisci le tue informazioni.
6. Dopo aver letto il contratto con il cliente, seleziona la casella di controllo dei termini e condizioni e scegli Create Account and Continue (Crea un account e continua).
7. Nella pagina Payment Information (Informazioni di pagamento), immetti il metodo di pagamento che intendi utilizzare.
8. SottoInformazioni PAN, scegliNose non disponi di un Permanent Account Number (PAN) o desideri aggiungerlo in un secondo momento. Se hai un PAN e vuoi aggiungerlo ora, sceglisì, e nelPADELLAnel campo inserisci il tuo PAN.

9. Scegli Verify Card and Continue (Verifica la carta e continua). È necessario fornire il CVV come parte del processo di verifica. AISPL addebiterà 2 INR sulla tua carta come parte del processo di verifica, che ti verranno rimborsati da AISPL al termine della verifica.
10. PerFornisci un numero di telefono, inserisci il tuo numero di telefono. Se disponi di un'estensione telefonica, perExt, inserisci l'estensione del tuo telefono.
11. Scegli Call Me Now (Chiamami ora). Dopo qualche secondo, sulla schermata viene visualizzato un PIN di quattro cifre.
12. Accetta la chiamata automatica da AISPL. Sulla tastiera del telefono, inserisci il pin a quattro cifre visualizzato sullo schermo.
13. Dopo che la chiamata automatica ha verificato il tuo numero di contatto, scegli Continue to Select Your Support Plan (Continua per selezionare il piano di supporto).
14. Nella pagina Support Plan (Piano di supporto), seleziona un piano di supporto, quindi scegli Continue (Continua). Dopo la verifica del metodo di pagamento e l'attivazione dell'account, riceverai un messaggio e-mail di conferma dell'attivazione dell'account.

AWS CLI & SDKs

Questa attività non è supportata nelAWS CLIo tramite un'operazione API da uno deiAWSSDK. È possibile eseguire questa operazione solo utilizzandoAWS Management Console.

Gestisci il tuo account AISPL

Ad eccezione delle seguenti attività, le procedure per la gestione dell'account sono le stesse degli account creati al di fuori dell'India. Consultare Gestisci il tuoAccount AWS.

Usa ilAWS Management Consoleper eseguire le seguenti attività:

- Aggiungere o modificare un numero di conto permanente (PAN)
- Modifica più numeri di conto permanenti (PAN)
- Modifica più codici fiscali per beni e servizi (GST)
- Visualizza una fattura fiscale

Chiudi un Account AWS

Se non ti serve più il tuo Account AWS, puoi chiuderlo in qualsiasi momento seguendo le istruzioni in questa sezione. Dopo averlo chiuso, puoi riaprirlo entro 90 giorni dal giorno in cui hai chiuso l'account. L'intervallo di tempo che intercorre tra il giorno in cui hai chiuso l'account e la chiusura AWS definitiva dell'account viene definito periodo successivo alla chiusura.

Cosa devi sapere prima di chiudere l'account

Prima di chiudere il tuo Account AWS, dovresti considerare quanto segue:

- La chiusura dell'account servirà come avviso di risoluzione del Contratto con il AWS cliente relativo a tale account.
- Non è necessario eliminare le risorse dal tuo account Account AWS prima di chiuderlo. Tuttavia, ti consigliamo di eseguire il backup di tutte le risorse o i dati che desideri conservare. Per istruzioni su come eseguire il backup di una particolare risorsa, consulta la AWS documentazione appropriata per quel servizio.
- Puoi riaprire il tuo account durante il periodo successivo alla chiusura. Gli addebiti per i servizi rimasti nel tuo account verranno riavviati se lo riapri. Rimani inoltre responsabile per eventuali fatture non pagate e Reserved Instances e Savings Plans in sospeso.
- Rimani responsabile di tutte le commissioni e gli addebiti in sospeso per i servizi consumati prima della chiusura dell'account. Riceverai una AWS fattura il mese successivo alla chiusura dell'account. Ad esempio, se hai chiuso il tuo account il 15 gennaio, riceverai una fattura all'inizio di febbraio per l'utilizzo effettuato dal 1° gennaio al 15 gennaio. Continuerai a ricevere fatture per Reserved Instances e Savings Plans dopo aver chiuso l'account fino alla loro scadenza.
- Non sarai più in grado di accedere ai AWS servizi precedentemente disponibili nel tuo account. Tuttavia, puoi accedere e accedere a un account chiuso Account AWS durante il periodo successivo alla chiusura solo per visualizzare le informazioni di fatturazione precedenti, accedere alle impostazioni dell'account o contattare. AWS Support
- Non puoi utilizzare lo stesso indirizzo email che hai registrato al Account AWS momento della chiusura come indirizzo email principale di un altro. Account AWS Se desideri utilizzare lo stesso indirizzo email per un indirizzo diverso Account AWS, ti consigliamo di aggiornarlo prima della chiusura. Consulta Aggiorna il Account AWS nome, l'indirizzo email o la password per l'utente root le istruzioni su come aggiornare il tuo indirizzo e-mail.
- Se hai abilitato l'autenticazione a più fattori (MFA) sul Account AWS tuo utente root o configurato un dispositivo MFA su un utente IAM, l'MFA non viene rimossa automaticamente alla chiusura

dell'account. Se scegli di lasciare la MFA attiva durante i 90 giorni successivi alla chiusura, mantieni attivo il dispositivo MFA fino alla scadenza del periodo successivo alla chiusura, nel caso in cui sia necessario accedere all'account durante quel periodo. Nota, i dispositivi hardware con token TOTP non possono essere associati a un altro utente dopo la chiusura permanente dell'account. Se desideri utilizzare il token TOTP hardware con un altro utente in un secondo momento, hai la possibilità di disattivare il dispositivo MFA hardware prima di chiudere l'account. I dispositivi MFA per utenti IAM devono essere eliminati dall'amministratore dell'account.

Considerazioni aggiuntive per gli account dei membri

- Quando chiudi un account membro, tale account viene rimosso dall'organizzazione solo dopo il periodo successivo alla chiusura. Durante il periodo di post-chiusura, un account membro chiuso conta ancora ai fini della quota di account nell'organizzazione. Per evitare che l'account venga conteggiato ai fini della quota, consulta Rimuovere un account membro dall'organizzazione prima di chiuderla.
- In un periodo di 30 giorni puoi chiudere solo il 10% degli account membri. Questa quota non è vincolata da un mese di calendario, ma inizia quando chiudi un account. Entro 30 giorni dalla chiusura iniziale dell'account, non potrai superare il limite di chiusura dell'account del 10%. La chiusura minima dell'account è 10 e la chiusura massima dell'account è 1000, anche se il 10% degli account supera 1000. Per ulteriori informazioni sulle quote di Organizations, vedere Quotas for. AWS Organizations
- Se utilizzi AWS Control Tower, devi annullare la gestione dell'account membro prima di tentare di chiudere l'account. Consulta la sezione Annullamento della gestione di un account membro nella Guida per l'utente di AWS Control Tower.

Considerazioni specifiche sul servizio

- Marketplace AWS gli abbonamenti non vengono annullati automaticamente alla chiusura dell'account. Se disponi di abbonamenti, per prima cosa interrompi tutte le istanze del software incluse negli abbonamenti. Quindi, vai alla pagina Gestisci gli abbonamenti della Marketplace AWS console e annulla gli abbonamenti.
- I domini registrati con Route 53 non vengono eliminati automaticamente. Prima di chiudere il tuo Account AWS, hai quattro opzioni:
  - Puoi disabilitare il rinnovo automatico e i domini vengono eliminati automaticamente alla scadenza del periodo di registrazione. Per ulteriori informazioni, consulta Abilitare o disabilitare il rinnovo automatico per un dominio nella Guida per sviluppatori di Amazon Route 53.

  - È possibile trasferire i domini a un altro Account AWS. Per ulteriori informazioni, consulta Trasferimento di un dominio a un diverso Account AWS.
  - È possibile trasferire i domini a un altro registrar di dominio. Per ulteriori informazioni, consulta Trasferimento di un dominio da Route 53 a un altro registrar.
  - Se hai già chiuso il tuo account, puoi aprire una richiesta di assistenza AWS Support per il trasferimento del dominio.
- AWS CloudTrail è un servizio di sicurezza fondamentale. Ciò significa che i percorsi creati dagli utenti continuano a esistere e a fornire eventi anche dopo la chiusura di un AWS account, a meno che un utente non elimini esplicitamente i percorsi dal proprio AWS account prima di chiuderlo. Questo comportamento si applica anche ai percorsi dell'organizzazione creati dall'account di gestione o dall'amministratore delegato e ai percorsi multi-regione dell'organizzazione che vengono creati in seguito negli account membri dell'organizzazione. Per ulteriori informazioni, consulta la sezione Chiusura e percorsi AWS dell'account nella Guida per l'CloudTrail utente.

Come chiudere l'account

Puoi chiudere il tuo Account AWS utilizzando la seguente procedura. Tieni presente che in ogni scheda vengono fornite indicazioni diverse a seconda del tipo di account [autonomo, membro, dirigente e AWS GovCloud (US)] che desideri chiudere.

Se riscontri problemi durante la procedura di chiusura dell'account, consultaRisoluzione dei problemi di Account AWS chiusura.

Standalone account

Un account autonomo è un account gestito individualmente di cui non fa parte AWS Organizations.

Per chiudere un account autonomo dalla pagina Account

1. Accedi AWS Management Console come utente root nel file Account AWS che desideri chiudere. Non puoi chiudere un account dopo aver effettuato l'accesso come utente o ruolo IAM.
2. Nella barra di navigazione nell'angolo in alto a destra, scegli il nome o il numero del tuo account, quindi scegli Account.
3. Nella pagina Account, scegli il pulsante Chiudi account.

4. Digita l'ID del tuo account (visualizzato nella parte superiore della finestra di dialogo di chiusura) per confermare di aver letto e compreso la procedura di chiusura dell'account.
5. Scegli il pulsante Chiudi account per avviare il processo di chiusura dell'account.
6. Entro pochi minuti, riceverai un'email di conferma della chiusura del tuo account.

> **Note**
>
> Questa attività non è supportata in AWS CLI o da un'operazione API di uno degli AWS SDK. È possibile eseguire questa attività solo utilizzando. AWS Management Console

Member account

Un account membro è un account Account AWS che fa parte di AWS Organizations.

Per chiudere un account membro dalla AWS Organizations console

1. Accedi alla console AWS Organizations.
2. Nella pagina Account AWS, individua e seleziona il nome dell'account membro che desideri chiudere. È possibile spostarsi nella gerarchia delle unità organizzative o visualizzare un elenco dei soli account senza la struttura dell'unità organizzativa.
3. Scegli Close (Chiudi) accanto al nome dell'account nella parte superiore della pagina. Le organizzazioni in modalità di fatturazione consolidata non saranno in grado di visualizzare il pulsante Chiudi nella console. Per chiudere un account in modalità di fatturazione consolidata, dovrai seguire i passaggi nella scheda Account autonomo.
4. Leggi e assicurati di aver compreso le linee guida sulla chiusura dell'account.
5. Inserisci l'ID dell'account membro, quindi scegli Chiudi account per avviare il processo di chiusura dell'account.

Per chiudere un account membro dalla pagina Account

Facoltativamente, puoi chiudere un account AWS membro direttamente dalla pagina Account in. AWS Management Console Per step-by-step ulteriori informazioni, segui le istruzioni nella scheda Account autonomo.

Per chiudere un account membro utilizzando gli AWS CLI SDK

Per istruzioni su come chiudere un account membro utilizzando gli SDK AWS CLI e, consulta Chiusura di un account membro nell'organizzazione nella Guida per l'AWS Organizations utente.

Management account

Un account di gestione è un account Account AWS che funge da account principale o root per AWS Organizations.

> **Note**
>
> Non è possibile chiudere un account di gestione direttamente dalla AWS Organizations console.

Per chiudere un account di gestione dalla pagina Account

1. Accedi AWS Management Console come utente root dell'account di gestione che desideri chiudere. Non puoi chiudere un account dopo aver effettuato l'accesso come utente o ruolo IAM.
2. Verifica che non ci siano ancora account membri attivi nella tua organizzazione. A tale scopo, accedi alla AWS Organizations console e assicurati che tutti gli account dei membri siano visualizzati `Suspended` accanto ai nomi dei rispettivi account. Se hai un account membro ancora attivo, dovrai seguire le linee guida sulla chiusura dell'account fornite nella scheda Account membro prima di poter passare alla fase successiva.
3. Nella barra di navigazione nell'angolo in alto a destra, scegli il nome o il numero del tuo account, quindi scegli Account.
4. Nella pagina Account, scegli il pulsante Chiudi account.
5. Digita l'ID del tuo account (visualizzato nella parte superiore della finestra di dialogo di chiusura) per confermare di aver letto e compreso la procedura di chiusura dell'account.
6. Scegli il pulsante Chiudi account per avviare il processo di chiusura dell'account.
7. Entro pochi minuti, riceverai un'email di conferma della chiusura del tuo account.

> **Note**
>
> Questa attività non è supportata in AWS CLI o da un'operazione API di uno degli AWS SDK. È possibile eseguire questa attività solo utilizzando. AWS Management Console

AWS GovCloud (US) account

Un AWS GovCloud (US) account è sempre collegato a un unico standard Account AWS per la fatturazione e il pagamento.

Per chiudere un account AWS GovCloud (US)

Se ne hai uno Account AWS collegato a un AWS GovCloud (US) account, devi chiudere l'account standard prima di chiudere l' AWS GovCloud (US) account. Per ulteriori dettagli, tra cui come eseguire il backup dei dati ed evitare AWS GovCloud (US) addebiti indesiderati, consulta Chiusura di un AWS GovCloud (US) account nella Guida per l' AWS GovCloud (US) utente.

Cosa aspettarsi dopo la chiusura dell'account

Immediatamente dopo la chiusura dell'account, si verificherà quanto segue:

- Riceverai un'email di conferma della chiusura dell'account all'indirizzo e-mail dell'utente root. Se non ricevi questa e-mail entro poche ore, consultaRisoluzione dei problemi di Account AWS chiusura.
- Qualsiasi account membro che chiudi mostrerà un'`SUSPENDED`etichetta accanto al nome dell'account nella AWS Organizations console.
- Se hai concesso le autorizzazioni per accedere ai servizi del tuo account Account AWS ad altri account, qualsiasi richiesta di accesso effettuata da tali account dovrebbe fallire dopo la chiusura dell'account. Se riapri il tuo Account AWS, altri Account AWS possono accedere nuovamente ai AWS servizi e alle risorse del tuo account se hai concesso loro le autorizzazioni necessarie.

Periodo successivo alla chiusura

Il periodo successivo alla chiusura si riferisce al periodo di tempo che intercorre tra il giorno in cui hai chiuso l'account e la chiusura AWS definitiva del tuo. Account AWS Il periodo successivo alla chiusura è di 90 giorni. Durante il periodo successivo alla chiusura, puoi accedere ai tuoi contenuti e AWS servizi solo riaprendo il tuo account. Dopo il periodo successivo alla chiusura, chiude AWS definitivamente il tuo Account AWS e non puoi più riaprirlo. AWS eliminerà inoltre tutti i contenuti e le risorse del tuo account. Dopo che un account è stato chiuso definitivamente, il suo Account AWS ID non può più essere riutilizzato.

Riapertura del tuo Account AWS

Il tuo account verrà chiuso definitivamente tra 90 giorni, dopodiché non potrai più riaprirlo e AWS eliminerai i contenuti rimanenti nell'account. Per riaprire il tuo account prima che venga chiuso definitivamente, (1) devi contattarci il prima AWS Supportpossibile e (2) dobbiamo ricevere il pagamento completo di qualsiasi saldo dovuto, inclusa la fornitura delle informazioni richieste come specificato nella fattura, entro 60 giorni dalla data di chiusura dell'account.

> **Note**
>
> Gli addebiti per i servizi rimasti nel tuo account verranno riavviati se lo riapri.

Utilizzo della gestione degli AWS account nella tua organizzazione

AWS Organizationsè un AWS servizio che puoi usare per gestire Account AWS il tuo gruppo. Ciò fornisce funzionalità come la fatturazione consolidata, in cui tutte le fatture degli account sono raggruppate e gestite da un unico pagatore. Puoi anche gestire centralmente la sicurezza della tua organizzazione utilizzando controlli basati su policy. Per ulteriori informazioni su AWS Organizations, consulta la Guida per l'utente di AWS Organizations.

Accesso attendibile

Quando gestisci AWS Organizations i tuoi account come gruppo, la maggior parte delle attività amministrative dell'organizzazione può essere eseguita solo dall'account di gestione dell'organizzazione. Per impostazione predefinita, ciò include solo le operazioni relative alla gestione dell'organizzazione stessa. È possibile estendere questa funzionalità aggiuntiva ad altri AWS servizi abilitando l'accesso affidabile tra le organizzazioni e quel servizio. L'accesso affidabile concede al AWS servizio specificato le autorizzazioni per accedere alle informazioni sull'organizzazione e sugli account in essa contenuti. Quando abiliti l'accesso affidabile per Account Management, il servizio Account Management concede alle organizzazioni e ai relativi account di gestione le autorizzazioni per accedere ai metadati, come le informazioni di contatto primarie o alternative, per tutti gli account dei membri dell'organizzazione.

Per ulteriori informazioni, consulta Abilitare l'accesso affidabile per la gestione degli AWS account.

Amministratore delegato

Dopo aver abilitato l'accesso affidabile, puoi anche scegliere di designare uno dei tuoi account membri come account amministratore delegato per la gestione degli AWS account. Ciò consente all'account amministratore delegato di eseguire le stesse attività di gestione dei metadati di Account Management per gli account dei membri dell'organizzazione che in precedenza poteva eseguire solo l'account di gestione. L'account amministratore delegato può accedere solo alle attività di gestione del servizio Account Management. L'account amministratore delegato non dispone di tutti gli accessi amministrativi all'organizzazione di cui dispone l'account di gestione.

Per ulteriori informazioni, consulta Abilitazione di un account amministratore delegato perAWSGestione dell'account.

Policy di controllo dei servizi

Quando fai Account AWS parte di un'organizzazione gestita daAWS Organizations, l'amministratore dell'organizzazione può applicare politiche di controllo dei servizi (SCP) che possono limitare le attività dei responsabili degli account dei membri. Un SCP non concede mai autorizzazioni; è invece un filtro che limita le autorizzazioni che possono essere utilizzate dall'account membro. Un utente o un ruolo (principale) in un account membro può eseguire solo le operazioni che si trovano all'incrocio tra quanto consentito dagli SCP che si applicano all'account e le politiche di autorizzazione IAM allegate al principale. Ad esempio, puoi usare gli SCP per impedire a qualsiasi preside di un account di modificare i contatti alternativi del proprio account.

Ad esempio, gli SCP che si applicano aAccount AWS, vediLimitazione dell'accesso conAWS OrganizationsPolicy di controllo dei servizi.

Abilitare l'accesso affidabile per la gestione degli AWS account

L'attivazione dell'accesso affidabile per AWS Account Management consente all'amministratore dell'account di gestione di modificare le informazioni e i metadati (ad esempio, i dettagli di contatto principali o alternativi) specifici per ciascun account membro in. AWS Organizations Per ulteriori informazioni, consulta Gestione AWS dell'account e AWS Organizations nella Guida per l'AWS Organizationsutente. Per informazioni generali sul funzionamento di Trusted Access, vedere Utilizzo AWS Organizations con altri AWS servizi.

Dopo aver abilitato l'accesso affidabile, puoi utilizzare il `accountID` parametro nelle operazioni API di gestione degli account che lo supportano. Puoi utilizzare questo parametro con successo solo se chiami l'operazione utilizzando le credenziali dell'account di gestione o dall'account amministratore delegato della tua organizzazione se ne abiliti uno. Per ulteriori informazioni, consulta Abilitazione di un account amministratore delegato perAWSGestione dell'account.

Utilizza la seguente procedura per abilitare l'accesso affidabile per la gestione degli account nella tua organizzazione.

Autorizzazioni minime

Per eseguire queste attività, è necessario soddisfare i seguenti requisiti:

- È possibile eseguire questa operazione solo dall'account di gestione dell'organizzazione.
- L'organizzazione deve avere tutte le caratteristiche abilitate.

AWS Management Console

Per abilitare l'accesso affidabile per la gestione degli AWS account

1. Accedi alla console AWS Organizations. È necessario accedere come utente IAM, assumere un ruolo IAM o accedere come utente root (non consigliato) nell'account di gestione dell'organizzazione.
2. Scegli Servizi nel riquadro di navigazione.
3. Scegli AWSAccount Management nell'elenco dei servizi.
4. Scegliere Enable trusted access (Abilita accesso sicuro).
5. Nella finestra di dialogo Abilita accesso affidabile per la gestione AWS dell'account, digita abilita per confermarlo, quindi scegli Abilita accesso affidabile.

AWS CLI & SDKs

Per abilitare l'accesso affidabile per la gestione degli AWS account

Dopo aver eseguito il comando seguente, è possibile utilizzare le credenziali dell'account di gestione dell'organizzazione per richiamare le operazioni dell'API di gestione degli account che utilizzano il `--accountId` parametro per fare riferimento agli account dei membri di un'organizzazione.

- AWS CLI: enable-aws-service-access

  L'esempio seguente abilita l'accesso affidabile per AWS Account Management nell'organizzazione dell'account chiamante.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Se ha esito positivo, questo comando non produrrà alcun output.

Abilitazione di un account amministratore delegato perAWSGestione dell'account

Un account amministratore delegato può chiamare ilAWSOperazioni dell'API di gestione degli account per altri account membri dell'organizzazione. Per designare un account membro dell'organizzazione come account amministratore delegato, attenersi alla procedura seguente.

Autorizzazioni minime

Per eseguire queste attività è necessario soddisfare i seguenti requisiti:

- È possibile eseguire questa operazione solo dall'account di gestione dell'organizzazione.
- L'organizzazione deve avere tutte le caratteristiche abilitate.
- È necessario avereaccesso attendibile abilitato per Gestione account nell'organizzazione.

Dopo aver specificato un account amministratore delegato per l'organizzazione, gli utenti e i ruoli in tale account possono chiamare ilAWS CLIeAWSOperazioni SDK nel`account`namespace che può funzionare in modalità Organizations supportando un facoltativo`AccountId`Parametro .

AWS Management Console

Questa attività non è supportata inAWSAccount Management console. È possibile eseguire questa attività solo utilizzando ilAWS CLIo un'operazione API da uno deiAWSSDK.

AWS CLI & SDKs

Per registrare un account amministratore delegato per il servizio Gestione account

Per abilitare un amministratore delegato per il servizio di gestione degli account, puoi utilizzare i seguenti comandi.

È necessario specificare il principale di servizio seguente:

```
account.amazonaws.com
```

- AWS CLI:register-delegato-amministratore

  L'esempio seguente registra un account membro dell'organizzazione come amministratore delegato per il servizio Gestione account.

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

Questo comando non produce alcun output se ha esito positivo.

Dopo aver eseguito questo comando, è possibile utilizzare le credenziali dell'account 123456789012 per chiamare Gestione accountAWS CLIe le operazioni dell'API SDK che utilizzano il`--account-id`parametro per fare riferimento agli account membri di un'organizzazione.

Limitazione dell'accesso conAWS OrganizationsPolicy di controllo dei servizi

In questo argomento vengono presentati esempi che mostrano come è possibile utilizzare le policy di controllo dei servizi (SCP) per limitare le attività che gli utenti e i ruoli negli account dell'organizzazione possono eseguire. Per ulteriori informazioni sui criteri di controllo dei servizi, consulta i seguenti argomenti nellaAWS OrganizationsGuida per l'utente di:

- Creazione di SCP
- Collegamento di SCP a unità organizzative e account
- Strategie per gli SCP
- Sintassi dei criteri SCP

Example Esempio 1: Impedire agli account di modificare i propri contatti alternativi

L'esempio seguente nega il`PutAlternateContact`e`DeleteAlternateContact`Le operazioni API non possono essere richiamate da qualsiasi account membro inmodalità di account autonoma. Ciò impedisce a qualsiasi principal negli account interessati di modificare i propri contatti alternativi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
```

```
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "arn:aws:account::*:account" ]
        }
    ]
}
```

Example Esempio 2: Impedire a qualsiasi account membro di modificare i contatti alternativi per qualsiasi altro account membro nell'organizzazione

L'esempio seguente generalizza il`Resource`elemento a «*», il che significa che si applica a entrambirichieste in modalità standalone e richieste in modalità organizzazione. Ciò significa che anche l'account amministratore delegato per la gestione dell'account, se l'SCP si applica ad esso, è bloccato dalla modifica di qualsiasi contatto alternativo per qualsiasi account nell'organizzazione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": [
                "account:PutAlternateContact",
                "account:DeleteAlternateContact"
            ],
            "Resource": [ "*" ]
        }
    ]
}
```

Example Esempio 3: Impedire a un account membro in un'unità organizzativa di modificare i propri contatti alternativi

Il seguente esempio SCP include una condizione che confronta il percorso dell'organizzazione dell'account con un elenco di due unità organizzative. Ciò comporta il blocco da parte di un principal in qualsiasi account nelle unità organizzative specificate di modificare i propri contatti alternativi.

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

```
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "Action": "account:PutAlternateContact",
            "Resource": [
                "arn:aws:account::*:account"
            ],
            "Condition": {
                "ForAnyValue:StringLike": {
                    "account:AccountResourceOrgPath": [
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/",
                        "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/"
                    ]
                }
            }
    ]
}
```

Sicurezza inAWSGestione dell'account

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS in Cloud AWS. AWS fornisce inoltre i servizi che è possibile utilizzare in modo sicuro. I revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano a Gestione dell'account, consultaServizi AWSnell'ambito del programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che viene utilizzato. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione consente di comprendere come applicare il modello di responsabilità condivisa quando si usaAWSGestione dell'account. Viene illustrato come configurare Gestione dell'account per soddisfare gli obiettivi di sicurezza e conformità. Viene anche illustrato come utilizzare gli altriAWSservizi che possono aiutarti a monitorare e proteggere le risorse di Gestione dell'account.

Argomenti

Protezione dei dati nella gestione degli AWS account

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati nella gestione degli AWS account. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile di mantenere il controllo sui contenuti ospitati su questa infrastruttura. Sei inoltre responsabile delle attività di configurazione e gestione della sicurezza per i Servizi AWS che utilizzi. 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.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare i singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il suo lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura la creazione di logo delle attività di API e utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza di default all'interno dei Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, ad esempio Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni identificative sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio un campo Nome. Ciò include quando lavori con Account Management o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i log di fatturazione o 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.

AWS PrivateLinkperAWSGestione dell'account

Se utilizzi Amazon Virtual Private Cloud (Amazon VPC) per ospitare il tuoAWSrisorse, puoi accedere allaAWSServizio di gestione account dall'interno del VPC senza dover attraversare Internet pubblico.

Amazon VPC ti consente di lanciareAWSrisorse in una rete virtuale personalizzata. Puoi utilizzare un VPC per controllare le impostazioni di rete, come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Per ulteriori informazioni sui VPC, consultaAmazon VPC User Guide.

Per connettere il tuo Amazon VPC a Gestione account, devi prima definire unendpoint VPC dell'interfaccia, che consente di connettere il VPC ad altriAWSServizi . L'endpoint offre una connettività scalabile e affidabile senza necessità di disporre di un gateway Internet, un'istanza NAT (Network Address Translation) o una connessione VPN. Per ulteriori informazioni, consulta Endpoint VPC di interfaccia (AWS PrivateLink) nella Guida per l'utente di Amazon VPC.

Creazione dell'endpoint

Puoi creare unaAWSEndpoint Gestione account nel tuo VPC utilizzando ilAWS Management Console, ilAWS Command Line Interface(AWS CLI), unAWSSDK, ilAWSAPI di gestione account, oAWS CloudFormation.

Per informazioni sulla creazione e sulla configurazione di un endpoint utilizzando la console Amazon VPC o il AWS CLI, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di Amazon VPC.

> **Note**
>
> Quando crei un endpoint, specifica Gestione account come servizio a cui desideri che il tuo VPC si connetta, utilizzando il seguente formato:
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> È necessario utilizzare la stringa esattamente come mostrato, specificando la`us-east-1`Regione . Come servizio globale, Account Management è ospitato solo in quelloAWSRegione .

Per informazioni sulla creazione e sulla configurazione di un endpoint utilizzando AWS CloudFormation, consulta la risorsa AWS::EC2::VPCEndpoint nella Guida per l'utente di AWS CloudFormation.

Policy di endpoint VPC di Amazon

Puoi controllare quali azioni possono essere eseguite tramite questo endpoint del servizio allegando una policy degli endpoint quando crei l'endpoint Amazon VPC. Puoi creare regole IAM complesse collegando più policy endpoint. Per ulteriori informazioni, consulta:

- Policy di endpoint di Amazon Virtual Private Cloud per l'
- Controllo dell'accesso ai servizi con endpoint VPCnellaAWS PrivateLinkGuida.

Policy di endpoint di Amazon Virtual Private Cloud per l'

Puoi creare una policy di endpoint VPC di Amazon per la Gestione dell'account in cui puoi specificare quanto segue:

- Il principale che può eseguire operazioni.
- Le azioni che le entità possono eseguire.
- Le risorse in cui è possibile eseguire le operazioni.

L'esempio seguente mostra un criterio degli endpoint Amazon VPC che consente a un utente IAM chiamato Alice nell'account 123456789012 di recuperare e modificare le informazioni di contatto alternative per qualsiasiAccount AWS, ma nega a tutti gli utenti IAM il permesso di eliminare qualsiasi informazione di contatto alternativa su qualsiasi account.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "account:GetAlternateContact",
                "account:PutAlternateContact"
            ],
            "Resource": "arn:aws::iam:*:account,
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": "arn:aws::iam:123456789012:user/Alice"
            }
        },
        {
            "Action": "account:DeleteAlternateContact",
            "Resource": "*",
            "Effect": "Deny",
            "Principal": "arn:aws::iam:*:root"
        }
    ]
}
```

Se desideri concedere l'accesso ad account che fanno parte di unaAWSOrganizzazione a un principale che si trova in uno degli account membri dell'organizzazione, quindi`Resource`l'elemento deve utilizzare il seguente formato:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Per ulteriori informazioni sulla creazione di policy di endpoint, consultaControllo dell'accesso ai servizi con endpoint VPCnellaAWS PrivateLinkGuida.

Identity and Access Management per la gestione degli AWS account

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 di Account Management. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come funziona la gestione degli AWS account con IAM
- Esempi di policy basate sull'identità per la gestione degli account AWS
- Utilizzo di politiche basate sull'identità (politiche IAM) per la gestione degli account AWS

- Risoluzione dei problemi relativi AWS all'identità e all'accesso alla gestione dell'account

Destinatari

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

Utente del servizio: se utilizzi il servizio di gestione degli account per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di gestione dell'account 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 in Gestione account, consultaRisoluzione dei problemi relativi AWS all'identità e all'accesso alla gestione dell'account.

Amministratore del servizio: se sei responsabile delle risorse di gestione degli account presso la tua azienda, probabilmente hai pieno accesso alla gestione degli account. È tuo compito determinare a quali funzionalità e risorse di gestione degli account 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 Account Management, consultaCome funziona la gestione degli AWS account con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere politiche per gestire l'accesso alla gestione degli account. Per visualizzare esempi di policy basate sull'identità di Account Management che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per la gestione degli account 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 sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

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

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

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di

utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

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

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

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

Ruoli IAM

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

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

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene

autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.
- Accesso tra servizi: alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli

collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

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

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

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

Policy basate su identità

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

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

Policy basate su risorse

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

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

Liste di controllo degli accessi (ACL)

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

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

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

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

Come funziona la gestione degli AWS account con IAM

Prima di utilizzare IAM per gestire l'accesso alla gestione degli account, scopri quali funzionalità IAM sono disponibili per l'uso con Account Management.

Funzionalità IAM che puoi utilizzare con AWS Account Management

Funzionalità IAM	Supporto per la gestione degli account
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
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una visione generale di come la gestione degli account e gli 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 la gestione degli account

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 azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente IAM.

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 la gestione degli account

Per visualizzare esempi di politiche basate sull'identità di Account Management, consulta. Esempi di policy basate sull'identità per la gestione degli account AWS

Politiche basate sulle risorse all'interno di Account Management

Supporta le policy basate su risorse	No

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

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 Cross Account Resource Access in IAM nella IAM User Guide.

Azioni politiche per la gestione degli account

Supporta le operazioni di policy	Sì

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

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

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

Per visualizzare un elenco delle azioni di gestione dell'account, consulta Azioni definite da AWS Account Management nel Service Authorization Reference.

Le azioni politiche in Account Management utilizzano il seguente prefisso prima dell'azione.

```
account
```

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

```
"Action": [
      "account:action1",
      "account:action2"
         ]
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che funzionano con i contatti alternativi Account AWS di un utente, includi l'azione seguente.

```
"Action": "account:*AlternateContact"
```

Per visualizzare esempi di politiche basate sull'identità di Account Management, consulta. Esempi di policy basate sull'identità per la gestione degli account AWS

Risorse politiche per la gestione degli account

Supporta le risorse di policy	Sì

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

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

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

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

Il servizio Account Management supporta i seguenti tipi di risorse specifici nell'`Resource`elemento di una policy IAM per aiutarti a filtrare la policy e distinguere tra questi tipi di: Account AWS

- account

  Questo `resource` tipo corrisponde solo agli account autonomi Account AWS che non sono membri di un'organizzazione gestita dal AWS Organizations servizio.
- accountInOrganization

  Questo `resource` tipo corrisponde solo Account AWS agli account membro di un'organizzazione gestita dal AWS Organizations servizio.

Per visualizzare un elenco dei tipi di risorse di Account Management e dei relativi ARN, consulta Risorse definite da AWS Account Management nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, vedere Azioni definite da AWS Account Management.

Per visualizzare esempi di politiche basate sull'identità di Account Management, consulta. Esempi di policy basate sull'identità per la gestione degli account AWS

Criteri relativi alle condizioni delle politiche per la gestione degli account

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. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

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

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

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

Il servizio Account Management supporta le seguenti chiavi di condizione che puoi utilizzare per fornire filtri dettagliati per le tue politiche IAM:

- conto: TargetRegion

  Questa chiave condizionale accetta un argomento costituito da un elenco di codici AWS regionali. Consente di filtrare la politica in modo da influire solo sulle azioni che si applicano alle regioni specificate.

- conto: AlternateContactTypes

  Questa chiave condizionale richiede un elenco di tipi di contatto alternativi:

  - FATTURAZIONE
  - OPERAZIONI
  - SECURITY

  L'utilizzo di questa chiave consente di filtrare la richiesta solo in base alle azioni destinate ai tipi di contatto alternativi specificati.

- conto: AccountResourceOrgPaths

  Questa chiave condizionale accetta un argomento costituito da un elenco di ARN con caratteri jolly che rappresentano gli account di un'organizzazione. Consente di filtrare la policy in modo da influire solo sulle azioni destinate agli account con ARN corrispondenti. Ad esempio, il seguente ARN corrisponde solo agli account dell'organizzazione specificata e dell'unità organizzativa (OU) specificata.

  ```
  arn:aws:account::111111111111:ou/o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
  ```

- conto: AccountResourceOrgTags

  Questa chiave condizionale accetta un argomento che consiste in un elenco di chiavi e valori di tag. Consente di filtrare la politica in modo da influire solo sugli account che sono membri di un'organizzazione e che sono contrassegnati con le chiavi e i valori dei tag specificati.

Per visualizzare un elenco delle chiavi di condizione di Account Management, consulta la sezione Chiavi di condizione per la gestione degli AWS account nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS Account Management.

Per visualizzare esempi di politiche basate sull'identità di Account Management, consulta. Esempi di policy basate sull'identità per la gestione degli account AWS

Accedi agli elenchi di controllo in Account Management

Supporta le ACL	No

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

Controllo degli accessi basato sugli attributi con Account Management

Supporta ABAC (tag nelle policy)	Sì

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 Che cos'è 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 Account Management

Supporta le credenziali temporanee	Sì

Alcune 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 accedi AWS utilizzando il link Single Sign-On (SSO) della tua 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 Cambio di un ruolo (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 per tutti i servizi per la gestione degli account

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

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 la pagina Forward access sessions.

Ruoli di servizio per la gestione degli account

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 Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

Ruoli collegati al servizio per la gestione degli account

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 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.

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 la gestione degli account AWS

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare le risorse di gestione degli account. 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 nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Account Management, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per la gestione degli AWS account nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzando la pagina Account nel AWS Management Console
- Fornendo l'accesso in sola lettura alla pagina Account nel AWS Management Console
- Fornire l'accesso completo alla pagina Account nel AWS Management Console

Best practice per le policy

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

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

Utilizzando la pagina Account nel AWS Management Console

Per accedere alla pagina Account di AWS Management Console, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli relativi ai tuoi. Account AWS Se crei una policy basata su identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti e ruoli IAM) associate a tale policy.

Per garantire che utenti e ruoli possano utilizzare la console di gestione dell'account, puoi scegliere di allegare la policy `AWSAccountManagementReadOnlyAccess` o la policy `AWSAccountManagementFullAccess` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Non è necessario consentire le autorizzazioni minime della console per gli utenti che effettuano chiamate solo alla AWS CLI o AWS all'API. Invece, in molti casi puoi scegliere di consentire l'accesso solo alle azioni che corrispondono alle operazioni API che stai cercando di eseguire.

Fornendo l'accesso in sola lettura alla pagina Account nel AWS Management Console

Nell'esempio seguente, desideri concedere a un utente IAM in modalità di sola lettura l'accesso in Account AWS sola lettura alla pagina Account in. AWS Management Console Gli utenti a cui è associata questa policy non possono apportare modifiche.

L'`account:GetAccountInformation`azione consente l'accesso alla visualizzazione della maggior parte delle impostazioni nella pagina Account. Tuttavia, per visualizzare le AWS regioni attualmente abilitate, è necessario includere anche l'`account:ListRegions`azione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantReadOnlyAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Fornire l'accesso completo alla pagina Account nel AWS Management Console

Nell'esempio seguente, desideri concedere a un utente IAM l'accesso Account AWS completo alla pagina Account in AWS Management Console. Gli utenti a cui è associata questa politica possono modificare le impostazioni dell'account.

Questo criterio di esempio si basa sul criterio di esempio precedente aggiungendo tutti i permessi di scrittura disponibili (ad eccezione di CloseAccount), il che consente all'utente di modificare la maggior parte delle impostazioni dell'account, incluse le `account:EnableRegion` autorizzazioni and. `account:DisableRegion`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GrantFullAccessToAccountSettings",
            "Effect": "Allow",
            "Action": [
                "account:GetAccountInformation",
                "account:ListRegions",
                "account:PutContactInformation",
                "account:PutChallengeQuestions",
                "account:PutAlternateContact",
                "account:DeleteAlternateContact",
                "account:EnableRegion",
                "account:DisableRegion"
            ],
            "Resource": "*"
        }
    ]
}
```

Utilizzo di politiche basate sull'identità (politiche IAM) per la gestione degli account AWS

Per una discussione completa sugli AWS account e sugli utenti IAM, consulta Che cos'è IAM? nella Guida per l'utente IAM.

Per istruzioni su come aggiornare le policy gestite dal cliente, vedi Modifica delle policy gestite dal cliente (console) nella Guida per l'utente do IAM.

AWS Politiche relative alle azioni di gestione degli account

Questa tabella riassume le autorizzazioni che garantiscono l'accesso alle impostazioni dell'account. Per esempi di politiche che utilizzano queste autorizzazioni, consulta Esempi di politiche di gestione degli AWS account.

> **Note**
>
> Per concedere agli utenti IAM l'accesso in scrittura a una specifica impostazione dell'account nella pagina Account di AWS Management Console, devi consentire l'`GetAccountInformation`autorizzazione, oltre all'autorizzazione (o alle autorizzazioni) che desideri utilizzare per modificare tale impostazione.

Nome autorizzazione	Livello di accesso	Descrizione
`account:ListRegions`	Elenco	Concede l'autorizzazione a elencare le regioni disponibili.
`account:GetAccount Information`	Lettura	Concede l'autorizzazione a recuperare le informazioni relative a un account.
`account:GetAlterna teContact`	Lettura	Concede l'autorizzazione a recuperare i contatti alternativi per un account.
`account:GetChallen geQuestions`	Lettura	Concede l'autorizzazione a recuperare le domande della sfida per un account.
`account:GetContact Information`	Lettura	Concede l'autorizzazione a recuperare le informazioni di contatto principali di un account.

Nome autorizzazione	Livello di accesso	Descrizione
`account:GetRegionOptStatus`	Lettura	Concede l'autorizzazione a ottenere lo status di opt-in di una regione.
`account:AcceptPrimaryEmailUpdate`	Scrittura	Concede l'autorizzazione ad accettare l'aggiornamento dell'indirizzo e-mail principal e dell'account membro di un'organizzazione. AWS
`account:CloseAccount`	Scrittura	Concede l'autorizzazione a chiudere un account. **Note** Questa autorizzazione vale solo per la console. Per questa autorizzazione non è disponibile alcun accesso API.
`account:DeleteAlternateContact`	Scrittura	Concede l'autorizzazione a eliminare i contatti alternativi per un account.
`account:DisableRegion`	Scrittura	Concede l'autorizzazione a disabilitare l'uso di una regione.
`account:EnableRegion`	Scrittura	Concede l'autorizzazione per consentire l'uso di una regione.

Nome autorizzazione	Livello di accesso	Descrizione
`account:PutAlternateContact`	Scrittura	Concede l'autorizzazione a modificare i contatti alternativi per un account.
`account:PutChallengeQuestions`	Scrittura	Concede l'autorizzazione a modificare le domande della sfida per un account. **Note** Questa autorizzazione vale solo per la console. Per questa autorizzazione non è disponibile alcun accesso API.
`account:PutContactInformation`	Scrittura	Concede l'autorizzazione ad aggiornare le informazioni di contatto principali di un account.
`account:StartPrimaryEmailUpdate`	Scrittura	Concede l'autorizzazione ad avviare l'aggiornamento dell'indirizzo e-mail principale dell'account membro in un'organizzazione. AWS

Risoluzione dei problemi relativi AWS all'identità e all'accesso alla gestione dell'account

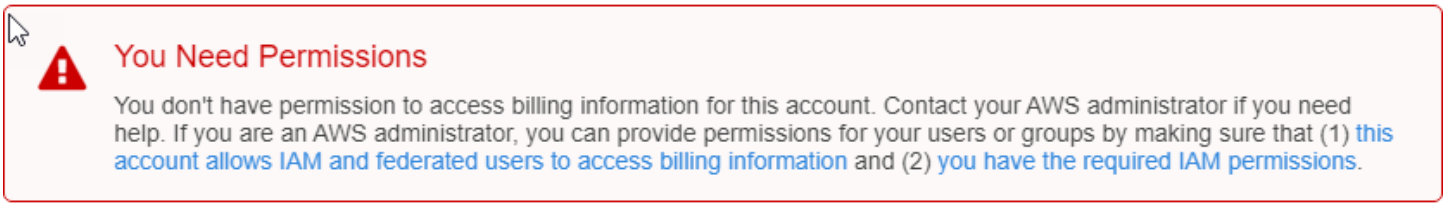
Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Account Management e IAM.

Argomenti

Non sono autorizzato a eseguire alcuna azione nella pagina Account

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

Il seguente errore di esempio si verifica quando l'utente `mateojackson` IAM tenta di utilizzare la console per visualizzare i dettagli sul proprio account Account AWS nella pagina Account di AWS Management Console ma non dispone delle `account:GetAccountInformation` autorizzazioni.



In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *`my-example-widget`* utilizzando l'azione `account:`*`GetWidget`*.

Non sono autorizzato a eseguire **`iam:PassRole`**

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di assegnare un ruolo alla gestione dell'account.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Account Management. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne al mio account di accedere Account AWS ai dettagli del mio account

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Account Management supporta queste funzionalità, consultaCome funziona la gestione degli AWS account 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 scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta Cross Account Resource Access in IAM nella IAM User Guide.

AWSpolitiche gestite perAWSGestione dell'account

AWSAccount Management attualmente ne fornisce dueAWSpolitiche gestite disponibili per l'uso:

- AWSPolicy gestita: AWSAccountManagementReadOnlyAccess
- AWSPolicy gestita: AWSAccountManagementFullAccess

- Aggiornamenti di Account Management aAWSpolitiche gestite

Una policy gestita da AWS è una policy autonoma creata e amministrata da AWS. Le policy gestite da AWS sono progettate per fornire autorizzazioni per molti casi d'uso comuni in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Ricorda che le policy gestite da AWS potrebbero non concedere autorizzazioni con privilegi minimi per i tuoi casi d'uso specifici perché possono essere utilizzate da tutti i clienti AWS. Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle policy gestite da AWS. Se AWS aggiorna le autorizzazioni definite in una policy gestita da AWS, l'aggiornamento riguarda tutte le identità principali (utenti, gruppi e ruoli) a cui è collegata la policy. È molto probabile che AWS aggiorni una policy gestita da AWS quando viene lanciato un nuovo Servizio AWS o nuove operazioni API diventano disponibili per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

AWSPolicy gestita: AWSAccountManagementReadOnlyAccess

È possibile allegare la policy `AWSAccountManagementReadOnlyAccess` alle identità IAM.

Questa politica fornisce autorizzazioni di sola lettura per visualizzare solo quanto segue:

- I metadati relativi al tuoAccount AWS
- LaRegioni AWSche sono abilitati o disattivati perAccount AWS(puoi visualizzare lo stato delle regioni nel tuo account solo utilizzando ilAWSconsolle)

Lo fa concedendo il permesso di eseguire uno qualsiasi dei`Get*`o`List*`operazioni. Non offre alcuna possibilità di modificare i metadati dell'account o abilitare o disabilitareRegioni AWSper l'account.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `account`— Consente ai responsabili di recuperare le informazioni sui metadati suAccount AWS. Consente inoltre ai presidi di elencare iRegioni AWSche sono abilitati per l'account nelAWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "account:Get*",
                "account:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSPolicy gestita: AWSAccountManagementFullAccess

È possibile allegare la policy `AWSAccountManagementFullAccess` alle identità IAM.

Questa politica fornisce l'accesso amministrativo completo per visualizzare o modificare quanto segue:

- I metadati relativi al tuoAccount AWS
- LaRegioni AWSche sono abilitati o disattivati perAccount AWS(puoi visualizzare lo stato o abilitare o disabilitare le Regioni per il tuo account solo utilizzando ilAWSconsolle)

Lo fa concedendo il permesso di eseguire qualsiasi`account`operazioni.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `account`— Consente ai responsabili di visualizzare o modificare le informazioni sui metadati suAccount AWS. Consente inoltre ai presidi di elencare iRegioni AWSche sono abilitati per l'account e che li abilitano o li disattivano nelAWS Management Console.

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

```
            "Action": "account:*",
            "Resource": "*"
        }
    ]
}
```

Aggiornamenti di Account Management aAWSpolitiche gestite

Visualizza i dettagli sugli aggiornamenti diAWSpolitiche gestite per la gestione degli account da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina Cronologia dei documenti di gestione dell'account.

Modifica	Descrizione	Data
AWSLa gestione degli account è stata lanciata con una nuovaAWSpolitiche gestite e iniziato a tracciare le modifiche	Account Management è stato inizialmente lanciato con quanto segueAWSpolitiche gestite: • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	30 settembre 2021

Convalida della conformità per la gestione AWS dell'account

I revisori di terze parti valutano la sicurezza e la conformità dei AWS servizi che possono essere eseguiti presso di voi nell'Account AWSambito di diversi programmi di AWS conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei AWS servizi che rientrano nell'ambito di programmi di conformità specifici, vedere Servizi AWSScope by compliance program Servizi AWS . Per informazioni generali, consulta Programmi per la conformità di AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, vedere Scaricamento dei report nella sezione AWS Artifact Guida per l'AWS Artifactutente.

La responsabilità di conformità dell'utente nell'utilizzo dei servizi Account AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWSfornisce le seguenti risorse per contribuire alla conformità:

- Guide Quick Start per la sicurezza e conformità: queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono la procedura per l'implementazione di ambienti di base su AWS incentrati sulla sicurezza e sulla conformità.
- Architetture per la sicurezza e la conformità HIPAA su Amazon Web Services: questo whitepaper descrive come le aziende possono utilizzare AWS per creare applicazioni conformi alla normativa HIPAA.

> **Note**
>
> Non tutti i Servizi AWS sono conformi ai requisiti HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Valutazione delle risorse con le regole nella Guida per lo sviluppatore di AWS Config: il servizio AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.
- AWS Audit Manager: questo Servizio AWS aiuta a verificare continuamente l'utilizzo di AWS per semplificare la gestione dei rischi e della conformità alle normative e agli standard di settore.

Resilienza inAWSGestione dell'account

LaAWSl'infrastruttura globale di è basata suRegioni AWSe zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura in AWS Account Management

In quanto servizi gestiti, AWS i servizi in esecuzione nel tuo sistema Account AWS sono protetti dalla sicurezza AWS globale della rete. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Le chiamate API AWS pubblicate vengono utilizzate per accedere alle impostazioni dell'account tramite la rete. I clienti devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

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

Monitoraggio della gestione degli AWS account

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Account Management e delle altre AWS soluzioni. AWSfornisce i seguenti strumenti di monitoraggio per monitorare la gestione degli account, segnalare quando qualcosa non va e intraprendere azioni automatiche se necessario:

- AWS CloudTrailacquisisce (registra) le chiamate API e gli eventi correlati effettuati da o per conto tuo Account AWS e scrive i file di log in un bucket Amazon Simple Storage Service (Amazon S3) da te specificato. Ciò consente di identificare gli utenti e gli account chiamatiAWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.
- Amazon EventBridge aggiunge ulteriore automazione ai tuoi AWS servizi rispondendo automaticamente agli eventi di sistema, come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali operazioni automatizzate intraprendere quando un evento corrisponde a una regola. Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

Registrazione di logAWSChiamate API di gestione dell'account conAWS CloudTrail

LaAWSLe API di Account Management sono integrate conAWS CloudTrailun servizio che fornisce un record delle operazioni eseguite da un utente, un ruolo o unAWSservizio che chiama un'operazione di Gestione account. CloudTrail acquisisce tutte le chiamate API di Account Management come eventi. Le chiamate acquisite includono tutte le chiamate alle operazioni di Gestione account. Se crei un percorso, puoi abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per le operazioni di Gestione account. Se non si configura un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta che ha chiamato un'operazione di Account Management, l'indirizzo IP utilizzato per effettuare la richiesta, l'autore della richiesta e il momento in cui e altri dettagli.

Per ulteriori informazioni su CloudTrail, consultare la AWS CloudTrailGuida per l'utente di .

Informazioni sulla gestione degli account in CloudTrail

CloudTrail è abilitato nella tuaAccount AWSquando crei l'account. Quando si verifica un'attività con un'operazione di Gestione account, CloudTrail registra questa in un evento CloudTrail insieme ad altri.AWSeventi di servizi inCronologia eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia eventi di CloudTrail.

Per una registrazione continuativa di attività ed eventi nella tuaAccount AWS, inclusi gli eventi per le operazioni di Account Management, crea un trail. Un trail consente a CloudTrail di distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando crei un trail nellaAWS Management Console, il sentiero si applica a tuttiRegioni AWS. Il trail registra gli eventi di tutte le regioni nella partizione AWS e distribuisce i file di registro nel bucket Amazon S3 specificato. Puoi configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei registri CloudTrail. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail supported services and integrations (Servizi e integrazioni CloudTrail supportati)
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di log CloudTrail da più regioni
- Ricezione di file di log CloudTrail da più account

AWS CloudTrailregistra tutte le operazioni dell'API di Account Management trovate nelDocumentazione di riferimento APIsezione di questa guida. Ad esempio, le chiamate alle operazioni `CreateAccount`, `DeleteAlternateContact` e `PutAlternateContact` generano voci nei file di log di CloudTrail.

Ogni evento o voce del registro 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 l'utente root oAWS Identity and Access Managementcredenziali utente (IAM)
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo IAM o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci del registro di Account Management

Un trail è una configurazione che consente l'implementazione di eventi come i file di log in un bucket Amazon S3 che specifichi. I file di registro di CloudTrail possono contenere una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'operazione desiderata, la data e l'ora della stessa, i parametri della richiesta e così via. I file di log CloudTrail non sono una traccia di pila ordinata delle chiamate API pubbliche e di conseguenza non devono apparire in base a un ordine specifico.

Esempio 1: L'esempio seguente mostra una voce di log di CloudTrail per una chiamata alla`GetAlternateContact`operazione per recuperare la corrente`OPERATIONS`contatto alternativo per un account. I valori restituiti dall'operazione non sono inclusi nelle informazioni registrate.

Example Esempio 1


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
```

```
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "SECURITY"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Esempio 2: L'esempio seguente mostra una voce di log di CloudTrail per una chiamata alla`PutAlternateContact`operazione per aggiungere un nuovo`BILLING`contatto alternativo a un account.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
```

```
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "PutAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "name": "*Alejandro Rosalez*",
    "emailAddress": "alrosalez@example.com",
    "title": "CFO",
    "alternateContactType": "BILLING"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

Esempio 3: L'esempio seguente mostra una voce di log di CloudTrail per una chiamata alla`DeleteAlternateContact`operazione per eliminare la corrente`OPERATIONS`contatto alternativo.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA1234567890EXAMPLE:AccountAPITests",
    "arn":"arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROA1234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
```

```
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:16Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "DeleteAlternateContact",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.24.34.250",
  "userAgent": "Mozilla/5.0",
  "requestParameters": {
    "alternateContactType": "OPERATIONS"
  },
  "responseElements": null,
  "requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
  "eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```


Monitoraggio degli eventi di gestione degli account con EventBridge

Amazon EventBridge, precedentemente chiamato CloudWatch Events, ti aiuta a monitorare eventi specifici e ad avviare azioni mirate che utilizzano altri. Servizi AWS Gli eventi di Servizi AWS vengono trasmessi quasi EventBridge in tempo reale.

In questo modo è possibile creare regole che corrispondano agli eventi in arrivo e indirizzarli verso le destinazioni per l'elaborazione. EventBridge

Per ulteriori informazioni, consulta la sezione Guida introduttiva ad Amazon EventBridge nella Amazon EventBridge User Guide.

Eventi di gestione dell'account

Gli esempi seguenti mostrano gli eventi per la gestione degli account. Gli eventi vengono prodotti nel miglior modo possibile.

Solo gli eventi specifici per l'attivazione e la disabilitazione delle regioni e delle chiamate API CloudTrail sono attualmente disponibili per la gestione degli account.

Event types (Tipi di evento)

- Evento per l'attivazione e la disabilitazione delle regioni

Evento per l'attivazione e la disabilitazione delle regioni

Quando abiliti o disabiliti una regione in un account, dalla console o dall'API, viene avviata un'attività asincrona. La richiesta iniziale verrà registrata come CloudTrail evento nell'account di destinazione. Inoltre, un EventBridge evento verrà inviato all'account chiamante all'avvio del processo di attivazione o disabilitazione e nuovamente una volta completato uno dei due processi.

L'evento di esempio seguente mostra come verrà inviata una richiesta indicante che `2020-09-30` nella `ap-east-1` regione si riferiva `ENABLED` all'account`123456789012`.

```
{
   "version":"0",
   "id":"11112222-3333-4444-5555-666677778888",
   "detail-type":"Region Opt-In Status Change",
   "source":"aws.account",
   "account":"123456789012",
   "time":"2020-09-30T06:51:08Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:account::123456789012:account"
   ],
   "detail":{
      "accountId":"123456789012",
      "regionName":"ap-east-1",
      "status":"ENABLED"
   }
}
```

Esistono quattro stati possibili che corrispondono agli stati restituiti dalle API `GetRegionOptStatus` and`ListRegions`:

- `ENABLED`— La regione è stata abilitata con successo per quanto indicato `accountId`
- `ENABLING`— La Regione è in procinto di essere abilitata per `accountId` quanto indicato
- `DISABLED`— La Regione è stata disabilitata con successo per `accountId` quanto indicato

- `DISABLING`— La Regione è in fase di disabilitazione per `accountId` quanto indicato

Il seguente modello di evento di esempio crea una regola che acquisisce tutti gli eventi della regione.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ]
}
```

Il seguente modello di eventi di esempio crea una regola che acquisisce solo gli eventi `ENABLED` `DISABLED` regionali.

```
{
   "source":[
      "aws.account"
   ],
   "detail-type":[
      "Region Opt-In Status Change"
   ],
   "detail":{
      "status":[
         "DISABLED",
         "ENABLED"
      ]
   }
}
```

Documentazione di riferimento delle API

Le operazioni API nella gestione degli account (`account`) namespace ti consente di modificare il tuoAccount AWS.

OgniAccount AWSsupporta metadati con informazioni sull'account, incluse informazioni su un massimo di tre contatti alternativi associati all'account. Questi sono in aggiunta all'indirizzo e-mail associato alutente rootdell'account. È possibile specificare solo uno dei seguenti tipi di contatto associati a un account.

- Contatto per la fatturazione
- Contatto operativo
- Contatto di sicurezza

Per impostazione predefinita, le operazioni API descritte in questa guida si applicano direttamente all'account che chiama l'operazione. Laidentitànell'account che sta chiamando l'operazione c'è in genere un ruolo IAM o un utente IAM e deve avere l'autorizzazione applicata da una policy IAM per chiamare l'operazione API. In alternativa, puoi richiamare queste operazioni API da un'identità in unAWS Organizationsaccount di gestione e specifica il numero ID dell'account per ogni accountAccount AWSche è un membro dell'organizzazione.

Versione API

Questa versione di Accounts API Reference documenta la versione dell'API di gestione degli account 2021-02-01.

> **Note**
>
> In alternativa all'utilizzo diretto dell'API, puoi utilizzare uno deiAWSSDK, che consistono in librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (Java, Ruby, .NET, iOS, Android e altro). Gli SDK forniscono un modo conveniente per creare un accesso programmatico aAWSOrganizzazioni. Ad esempio, gli SDK si occupano della firma crittografica delle richieste, della gestione degli errori e dei tentativi automatici delle richieste. Per ulteriori informazioni sugli SDK AWS, inclusi i dettagli su come scaricarli e installarli, consulta la pagina relativa agli strumenti per Amazon Web Services.

Ti consigliamo di utilizzare ilAWSSDK per effettuare chiamate API programmatiche al servizio Account Management. Tuttavia, puoi anche utilizzare l'API Account Management Query per effettuare chiamate dirette al servizio web Account Management. Per ulteriori informazioni sull'API Account Management Query, consultaChiamata dell'API tramite richieste di query HTTPnella Guida per l'utente di Account Management. Le organizzazioni supportano le richieste GET e POST per tutte le azioni. Questo significa che l'API non richiede l'uso di GET per alcune operazioni e di POST per altre. Tuttavia, le richieste GET sono soggette alla limitazione delle dimensioni di un URL. Pertanto, per operazioni che richiedono dimensioni maggiori, utilizza una richiesta POST.

Firma delle richieste

Quando invii richieste HTTP aAWS, devi firmare le richieste in modo cheAWSpuò identificare chi li ha inviati. Firmi le richieste con il tuoAWSchiave di accesso, che consiste in un ID chiave di accesso e una chiave di accesso segreta. Ti consigliamo vivamente di non creare una chiave di accesso per il tuo account root. Chiunque disponga della chiave di accesso per il tuo account root ha accesso illimitato a tutte le risorse del tuo account. Crea invece una chiave di accesso per un utente IAM con privilegi amministrativi. Come altra opzione, usaAWSSecurity Token Service per generare credenziali di sicurezza temporanee e utilizzare tali credenziali per firmare le richieste.

Per firmare le richieste, ti consigliamo di utilizzare la versione Signature 4. Se disponi di un'applicazione esistente che utilizza Signature Version 2, non devi aggiornarla per utilizzare Signature Version 4. Tuttavia, alcune operazioni ora richiedono la versione Signature 4. La documentazione per le operazioni che richiedono la versione 4 indica questo requisito. Per ulteriori informazioni, consulta la pagina Firma delle richieste API AWS nella Guida per l'utente IAM.

Quando si utilizza ilAWSInterfaccia a riga di comando (AWSCLI) o uno deiAWSSDK a cui inviare richiesteAWS, questi strumenti firmano automaticamente le richieste dell'utente con la chiave di accesso specificata durante la configurazione degli strumenti.

Supporto e feedback per la gestione degli account

Apprezziamo il tuo feedback. Invia i tuoi commenti afeedback-awsaccounts@amazon.comoppure pubblica il tuo feedback e le tue domande nelForum di supporto per la gestione degli account. Per ulteriori informazioni sui forum di supporto di AWS consulta la guida dei forum.

Come vengono presentati gli esempi

Il JSON restituito dalla Gestione dell'account come risposta alle tue richieste viene restituito come un'unica stringa lunga senza interruzioni di riga o spazi bianchi di formattazione. Sia le interruzioni di riga che gli spazi bianchi sono mostrati negli esempi di questa guida per migliorare la leggibilità.

Quando i parametri di input di esempio generano anche stringhe lunghe che si estendono oltre lo schermo, inseriamo interruzioni di riga per migliorare la leggibilità. Dovresti sempre inviare l'input come singola stringa di testo JSON.

Registrazione delle richieste API

Supporti per la gestione degli accountCloudTrail, un servizio che registraAWSChiamate API per i tuoiAccount AWSe invia i file di registro a un bucket Amazon S3. Utilizzando le informazioni raccolte daCloudTrail, puoi determinare quali richieste sono state inoltrate correttamente a Account Management, chi ha effettuato la richiesta, quando è stata effettuata e così via. Per ulteriori informazioni sulla gestione degli account e sul supporto perCloudTrail, vediRegistrazione di logAWSChiamate API di gestione dell'account conAWS CloudTrail. Per saperne di più suCloudTrail, incluso come attivarlo e trovare i file di registro, consulta laAWS CloudTrailGuida per l'utente.

Azioni

Sono supportate le operazioni seguenti:

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAlternateContact
- GetContactInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAlternateContact
- PutContactInformation
- StartPrimaryEmailUpdate

AcceptPrimaryEmailUpdate

Accetta la richiesta originata da StartPrimaryEmailUpdate per aggiornare l'indirizzo e-mail principale (noto anche come indirizzo e-mail dell'utente root) per l'account specificato.

Sintassi della richiesta

```
POST /acceptPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "Otp": "string",
   "PrimaryEmail": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificate il numero ID dell'account a 12 cifre del quale desiderate accedere o modificare con Account AWS questa operazione. Per utilizzare questo parametro, il chiamante deve avere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato. L'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

Questa operazione può essere richiamata solo dall'account di gestione o dall'account amministratore delegato di un'organizzazione per un account membro.

> **Note**
>
> L'account di gestione non può specificare il proprio. `AccountId`

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: sì

Otp

Il codice OTP inviato all'indirizzo `PrimaryEmail` specificato nella chiamata `StartPrimaryEmailUpdate` API.

Tipo: stringa

Modello: `^[a-zA-Z0-9]{6}$`

Campo obbligatorio: sì

PrimaryEmail

Il nuovo indirizzo e-mail principale da utilizzare con l'account specificato. Deve corrispondere `PrimaryEmail` a quello della chiamata `StartPrimaryEmailUpdate` API.

-Tipo: stringa

Vincoli di lunghezza: lunghezza minima di 5. La lunghezza massima è 64 caratteri.

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "Status": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Status

Recupera lo stato della richiesta di aggiornamento e-mail principale accettata.

- Tipo: stringa

Valori validi: `PENDING | ACCEPTED`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

ConflictException

La richiesta non può essere elaborata a causa di un conflitto nello stato corrente della risorsa. Ad esempio, ciò accade se si tenta di abilitare una regione attualmente disabilitata (con lo stato di DISABILITAZIONE) o se si tenta di modificare l'e-mail dell'utente root di un account con un indirizzo e-mail già in uso.

Codice di stato HTTP: 409

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Riprova l'operazione più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

L'operazione non è riuscita perché ha specificato una risorsa che non può essere trovata.

Codice di stato HTTP: 404

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DeleteAlternateContact

Elimina il contatto alternativo specificato da un. Account AWS

Per informazioni complete su come utilizzare le operazioni relative ai contatti alternativi, vedere Accesso o aggiornamento dei contatti alternativi.

> **Note**
>
> Prima di poter aggiornare le informazioni di contatto alternative per un Account AWS account gestito da AWS Organizations, devi prima abilitare l'integrazione tra AWS Account Management e Organizations. Per ulteriori informazioni, vedere Abilitazione dell'accesso affidabile per la gestione degli AWS account.

Sintassi della richiesta

```
POST /deleteAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificate il numero ID dell'account a 12 cifre dell' AWS account a cui desiderate accedere o modificare con questa operazione.

Se non si specifica questo parametro, per impostazione predefinita viene utilizzato l' AWS account dell'identità utilizzata per chiamare l'operazione.

Per utilizzare questo parametro, il chiamante deve essere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato e l'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

> **Note**
>
> L'account di gestione non può specificare il proprio`AccountId`; deve chiamare l'operazione in un contesto autonomo escludendo il parametro. `AccountId`

Per richiamare questa operazione su un account che non è membro di un'organizzazione, non specificate questo parametro e richiamate l'operazione utilizzando un'identità appartenente all'account di cui desiderate recuperare o modificare i contatti.

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: no

AlternateContactType

Speciifica quali contatti alternativi eliminare.

-Tipo: stringa

Valori validi: `BILLING | OPERATIONS | SECURITY`

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Ripetere l'operazione più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

L'operazione non è riuscita perché ha specificato una risorsa che non può essere trovata.

Codice di stato HTTP: 404

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Esempi

Esempio 1

L'esempio seguente elimina il contatto alternativo di sicurezza per l'account le cui credenziali vengono utilizzate per chiamare l'operazione.

Richiesta di esempio

```
POST / HTTP/1.1
```

```
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AlternateContactType": "SECURITY" }
```

Risposta di esempio

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Esempio 2

L'esempio seguente elimina il contatto alternativo di fatturazione per l'account membro specificato in un'organizzazione. È necessario utilizzare le credenziali dell'account di gestione dell'organizzazione o dell'account amministratore delegato del servizio di gestione degli account.

Richiesta di esempio

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "BILLING" }
```

Risposta di esempio

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript

- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

DisableRegion

Disattiva (disattiva) una particolare regione per un account.

> **Note**
>
> La disattivazione di una regione rimuoverà tutti gli accessi IAM a tutte le risorse che risiedono in quella regione.

Sintassi della richiesta

```
POST /disableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificare il numero ID dell'account a 12 cifre a Account AWS cui si desidera accedere o modificare con questa operazione. Se non specifichi questo parametro, il valore predefinito è l'account Amazon Web Services dell'identità utilizzata per chiamare l'operazione. Per utilizzare questo parametro, il chiamante deve essere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato. L'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

> **Note**
>
> L'account di gestione non può specificare il proprio. `AccountId` Deve chiamare l'operazione in un contesto autonomo escludendo il `AccountId` parametro.

Per chiamare questa operazione su un account che non è membro di un'organizzazione, non specificare questo parametro. Chiamate invece l'operazione utilizzando un'identità appartenente all'account di cui desiderate recuperare o modificare i contatti.

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: no

RegionName

Specificate il codice regionale per un determinato nome di regione (ad esempio,). `af-south-1` Quando disabiliti una regione, AWS esegue azioni per disattivare quella regione nel tuo account, come la distruzione delle risorse IAM nella regione. Questo processo richiede pochi minuti per la maggior parte degli account, ma potrebbero essere necessarie anche diverse ore. Non puoi abilitare la regione fino al completamento del processo di disabilitazione.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

ConflictException

La richiesta non può essere elaborata a causa di un conflitto nello stato corrente della risorsa. Ad esempio, ciò accade se si tenta di abilitare una regione attualmente disabilitata (con lo stato di DISABILITAZIONE) o se si tenta di modificare l'e-mail dell'utente root di un account con un indirizzo e-mail già in uso.

Codice di stato HTTP: 409

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Ripetere l'operazione più tardi.

Codice di stato HTTP: 500

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++

- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

EnableRegion

Abilita (attiva) una regione particolare per un account.

Sintassi della richiesta

```
POST /enableRegion HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificare il numero ID dell'account a 12 cifre a Account AWS cui si desidera accedere o modificare con questa operazione. Se non specifichi questo parametro, il valore predefinito è l'account Amazon Web Services dell'identità utilizzata per chiamare l'operazione. Per utilizzare questo parametro, il chiamante deve essere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato. L'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

> **Note**
>
> L'account di gestione non può specificare il proprio. `AccountId` Deve chiamare l'operazione in un contesto autonomo escludendo il `AccountId` parametro.

Per chiamare questa operazione su un account che non è membro di un'organizzazione, non specificare questo parametro. Chiamate invece l'operazione utilizzando un'identità appartenente all'account di cui desiderate recuperare o modificare i contatti.

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: no

RegionName

Specificate il codice regionale per un determinato nome di regione (ad esempio,). `af-south-1` Quando si abilita una regione, AWS esegue delle operazioni per preparare l'account in quella regione, ad esempio distribuendo le risorse IAM nella regione. Questo processo richiede alcuni minuti per la maggior parte degli account, ma può richiedere diverse ore. Non è possibile utilizzare la regione finché il processo viene completato. Inoltre, non è possibile disabilitare la regione fino al completamento del processo di abilitazione.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

ConflictException

La richiesta non può essere elaborata a causa di un conflitto nello stato corrente della risorsa. Ad esempio, ciò accade se si tenta di abilitare una regione attualmente disabilitata (con lo stato di DISABILITAZIONE) o se si tenta di modificare l'e-mail dell'utente root di un account con un indirizzo e-mail già in uso.

Codice di stato HTTP: 409

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Riprova l'operazione più tardi.

Codice di stato HTTP: 500

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3

- AWS SDK per Python
- AWS SDK per Ruby V3

GetAlternateContact

Recupera il contatto alternativo specificato collegato a un. Account AWS

Per informazioni complete su come utilizzare le operazioni relative ai contatti alternativi, vedere Accesso o aggiornamento dei contatti alternativi.

> **Note**
>
> Prima di poter aggiornare le informazioni di contatto alternative per un Account AWS account gestito da AWS Organizations, devi prima abilitare l'integrazione tra AWS Account Management e Organizations. Per ulteriori informazioni, vedere Abilitazione dell'accesso affidabile per la gestione degli AWS account.

Sintassi della richiesta

```
POST /getAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificate il numero ID dell'account a 12 cifre dell' AWS account a cui desiderate accedere o modificare con questa operazione.

Se non si specifica questo parametro, per impostazione predefinita viene utilizzato l' AWS account dell'identità utilizzata per chiamare l'operazione.

Per utilizzare questo parametro, il chiamante deve essere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato e l'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

> **Note**
>
> L'account di gestione non può specificare il proprio`AccountId`; deve chiamare l'operazione in un contesto autonomo escludendo il parametro. `AccountId`

Per richiamare questa operazione su un account che non è membro di un'organizzazione, non specificate questo parametro e richiamate l'operazione utilizzando un'identità appartenente all'account di cui desiderate recuperare o modificare i contatti.

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: no

AlternateContactType

Specificate quale contatto alternativo desiderate recuperare.

-Tipo: stringa

Valori validi: `BILLING | OPERATIONS | SECURITY`

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "AlternateContact": {
      "AlternateContactType": "string",
      "EmailAddress": "string",
```

```
        "Name": "string",
        "PhoneNumber": "string",
        "Title": "string"
    }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

AlternateContact

Una struttura che contiene i dettagli per il contatto alternativo specificato.

Tipo: oggetto AlternateContact

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Ripetere l'operazione più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

L'operazione non è riuscita perché ha specificato una risorsa che non può essere trovata.

Codice di stato HTTP: 404

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Esempi

Esempio 1

L'esempio seguente recupera il contatto alternativo di sicurezza per l'account le cui credenziali vengono utilizzate per chiamare l'operazione.

Richiesta di esempio

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AlternateContactType": "SECURITY" }
```

Risposta di esempio

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Security"
    }
}
```

Esempio 2

L'esempio seguente recupera il contatto alternativo operativo per l'account membro specificato in un'organizzazione. È necessario utilizzare le credenziali dell'account di gestione dell'organizzazione o dell'account amministratore delegato del servizio di gestione degli account.

Richiesta di esempio

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{ "AccountId": "123456789012", "AlternateContactType": "Operations" }
```

Risposta di esempio

```
HTTP/1.1 200 OK
Content-Type: application/json{
   "AlternateContact": {
        "Name": "Anika",
        "Title": "COO",
        "EmailAddress": "anika@example.com",
        "PhoneNumber": "206-555-0198"
        "AlternateContactType": "Operations"
    }
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetContactInformation

Recupera le informazioni di contatto principali di un Account AWS.

Per i dettagli completi su come utilizzare le operazioni di contatto principale, vedi Aggiornare le informazioni di contatto principali e alternative.

Sintassi della richiesta

```
POST /getContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificare il numero ID dell'account a 12 cifre a Account AWS cui si desidera accedere o modificare con questa operazione. Se non specifichi questo parametro, il valore predefinito è l'account Amazon Web Services dell'identità utilizzata per chiamare l'operazione. Per utilizzare questo parametro, il chiamante deve essere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato. L'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

> **Note**
>
> L'account di gestione non può specificare il proprio. `AccountId` Deve chiamare l'operazione in un contesto autonomo escludendo il `AccountId` parametro.

Per chiamare questa operazione su un account che non è membro di un'organizzazione, non specificare questo parametro. Chiamate invece l'operazione utilizzando un'identità appartenente all'account di cui desiderate recuperare o modificare i contatti.

Tipo: stringa

Modello: ^\d{12}$

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

ContactInformation

Contiene i dettagli delle informazioni di contatto principali associate a un Account AWS.

Tipo: oggetto ContactInformation

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Riprova l'operazione più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

L'operazione non è riuscita perché ha specificato una risorsa che non può essere trovata.

Codice di stato HTTP: 404

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS

- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetPrimaryEmail

Recupera l'indirizzo e-mail principale per l'account specificato.

Sintassi della richiesta

```
POST /getPrimaryEmail HTTP/1.1
Content-type: application/json

{
   "AccountId": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificare il numero ID dell'account a 12 cifre a Account AWS cui si desidera accedere o modificare con questa operazione. Per utilizzare questo parametro, il chiamante deve avere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato. L'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

Questa operazione può essere richiamata solo dall'account di gestione o dall'account amministratore delegato di un'organizzazione per un account membro.

> **Note**
>
> L'account di gestione non può specificare il proprio. `AccountId`

Tipo: stringa

Modello: ^\d{12}$

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "PrimaryEmail": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

PrimaryEmail

Recupera l'indirizzo e-mail principale associato all'account specificato.

Tipo: stringa

Vincoli di lunghezza: lunghezza minima di 5. La lunghezza massima è 64 caratteri.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Riprova l'operazione più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

L'operazione non è riuscita perché ha specificato una risorsa che non può essere trovata.

Codice di stato HTTP: 404

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

GetRegionOptStatus

Recupera lo stato di attivazione di una particolare regione.

Sintassi della richiesta

```
POST /getRegionOptStatus HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "RegionName": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificare il numero ID dell'account a 12 cifre a Account AWS cui si desidera accedere o modificare con questa operazione. Se non specifichi questo parametro, il valore predefinito è l'account Amazon Web Services dell'identità utilizzata per chiamare l'operazione. Per utilizzare questo parametro, il chiamante deve essere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato. L'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

> **Note**
>
> L'account di gestione non può specificare il proprio. `AccountId` Deve chiamare l'operazione in un contesto autonomo escludendo il `AccountId` parametro.

Per chiamare questa operazione su un account che non è membro di un'organizzazione, non specificare questo parametro. Chiamate invece l'operazione utilizzando un'identità appartenente all'account di cui desiderate recuperare o modificare i contatti.

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: no

RegionName

Specificate il codice regionale per un determinato nome di regione (ad esempio,). `af-south-1` Questa funzione restituirà lo stato di qualsiasi regione passata a questo parametro.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "RegionName": "string",
   "RegionOptStatus": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

RegionName

Il codice regionale che è stato passato.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

RegionOptStatus

Uno dei potenziali stati a cui può sottostare una regione (Enabled, Enabling, Disabled, Disabling, Enabled_By_Default).

- Tipo: stringa

Valori validi: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Riprova l'operazione più tardi.

Codice di stato HTTP: 500

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

ListRegions

Elenca tutte le regioni per un determinato account e i rispettivi stati di attivazione. Facoltativamente, questo elenco può essere filtrato in base al parametro. `region-opt-status-contains`

Sintassi della richiesta

```
POST /listRegions HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "MaxResults": number,
   "NextToken": "string",
   "RegionOptStatusContains": [ "string" ]
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificare il numero ID dell'account a 12 cifre a Account AWS cui si desidera accedere o modificare con questa operazione. Se non specifichi questo parametro, il valore predefinito è l'account Amazon Web Services dell'identità utilizzata per chiamare l'operazione. Per utilizzare questo parametro, il chiamante deve essere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato. L'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

> **Note**
>
> L'account di gestione non può specificare il proprio. `AccountId` Deve chiamare l'operazione in un contesto autonomo escludendo il `AccountId` parametro.

Per chiamare questa operazione su un account che non è membro di un'organizzazione, non specificare questo parametro. Chiamate invece l'operazione utilizzando un'identità appartenente all'account di cui desiderate recuperare o modificare i contatti.

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: no

MaxResults

Il numero totale di elementi da restituire nell'output del comando. Se il numero totale di elementi disponibili è superiore al valore specificato, nell'output del comando `NextToken` viene fornito a. Per riprendere la paginazione, specifica il valore `NextToken` nell'argomento `starting-token` di un comando successivo. Non utilizzare l'elemento di `NextToken` risposta direttamente all'esterno della AWS CLI. Per esempi di utilizzo, consulta Pagination nella AWS Command Line Interface User Guide.

Tipo: integer

Intervallo valido: valore minimo di 1. Valore massimo pari a 50.

Campo obbligatorio: no

NextToken

Un token utilizzato per specificare da dove iniziare l'impaginazione. Questo è il risultato `NextToken` di una risposta precedentemente troncata. Per esempi di utilizzo, vedere Pagination nella AWS Command Line Interface User Guide.

Tipo: stringa

Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 1000.

Campo obbligatorio: no

RegionOptStatusContains

Un elenco di stati delle regioni (Enabling, Enabled, Disabling, Disabled, Enabled_by_default) da utilizzare per filtrare l'elenco delle regioni per un determinato account. Ad esempio, il passaggio del valore ENABLING restituirà solo un elenco di regioni con lo stato di regione abilitato.

Tipo: matrice di stringhe

Valori validi: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Campo obbligatorio: no

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Regions": [
      {
         "RegionName": "string",
         "RegionOptStatus": "string"
      }
   ]
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

NextToken

Se ci sono più dati da restituire, questo verrà compilato. Dovrebbe essere passato al parametro di `next-token` richiesta di`list-regions`.

- Tipo: stringa

Regions

Questo è un elenco di regioni per un determinato account o, se è stato utilizzato il parametro filtrato, un elenco di regioni che corrispondono ai criteri di filtro impostati nel `filter` parametro.

Tipo: matrice di oggetti Region

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Riprova l'operazione più tardi.

Codice di stato HTTP: 500

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

PutAlternateContact

Modifica il contatto alternativo specificato collegato a un. Account AWS

Per informazioni complete su come utilizzare le operazioni relative ai contatti alternativi, vedere Accesso o aggiornamento dei contatti alternativi.

> **Note**
>
> Prima di poter aggiornare le informazioni di contatto alternative per un Account AWS account gestito da AWS Organizations, devi prima abilitare l'integrazione tra AWS Account Management e Organizations. Per ulteriori informazioni, vedere Abilitazione dell'accesso affidabile per la gestione degli AWS account.

Sintassi della richiesta

```
POST /putAlternateContact HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "AlternateContactType": "string",
   "EmailAddress": "string",
   "Name": "string",
   "PhoneNumber": "string",
   "Title": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificate il numero ID dell'account a 12 cifre dell' AWS account a cui desiderate accedere o modificare con questa operazione.

Se non si specifica questo parametro, per impostazione predefinita viene utilizzato l' AWS account dell'identità utilizzata per chiamare l'operazione.

Per utilizzare questo parametro, il chiamante deve essere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato e l'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

> **Note**
>
> L'account di gestione non può specificare il proprio`AccountId`; deve chiamare l'operazione in un contesto autonomo escludendo il parametro. `AccountId`

Per richiamare questa operazione su un account che non è membro di un'organizzazione, non specificate questo parametro e richiamate l'operazione utilizzando un'identità appartenente all'account di cui desiderate recuperare o modificare i contatti.

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: no

AlternateContactType

Specificate quale contatto alternativo desiderate creare o aggiornare.

-Tipo: stringa

Valori validi: `BILLING | OPERATIONS | SECURITY`

Campo obbligatorio: sì

EmailAddress

Specificate un indirizzo e-mail per il contatto alternativo.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 254.

Modello: `^[\s]*[\w+=.#|!&-]+@[\w.-]+\.[\w]+[\s]*$`

Campo obbligatorio: sì

Name

Specificate un nome per il contatto alternativo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 64 caratteri.

Campo obbligatorio: sì

PhoneNumber

Specificate un numero di telefono per il contatto alternativo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 25.

Modello: `^[\s0-9()+-]+$`

Campo obbligatorio: sì

Title

Specificate un titolo per il contatto alternativo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Riprova l'operazione più tardi.

Codice di stato HTTP: 500

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Esempi

Esempio 1

L'esempio seguente imposta il contatto alternativo di fatturazione per l'account le cui credenziali vengono utilizzate per chiamare l'operazione.

Richiesta di esempio

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
```

```
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

Risposta di esempio

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Esempio 2

L'esempio seguente imposta o sovrascrive il contatto alternativo di fatturazione per l'account membro specificato in un'organizzazione. È necessario utilizzare le credenziali dell'account di gestione dell'organizzazione o dell'account amministratore delegato del servizio di gestione degli account.

Richiesta di esempio

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
    "AccountId": "123456789012",
    "AlternateContactType": "Billing",
    "Name": "Carlos Salazar",
    "Title": "CFO",
    "EmailAddress": "carlos@example.com",
    "PhoneNumber": "206-555-0199"
}
```

Risposta di esempio

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

PutContactInformation

Aggiorna le informazioni di contatto principali di un Account AWS.

Per i dettagli completi su come utilizzare le operazioni di contatto principale, vedi Aggiornare le informazioni di contatto principali e alternative.

Sintassi della richiesta

```
POST /putContactInformation HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "ContactInformation": {
      "AddressLine1": "string",
      "AddressLine2": "string",
      "AddressLine3": "string",
      "City": "string",
      "CompanyName": "string",
      "CountryCode": "string",
      "DistrictOrCounty": "string",
      "FullName": "string",
      "PhoneNumber": "string",
      "PostalCode": "string",
      "StateOrRegion": "string",
      "WebsiteUrl": "string"
   }
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificare il numero ID dell'account a 12 cifre a Account AWS cui si desidera accedere o modificare con questa operazione. Se non specifichi questo parametro, il valore predefinito è l'account Amazon Web Services dell'identità utilizzata per chiamare l'operazione. Per

utilizzare questo parametro, il chiamante deve essere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato. L'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

> **Note**
>
> L'account di gestione non può specificare il proprio. `AccountId` Deve chiamare l'operazione in un contesto autonomo escludendo il `AccountId` parametro.

Per chiamare questa operazione su un account che non è membro di un'organizzazione, non specificare questo parametro. Chiamate invece l'operazione utilizzando un'identità appartenente all'account di cui desiderate recuperare o modificare i contatti.

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: no

ContactInformation

Contiene i dettagli delle informazioni di contatto principali associate a un Account AWS.

Tipo: oggetto ContactInformation

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
```

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 200 con un corpo HTTP vuoto.

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Riprova l'operazione più tardi.

Codice di stato HTTP: 500

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

StartPrimaryEmailUpdate

Avvia il processo di aggiornamento dell'indirizzo e-mail principale per l'account specificato.

Sintassi della richiesta

```
POST /startPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
   "AccountId": "string",
   "PrimaryEmail": "string"
}
```

Parametri della richiesta URI:

La richiesta non utilizza parametri URI.

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

AccountId

Specificate il numero ID dell'account a 12 cifre a Account AWS cui desiderate accedere o modificare con questa operazione. Per utilizzare questo parametro, il chiamante deve avere un'identità nell'account di gestione dell'organizzazione o un account amministratore delegato. L'ID dell'account specificato deve essere un account membro della stessa organizzazione. L'organizzazione deve avere tutte le funzionalità abilitate e deve avere abilitato l'accesso affidabile per il servizio di gestione degli account e, facoltativamente, deve essere assegnato un account amministratore delegato.

Questa operazione può essere richiamata solo dall'account di gestione o dall'account amministratore delegato di un'organizzazione per un account membro.

> **Note**
>
> L'account di gestione non può specificare il proprio. `AccountId`

Tipo: stringa

Modello: `^\d{12}$`

Campo obbligatorio: sì

PrimaryEmail

Il nuovo indirizzo e-mail principale (noto anche come indirizzo e-mail dell'utente root) da utilizzare nell'account specificato.

Tipo: stringa

Vincoli di lunghezza: lunghezza minima di 5. La lunghezza massima è 64 caratteri.

Campo obbligatorio: sì

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json

{
   "Status": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Status

Lo stato della richiesta di aggiornamento e-mail principale.

Tipo: stringa

Valori validi: `PENDING | ACCEPTED`

Errori

Per informazioni sugli errori comuni a tutte le operazioni, consultare Errori comuni.

AccessDeniedException

L'operazione non è riuscita perché l'identità chiamante non dispone delle autorizzazioni minime richieste.

Codice di stato HTTP: 403

ConflictException

La richiesta non può essere elaborata a causa di un conflitto nello stato corrente della risorsa. Ad esempio, ciò accade se si tenta di abilitare una regione attualmente disabilitata (con lo stato di DISABILITAZIONE) o se si tenta di modificare l'e-mail dell'utente root di un account con un indirizzo e-mail già in uso.

Codice di stato HTTP: 409

InternalServerException

L'operazione non è riuscita a causa di un errore interno a AWS. Riprova l'operazione più tardi.

Codice di stato HTTP: 500

ResourceNotFoundException

L'operazione non è riuscita perché ha specificato una risorsa che non può essere trovata.

Codice di stato HTTP: 404

TooManyRequestsException

L'operazione non è riuscita perché è stata chiamata troppo spesso e ha superato il limite di accelerazione.

Codice di stato HTTP: 429

ValidationException

L'operazione non è riuscita perché uno dei parametri di input non era valido.

Codice di stato HTTP: 400

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- Interfaccia a riga di comando AWS
- AWS SDK per.NET
- AWS SDK per C++
- AWS SDK per Go v2
- AWS SDK per Java V2
- AWS SDK per V3 JavaScript
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

Azioni correlate in altreAWSservizi

Le seguenti operazioni sono correlate aAWS Account Managementma sono parte dellaAWS Organizationsspazio dei nomi:

- CreateAccount
- Crea un account GovCloud
- DescribeAccount

CreateAccount

La`CreateAccount`L'operazione API è disponibile solo nel contesto di un'organizzazione gestita dalAWS Organizationsservizio. L'operazione API è definita nello spazio dei nomi di quel servizio.

Per ulteriori informazioni, consultaCreateAccountnellaAWS OrganizationsDocumentazione di riferimento API.

Crea un account GovCloud

La`CreateGovCloudAccount`L'operazione API è disponibile solo nel contesto di un'organizzazione gestita dalAWS Organizationsservizio. L'operazione API è definita nello spazio dei nomi di quel servizio.

Per ulteriori informazioni, consultaCrea un account GovCloudnellaAWS OrganizationsDocumentazione di riferimento API.

DescribeAccount

La`DescribeAccount`L'operazione API è disponibile solo nel contesto di un'organizzazione gestita dalAWS Organizationsservizio. L'operazione API è definita nello spazio dei nomi di quel servizio.

Per ulteriori informazioni, consultaDescribeAccountnellaAWS OrganizationsDocumentazione di riferimento API.

Tipi di dati

Sono supportati i tipi di dati seguenti:

- AlternateContact
- ContactInformation
- Region
- ValidationExceptionField

AlternateContact

Una struttura che contiene i dettagli di un contatto alternativo associato a un account AWS

Indice

AlternateContactType

Il tipo di contatto alternativo.

- Tipo: stringa

Valori validi: `BILLING | OPERATIONS | SECURITY`

Campo obbligatorio: no

EmailAddress

L'indirizzo e-mail associato a questo contatto alternativo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 254.

Modello: `^[\s]*[\w+=.#|!&-]+@[\w.-]+\.[\w]+[\s]*$`

Campo obbligatorio: no

Name

Il nome associato a questo contatto alternativo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 64 caratteri.

Campo obbligatorio: no

PhoneNumber

Il numero di telefono associato a questo contatto alternativo.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 25.

Modello: `^[\s0-9()+-]+$`

Campo obbligatorio: no

Title

Il titolo associato a questo contatto alternativo.

-Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ContactInformation

Contiene i dettagli delle informazioni di contatto principali associate a un Account AWS.

Indice

AddressLine1

La prima riga dell'indirizzo di contatto principale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 60.

Campo obbligatorio: sì

City

La città dell'indirizzo di contatto principale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: sì

CountryCode

Il codice del paese a due lettere ISO-3166 per l'indirizzo di contatto principale.

- Tipo: stringa

Vincoli di lunghezza: lunghezza fissa di 2.

Campo obbligatorio: sì

FullName

Il nome completo dell'indirizzo di contatto principale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: sì

PhoneNumber

Il numero di telefono delle informazioni di contatto principali. Il numero verrà convalidato e, in alcuni paesi, verificata l'attivazione.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 20.

Modello: `^[+][\s0-9()-]+$`

Campo obbligatorio: sì

PostalCode

Il codice postale dell'indirizzo di contatto principale.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 20.

Campo obbligatorio: sì

AddressLine2

La seconda riga dell'indirizzo di contatto principale, se presente.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 60.

Campo obbligatorio: no

AddressLine3

La terza riga dell'indirizzo di contatto principale, se presente.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 60.

Campo obbligatorio: no

CompanyName

Il nome dell'azienda associato alle informazioni di contatto principali, se presenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

DistrictOrCounty

Il distretto o la contea dell'indirizzo di contatto principale, se esistente.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

StateOrRegion

Lo stato o la regione dell'indirizzo di contatto principale. Se l'indirizzo postale si trova negli Stati Uniti (USA), il valore in questo campo può essere un codice di stato a due caratteri (ad esempio,`NJ`) o il nome completo dello stato (ad esempio,`New Jersey`). Questo campo è obbligatorio nei seguenti Paesi:`US`, `CAGB`,`DE`, `JPIN`, e`BR`.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

WebsiteUrl

L'URL del sito Web associato alle informazioni di contatto principali, se presenti.

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 256 caratteri.

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Region

Si tratta di una struttura che esprime la Regione per un determinato account, costituita da un nome e da uno stato di attivazione.

Indice

RegionName

Il codice regionale di una determinata regione (ad esempio,`us-east-1`).

- Tipo: stringa

Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 50 caratteri.

Campo obbligatorio: no

RegionOptStatus

Uno dei potenziali stati a cui può sottostare una regione (Enabled, Enabling, Disabled, Disabling, Enabled_By_Default).

- Tipo: stringa

Valori validi: `ENABLED | ENABLING | DISABLING | DISABLED | ENABLED_BY_DEFAULT`

Campo obbligatorio: no

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli SDK specifici della lingua, consulta quanto segue: AWS

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

ValidationExceptionField

L'input non è riuscito a soddisfare i vincoli specificati dal AWS servizio in un campo specificato.

Indice

message

Un messaggio sull'eccezione di convalida.

Tipo: stringa

Campo obbligatorio: sì

name

Il nome del campo in cui è stata rilevata la voce non valida.

Tipo: stringa

Campo obbligatorio: sì

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno degli AWS SDK specifici della lingua, consulta quanto segue:

- AWS SDK per C++
- AWS SDK per Java V2
- AWS SDK per Ruby V3

Parametri comuni

L'elenco seguente contiene i parametri utilizzati da tutte le azioni per firmare le richieste di Signature Version 4 con una stringa di query. Qualsiasi parametro specifico di un'operazione è riportato nell'argomento relativo all'operazione. Per ulteriori informazioni sull'utilizzo di Signature Version 4, consulta la pagina Firma delle richieste API AWS nella Guida per l'utente di IAM.

Action

azione da eseguire.

Tipo: stringa

Campo obbligatorio: sì

Version

Versione dell'API per cui è scritta la richiesta, espressa nel formato AAAA-MM-GG.

Tipo: stringa

Campo obbligatorio: sì

X-Amz-Algorithm

Algoritmo hash utilizzato per creare la firma della richiesta.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Valori validi: `AWS4-HMAC-SHA256`

Obbligatorio: condizionale

X-Amz-Credential

Il valore dell'ambito delle credenziali, che è una stringa che include la chiave di accesso, la data, la regione di destinazione, il servizio richiesto e una stringa di terminazione ("aws4_request"). Il valore viene espresso nel seguente formato: chiave_accesso/AAAAMMGG/regione/servizio/aws4_request.

Per ulteriori informazioni, consulta la pagina Creazione di una richiesta API AWS firmata nella Guida per l'utente di IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Date

La data utilizzata per creare la firma. Il formato deve essere il formato di base ISO 8601 (YYYYMMDD'T'HHMMSS'Z'). Ad esempio, la seguente combinazione data/ora è un valore X-Amz-Date valido: `20120325T120000Z`.

Condition: X-Amz-Date è facoltativo per tutte le richieste; può essere utilizzato per sovrascrivere la data utilizzata per firmare le richieste. Se l'intestazione Date è specificata nel formato base ISO 8601, X-Amz-Date non è richiesto. Quando utilizzi X-Amz-Date, sostituisce sempre il valore dell'intestazione Date. Per ulteriori informazioni, consulta la pagina Elementi di una firma di richiesta API AWS nella Guida per l'utente di IAM.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Security-Token

Il token di sicurezza provvisorio ottenuto tramite una chiamata ad AWS Security Token Service (AWS STS). Per un elenco di servizi che supportano le credenziali di sicurezza temporanee da AWS STS, consulta la pagina Servizi AWS che funzionano con IAM nella Guida per l'utente di IAM.

Condizione: se utilizzi le credenziali di sicurezza temporanee fornite da AWS STS, devi includere il token di sicurezza.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Signature

Specifica la firma con codifica esadecimale calcolata dalla stringa da firmare e dalla chiave di firma derivata.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-SignedHeaders

Specifica tutte le intestazioni HTTP incluse come parte della richiesta canonica. Per ulteriori informazioni sulla specifica delle intestazioni firmate, consulta la pagina Creazione di una richiesta API AWS firmata nella Guida per l'utente di IAM.

Condition: specifica questo parametro quando includi le informazioni di autenticazione in una stringa di query anziché nell'intestazione di autorizzazione HTTP.

Tipo: stringa

Obbligatorio: condizionale

Errori comuni

In questa sezione sono riportati gli errori comuni delle azioni API per tutti i servizi AWS. Per gli errori specifici di un'azione API per questo servizio, consulta l'argomento per quell'azione API.

AccessDeniedException

Non disponi dell'autorizzazione di accesso sufficiente per eseguire questa operazione.

Codice di stato HTTP: 400

IncompleteSignature

La firma della richiesta non è conforme agli standard AWS.

Codice di stato HTTP: 400

InternalFailure

L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto interno sconosciuto.

Codice di stato HTTP: 500

InvalidAction

L'azione o l'operazione richiesta non è valida. Verifica che l'operazione sia digitata correttamente.

Codice di stato HTTP: 400

InvalidClientTokenId

Il certificato X.509 o l'ID chiave di accesso AWS forniti non sono presenti nei nostri record.

Codice di stato HTTP: 403

NotAuthorized

Non disponi delle autorizzazioni per eseguire questa azione.

Codice di stato HTTP: 400

OptInRequired

L'ID chiave di accesso AWS necessita di una sottoscrizione al servizio.

Codice di stato HTTP: 403

RequestExpired

La richiesta ha raggiunto il servizio più di 15 minuti dopo il date stamp della richiesta o più di 15 minuti dopo la data di scadenza della richiesta (ad esempio per URL prefirmati) oppure il date stamp della richiesta è più di 15 minuti nel futuro.

Codice di stato HTTP: 400

ServiceUnavailable

La richiesta non è riuscita a causa di un errore temporaneo del server.

Codice di stato HTTP: 503

ThrottlingException

La richiesta è stata negata a causa del throttling della richiesta.

Codice di stato HTTP: 400

ValidationError

L'input non riesce a soddisfare i vincoli specificati da un servizio AWS.

Codice di stato HTTP: 400

Chiamata dell'API tramite richieste di query HTTP

Questa sezione contiene informazioni generali sull'utilizzo dell'API Query perAWSGestione dell'account. Per ulteriori informazioni sulle operazioni delle API e sugli errori, consulta la Documentazione di riferimento delle API.

> **Note**
>
> Invece di effettuare chiamate dirette alAWSAccount Management Query API, puoi utilizzare uno deiAWSSDK. Gli SDK AWS sono costituiti da librerie e codice di esempio per diversi

linguaggi di programmazione e piattaforme (Java, Ruby, .NET, iOS, Android e altri ancora). Gli SDK forniscono un modo conveniente per creare un accesso programmatico aAWSGestione dell'account eAWS. Ad esempio, gli SDK si occupano di attività quali la firma crittografica delle richieste, la gestione degli errori e la ripetizione automatica delle richieste. Per ulteriori informazioni sugli SDK AWS, inclusi i dettagli su come scaricarli e installarli, consulta Strumenti per Amazon Web Services.

Con l'API Query perAWSGestione dell'account, puoi chiamare le azioni di servizio. Le richieste API di query sono richieste HTTPS che devono contenere un`Action`parametro per indicare l'operazione da eseguire.AWS Supporti per la gestione degli account`GET`e`POST`richieste per tutte le operazioni. Cioè, l'API non richiede l'uso`GET`per alcune azioni e`POST`per gli altri. Tuttavia,`GET`le richieste sono soggette alla limitazione delle dimensioni di un URL. Sebbene questo limite dipenda dal browser, un limite tipico è di 2.048 byte. Pertanto, per le richieste API di Query che richiedono dimensioni maggiori, è necessario utilizzare un`POST`richiesta.

La risposta è un documento XML. Per ulteriori informazioni sulla risposta, consultare le singole pagine delle operazioni nella Documentazione di riferimento delle API.

Argomenti

- Endpoint
- HTTPS obbligatorio
- FirmaAWSRichieste API di gestione dell'account

Endpoint

AWSAccount Management dispone di un unico endpoint API globale ospitato negli Stati Uniti orientali (Virginia settentrionale)Regione AWS.

Per ulteriori informazioni sugli endpoint e le regioni AWS per tutti i servizi, consulta Regioni ed endpoint nella Riferimenti generali di AWS.

HTTPS obbligatorio

Poiché l'API Query può restituire informazioni sensibili come le credenziali di sicurezza, è necessario utilizzare HTTPS per crittografare tutte le richieste API.

FirmaAWSRichieste API di gestione dell'account

Le richieste devono essere firmate usando un ID chiave di accesso e una Secret Access Key. Ti consigliamo vivamente di non utilizzare il tuoAWScredenziali dell'account root per il lavoro quotidiano conAWSGestione dell'account. Puoi usare le credenziali perAWS Identity and Access Management(IAM) credenziali utente o temporanee, come quelle utilizzate con un ruolo IAM.

Per firmare le richieste API, devi usare AWS Signature Version 4. Per ulteriori informazioni sull'utilizzo di Signature Version 4, consulta Firma delle richieste API AWS nella Guida per l'utente di IAM.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Credenziali di sicurezza AWS: fornisce informazioni generali sui tipi di credenziali che puoi usare per accedere ad AWS
- Le migliori pratiche di sicurezza in IAM— Offre suggerimenti per l'utilizzo del servizio IAM per proteggere il tuoAWSrisorse, comprese quelle inAWSGestione dell'account.
- Credenziali di sicurezza temporanee in IAM: descrive come creare e usare credenziali di sicurezza temporanee.

Quote per AWS Account Management

Il tuo Account AWS dispone di quote di default, precedentemente definite limiti, per ogni servizio AWS. Salvo diversa indicazione, ogni quota è specificaRegione AWS.

Ciascuna Account AWS ha le seguenti quote relative alla gestione dell'account.

Risorsa	Quota
Numero di contatti alternativi in un Account AWS	3: uno ciascuno per `BILLINGSECURITY`, e `OPERATIONS`
Numero di richieste region-opt simultanee per account	6
Numero di richieste region-opt simultanee per organizzazione	20
Tasso di richieste per account `DeleteAlternateContact`	1 al secondo, raffica a 6 al secondo
Tasso di `DisableRegion` richieste per account	1 al secondo, raffica a 1 al secondo
Tasso di `EnableRegion` richieste per account	1 al secondo, raffica a 1 al secondo
Tasso di `GetAlternateContact` richieste per account	10 al secondo, raffica a 15 al secondo
Tasso di `GetContactInformation` richieste per account	10 al secondo, raffica a 15 al secondo
Tasso di `GetRegionOptStatus` richieste per account	5 al secondo, raffica a 5 al secondo
Frequenza di `ListRegions` richieste per account	5 al secondo, raffica a 5 al secondo

Risorsa	Quota
Frequenza di `PutAlternateContact` richieste per account	5 al secondo, raffica a 8 al secondo
Frequenza di `PutContactInformation` richieste per account	5 al secondo, raffica a 8 al secondo

Risoluzione dei problemi Account AWS

Utilizza le informazioni contenute nei seguenti argomenti per aiutarti a diagnosticare e risolvere i Account AWS problemi relativi a. Per assistenza con l'utente root, consulta Risoluzione dei problemi con l'utente root nella Guida per l'utente IAM. Per assistenza con la procedura di accesso, consulta Risoluzione dei problemi di Account AWS accesso nella Guida per l'utente di AWSaccesso.

Argomenti sulla risoluzione dei problemi

- Risoluzione dei problemi relativi alla Account AWS creazione
- Risoluzione dei problemi di Account AWS chiusura
- Risoluzione dei problemi relativi aAccount AWS

Risoluzione dei problemi relativi alla Account AWS creazione

Utilizza i link di riferimento nella tabella seguente per aiutarti a diagnosticare e risolvere i problemi relativi alla creazione di un nuovo Account AWS.

Problema	Link di riferimento	Origine
Non so come registrarmi o creare un account	Crea uno standalone Account AWS	Questa guida
Cosa devo fare se non ho ricevuto una chiamata AWS per verificare il mio nuovo account o se il PIN che ho inserito non funziona?	https://repost.aws/knowledge-center/ phone-verify-no-call	AWS re:Post
Come posso risolvere l'errore «numero massimo di tentativi falliti» quando provo a verificar lo Account AWS telefonic amente?	https://repost.aws/knowledge-center/ maximum-failed-attempts	AWS re:Post

Problema	Link di riferimento	Origine
Sono passate più di 24 ore e il mio account non è stato attivato	https://repost.aws/knowledge-center/ create-and-activate-aws -account	AWS re:Post
Non riesco ad accedere al mio nuovo account dopo che è stato creato	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues .html	AWS Guida per l'utente di accesso

Per ulteriore assistenza, ti consigliamo di AWS re:Postcercare contenuti correlati al tuo problema specifico. Se hai ancora bisogno di assistenza, contatta AWS Support.

Risoluzione dei problemi di Account AWS chiusura

Utilizza le informazioni riportate di seguito per aiutarti a diagnosticare e risolvere i problemi più comuni riscontrati durante il processo di chiusura dell'account. Per informazioni generali sulla procedura di chiusura dell'account, consultaChiudi un Account AWS.

Argomenti

- Non so come eliminare o cancellare il mio account
- Non vedo il pulsante Chiudi account nella pagina Account
- Ho chiuso il mio account ma non ho ancora ricevuto un'e-mail di conferma
- Ricevo un errore "ConstraintViolationException" quando cerco di chiudere il mio account
- Ricevo un errore «CLOSE_ACCOUNT_QUOTA_EXCEEDED» quando cerco di chiudere un account membro
- Devo eliminare la mia AWS organizzazione prima di chiudere l'account di gestione?

Non so come eliminare o cancellare il mio account

Per chiudere il tuo account, segui le istruzioni riportate inChiudi un Account AWS.

Non vedo il pulsante Chiudi account nella pagina Account

Se non hai effettuato l'accesso come utente root, non vedrai il pulsante Chiudi account visualizzato nella pagina Account. È necessario accedere AWS Management Console come utente root per chiudere l'account. Se non riesci ad accedere, vedi Risoluzione dei problemi con l'utente root.

Ho chiuso il mio account ma non ho ancora ricevuto un'e-mail di conferma

Questa e-mail di conferma viene inviata solo all'indirizzo e-mail dell'utente root per Account AWS. Se non ricevi questa e-mail entro poche ore, puoi accedere AWS Management Console come utente root per verificare che il tuo account sia chiuso. Se il tuo account è stato chiuso con successo, verrà visualizzato un messaggio che indica che l'account è chiuso. Se l'account che hai chiuso è un account membro, puoi verificarne l'avvenuta chiusura controllando se l'account chiuso è etichettato come SUSPENDED nella AWS Organizations console. Per maggiori informazioni, consulta Chiusura di un account membro nell'organizzazione nella Guida per l'utente diAWS Organizations .

Se stai cercando di chiudere un account di gestione e non ricevi un'e-mail di conferma della chiusura dell'account, è molto probabile che la tua organizzazione abbia account membri attivi. Puoi chiudere l'account di gestione solo se la tua organizzazione non ha account membri attivi. Per verificare che non vi siano ancora account membri attivi nell'organizzazione, accedi alla AWS Organizations console e assicurati che tutti gli account dei membri siano visualizzati Suspended accanto ai nomi dei rispettivi account. Dopodiché, puoi chiudere l'account di gestione.

Ricevo un errore "ConstraintViolationException" quando cerco di chiudere il mio account

Stai cercando di chiudere un account di gestione utilizzando la AWS Organizations console, operazione non possibile. Per chiudere un account di gestione, devi accedere AWS Management Console come utente root dell'account di gestione e chiuderlo dalla pagina Account. Per ulteriori informazioni, consulta Chiusura di un account di gestione nell'organizzazione nella GuidaAWS Organizations per l'utente.

Ricevo un errore «CLOSE_ACCOUNT_QUOTA_EXCEEDED» quando cerco di chiudere un account membro

In un periodo di 30 giorni puoi chiudere solo il 10% degli account membri. Questa quota non è vincolata da un mese di calendario, ma inizia quando chiudi un account. Entro 30 giorni dalla

chiusura iniziale dell'account, non potrai superare il limite di chiusura dell'account del 10%. La chiusura minima dell'account è 10 e la chiusura massima dell'account è 1000, anche se il 10% degli account supera 1000. Per ulteriori informazioni sulle quote di Organizations, vedere Quotas for AWS Organizationsnella Guida per l'AWS Organizations utente.

Devo eliminare la mia AWS organizzazione prima di chiudere l'account di gestione?

No, non è necessario eliminare l' AWS organizzazione prima di chiudere l'account di gestione. Tuttavia, puoi chiudere l'account di gestione solo se la tua organizzazione non ha alcun account membro attivo. Per verificare che non vi siano ancora account membri attivi nell'organizzazione, accedi alla AWS Organizations console e assicurati che tutti gli account dei membri siano visualizzati `Suspended` accanto ai nomi dei rispettivi account. Dopodiché, puoi chiudere l'account di gestione.

Risoluzione dei problemi relativi aAccount AWS

Utilizza le informazioni qui riportate per risolvere i problemi relativi aAccount AWS.

Problemi

- Devo cambiare la carta di credito perAccount AWS
- Devo segnalare fraudolenteAccount AWSattività
- Devo chiudereAccount AWS

Devo cambiare la carta di credito perAccount AWS

Per cambiare la carta di credito perAccount AWS, devi essere in grado di accedere.AWSdispone di protezioni che ti richiedono di dimostrare di essere il proprietario dell'account. Per istruzioni, consultaGestione dei metodi di pagamento con carta di creditonellaAWS BillingGuida per l'utente di.

Devo segnalare fraudolenteAccount AWSattività

Se sospetti un'attività fraudolenta usando il tuoAccount AWSe vorrei fare un rapporto, vediCome segnalare un abuso diAWSrisorse.

Se riscontri problemi con un acquisto effettuato su Amazon.com, consultaServizio clienti Amazon.

Devo chiudereAccount AWS

Per assistenza nella risoluzione dei problemi con la chiusura del tuoAccount AWS, vediChiudi un Account AWS.

Cronologia dei documenti per la Guida per l'utente di Account Management

La tabella seguente descrive le versioni della documentazione per AWS Account Management.

Modifica	Descrizione	Data
Nuove API di posta elettronica principali	Support per nuove `GetPrimaryEmail` `AcceptPrimaryEmail` `Update` API e per l'aggiornamento centralizzato dell'indirizzo email dell'utente root per qualsiasi account membro in AWS Organizations. `StartPrimaryEmailUpdate` Per ulteriori informazioni, vedere Aggiornamento dell'indirizzo e-mail dell'utente root per un account membro nella Guida per l'AWS Organizations utente.	6 giugno 2024
Riscrittura dell'argomento relativo alla chiusura dell'account	L'intero argomento relativo alla chiusura degli account è stato completamente rivisto, inclusa l'aggiunta di passaggi su come chiudere gli account dei membri e degli account di gestione.	1 febbraio 2024
Fine del supporto per l'aggiunta di nuove domande relative alle sfide di sicurezza	È stato aggiunto un nuovo contenuto in cui si segnala che l'opzione per aggiungere nuove domande di sfida è	5 gennaio 2024

	stata rimossa dalla pagina Account.	
Fine del supporto per il `aws-portal` namespace	AWS Identity and Access Management Le azioni (IAM) utilizzate in precedenza per gestire l'account (ad esempio `aws-portal:ModifyAccount` e `aws-portal:ViewAccount`) hanno raggiunto la fine del supporto standard.	1 gennaio 2024
Riscrittura dell'argomento Regioni	L'intero argomento Regioni è stato completamente revisionato, inclusa l'aggiunta dei controlli di espansione e compressione.	8 ottobre 2023
Gli argomenti relativi agli utenti root sono stati trasferiti nella Guida per l'utente IAM	La discussione sugli utenti root è stata consolidata in un unico argomento, sono stati aggiunti collegamenti incrociati agli argomenti relativi agli utenti root che sono stati spostati nella IAM User Guide.	18 settembre 2023
Nuova sezione aggiunta all'argomento di contatto principale dell'account	È stata aggiunta una nuova sezione relativa ai requisiti relativi al numero di telefono e all'indirizzo e-mail.	12 settembre 2023
Nuove API per le informazioni di contatto	Support per `GetContactInformation` nuove `PutContactInformation` API.	22 luglio 2022

AWS Account Management ora supporta l'aggiornamento di contatti alternativi tramite la console. AWS Organizations	Ora puoi aggiornare i contatti alternativi della tua organizzazione tramite AWS Organizations console utilizzando le autorizzazioni dell'Account API fornite dalle politiche gestite aggiornate AWS Organizations .	8 febbraio 2022
Versione iniziale	Versione iniziale della Guida di riferimento per la gestione degli AWS account	30 settembre 2021

Glossario per AWS

Per la terminologia AWS più recente, consultare il glossario AWS nella documentazione di riferimento per Glossario AWS.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.