Guida di riferimento

AWS Gestione dell'account

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Gestione dell'account: Guida di riferimento

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Che cos'è un Account AWS? ... 1
Caratteristiche di un Account AWS ... 3
Sei un utente alle prime armi AWS ? ... 3
AWS Servizi correlati ... 4
Usare l'utente root ... 4
Supporto e feedback ... 5
Altre risorse AWS ... 5
Guida introduttiva al tuo account ... 7
Rivedi i prerequisiti ... 7
Fase 1: Crea il tuo account ... 8
Passaggio 2: attiva l'MFA per il tuo utente root ... 11
Fase 3: Creare un utente amministratore ... 11
Argomenti correlati ... 11
Accesso al tuo account ... 12
Pianifica la tua struttura di governance ... 13
Vantaggi dell'utilizzo di più Account AWS ... 13
Gestione di più Account AWS ... 14
Quando usare AWS Organizations ... 15
Abilitazione dell'accesso attendibile ... 16
Abilita un account amministratore delegato ... 17
Limita l'accesso utilizzando SCPs ... 19
Quando usare AWS Control Tower ... 21
Comprensione delle modalità operative delle API ... 22
Concessione delle autorizzazioni per aggiornare gli attributi dell'account ... 23
Configura il tuo account ... 26
Crea o aggiorna l'alias del tuo account ... 26
Abilita o disabilita Regioni AWS nel tuo account ... 26
Considerazioni prima di abilitare e disabilitare le regioni ... 28
Abilita o disabilita una regione per gli account autonomi ... 31
Abilita o disabilita una regione nella tua organizzazione ... 33
Aggiorna la fatturazione per il tuo Account AWS ... 36
Aggiornare l'e-mail dell'utente root (e-mail di) ... 36
Aggiorna l'e-mail dell'utente root () per una versione autonoma. Account AWS ... 37

Aggiorna l'e-mail dell'utente root (e-mail di) per qualsiasi Account AWS membro dell'organizzazione. ... 38
Aggiorna la password dell'utente root ... 41
Aggiorna il tuo Account AWS nome ... 42
Aggiorna il nome del tuo account per renderlo indipendente Account AWS ... 43
Aggiorna il nome dell'account per qualsiasi Account AWS utente dell'organizzazione ... 45
Aggiorna i contatti alternativi per il Account AWS ... 47
Requisiti relativi al numero di telefono e all'indirizzo e-mail ... 48
Aggiorna i contatti alternativi per renderli autonomi Account AWS ... 48
Aggiorna i contatti alternativi per tutti i Account AWS membri dell'organizzazione ... 51
account: chiave AlternateContactTypes contestuale ... 55
Aggiorna il contatto principale per il tuo Account AWS ... 56
Requisiti relativi al numero di telefono e all'indirizzo e-mail ... 57
Aggiorna il contatto principale per uno standalone Account AWS ... 57
Aggiorna il contatto principale per qualsiasi membro Account AWS della tua organizzazione ... 60
Visualizza gli identificatori del tuo account ... 62
Trova il tuo Account AWS ID ... 63
Trova l'ID utente canonico per il tuo Account AWS ... 66
Proteggi il tuo account ... 69
Protezione dei dati ... 70
AWS PrivateLink ... 71
Creazione dell'endpoint ... 71
Politiche degli endpoint Amazon VPC ... 72
Policy di endpoint ... 72
Identity and Access Management ... 73
Destinatari ... 74
Autenticazione con identità ... 74
Gestione dell'accesso con policy ... 78
AWS Gestione degli account e IAM ... 81
Esempi di policy basate su identità ... 89
Utilizzo di policy basate su identità ... 93
Risoluzione dei problemi ... 96
AWS politiche gestite ... 98
AWSAccountManagementReadOnlyAccess ... 98
AWSAccountManagementFullAccess ... 99

Aggiornamenti alle policy ... 100
Convalida della conformità ... 101
Resilienza ... 102
Sicurezza dell'infrastruttura ... 102
Monitora il tuo account ... 103
CloudTrail registri ... 103
Informazioni sulla gestione dell'account in CloudTrail ... 104
Comprensione delle voci del registro di Account Management ... 105
Monitoraggio degli eventi di gestione degli account con EventBridge ... 108
Eventi di gestione dell'account ... 108
Risolvi i problemi relativi al tuo account ... 111
Problemi relativi alla creazione dell'account ... 111
Problemi di chiusura dell'account ... 112
Non so come eliminare o cancellare il mio account ... 112
Non vedo il pulsante Chiudi account nella pagina Account ... 113
Ho chiuso il mio account ma non ho ancora ricevuto un'e-mail di conferma ... 113
Ricevo un errore "ConstraintViolationException" quando cerco di chiudere il mio account ... 113
Ricevo un errore «CLOSE_ACCOUNT_QUOTA_EXCEEDED» quando cerco di chiudere un account membro ... 113
Devo eliminare la mia AWS organizzazione prima di chiudere l'account di gestione? ... 114
Altri problemi. ... 114
Devo cambiare la mia carta di credito Account AWS ... 114
Devo segnalare attività fraudolente Account AWS ... 114
Devo chiudere il mio Account AWS ... 115
Chiudi il tuo account ... 116
Cosa devi sapere prima di chiudere l'account ... 116
Come chiudere il tuo account ... 118
Cosa aspettarsi dopo la chiusura dell'account ... 121
Periodo successivo alla chiusura ... 122
Riapertura del Account AWS ... 122
Documentazione di riferimento API ... 123
Azioni ... 125
AcceptPrimaryEmailUpdate ... 126
DeleteAlternateContact ... 130
DisableRegion ... 135
EnableRegion ... 139

GetAccountInformation ... 143
GetAlternateContact ... 148
GetContactInformation ... 154
GetPrimaryEmail ... 158
GetRegionOptStatus ... 161
ListRegions ... 165
PutAccountName ... 170
PutAlternateContact ... 174
PutContactInformation ... 180
StartPrimaryEmailUpdate ... 184
Operazioni correlate ... 187
CreateAccount ... 187
CreateGovCloudAccount ... 187
DescribeAccount ... 188
Tipi di dati ... 188
AlternateContact ... 189
ContactInformation ... 191
Region ... 195
ValidationExceptionField ... 196
Parametri comuni ... 196
Errori comuni ... 199
Chiamata di richieste di query HTTP ... 200
Endpoints ... 201
HTTPS obbligatorio ... 201
Richieste API per la gestione AWS degli account di firma ... 202
Quote ... 203
Gestire gli account in India ... 205
Crea un uomo Account AWS con AWS l'India ... 205
Gestisci le informazioni di verifica dei clienti ... 208
Controlla lo stato della verifica del cliente ... 208
Crea le informazioni di verifica del cliente ... 208
Modifica le informazioni di verifica del cliente ... 209
Documenti indiani accettati per la verifica del cliente ... 210
Gestisci il tuo account AWS in India ... 212
Cronologia dei documenti ... 213
... ccxvi

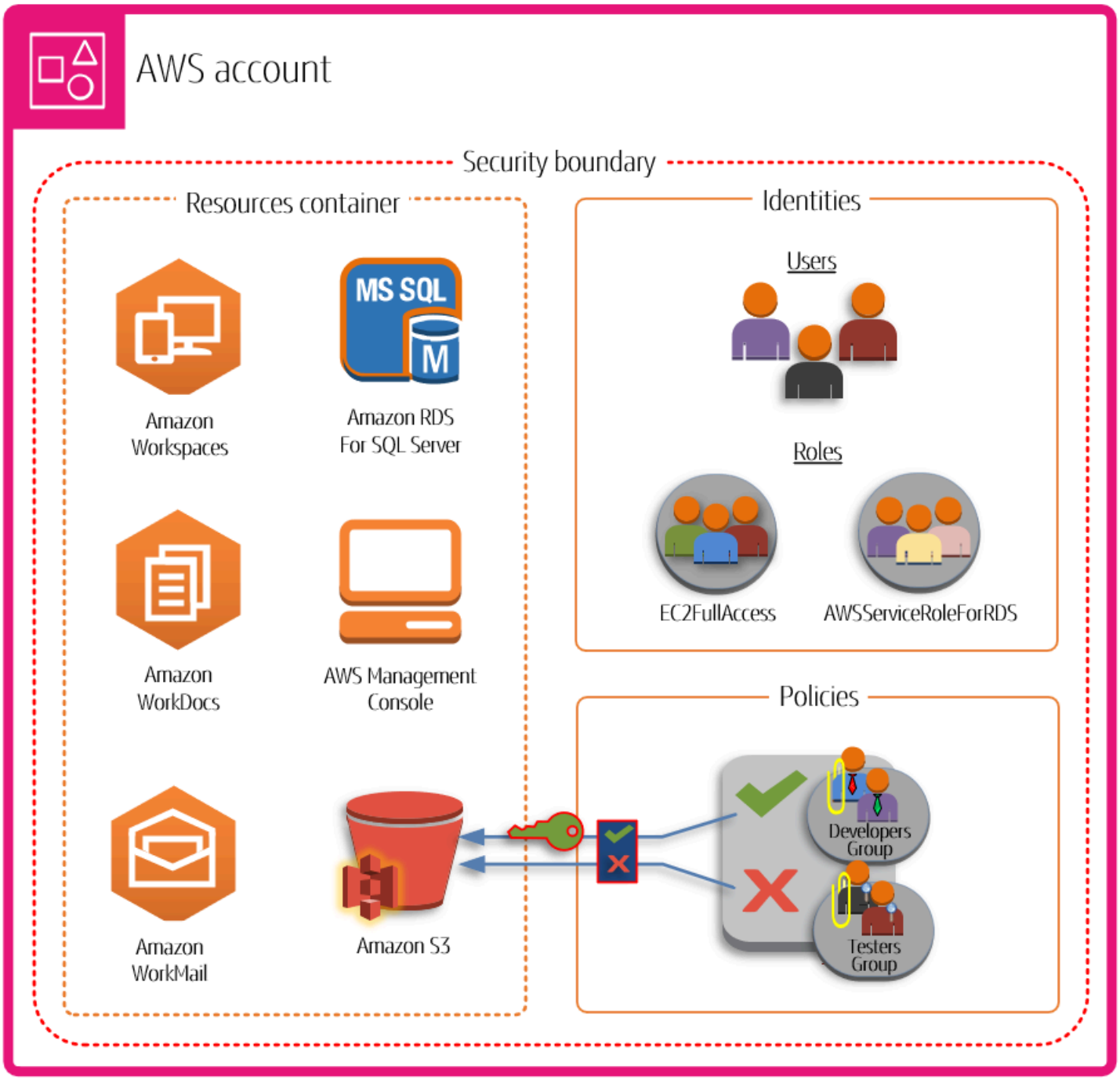
Che cos'è un Account AWS?

An Account AWS rappresenta una relazione commerciale formale con cui si instaura AWS. Crei e gestisci AWS le tue risorse in un Account AWS account e il tuo account offre funzionalità di gestione delle identità per l'accesso e la fatturazione. Ciascuno Account AWS ha un ID univoco che lo differenzia dagli altri. Account AWS

Le tue risorse e i tuoi dati cloud sono contenuti in un Account AWS. Un account funge da limite di isolamento per la gestione delle identità e degli accessi. Quando è necessario condividere risorse e dati tra due account, è necessario consentire esplicitamente questo accesso. Per impostazione predefinita, non è consentito l'accesso tra account. Ad esempio, se si designano account diversi per contenere le risorse e i dati di produzione e non di produzione, per impostazione predefinita non è consentito alcun accesso tra questi ambienti.

Account AWS sono anche una parte fondamentale dell'accesso ai AWS servizi. Come illustrato nella figura seguente, an Account AWS svolge due funzioni principali:

- Contenitore di risorse: An Account AWS è il contenitore di base per tutte le AWS risorse create 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 EC2 (Amazon) 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.



L'utilizzo di più opzioni Account AWS è una best practice per scalare l'ambiente, in quanto fornisce un limite naturale di fatturazione per i costi, isola le risorse per la sicurezza, offre flessibilità a singoli e team, oltre ad essere adattabile ai nuovi processi aziendali. Per ulteriori informazioni, consulta Vantaggi dell'utilizzo di più Account AWS.

Caratteristiche di un Account AWS

Account AWS includono le seguenti funzionalità principali:

- Monitoraggio e controllo dei costi: un account è lo strumento predefinito con cui vengono allocati AWS i costi. Per questo motivo, l'utilizzo di account diversi per diverse unità aziendali e gruppi di carichi di lavoro può aiutarti a tracciare, controllare, prevedere, pianificare e riportare più facilmente le tue spese per il cloud. Oltre alla rendicontazione dei costi a livello di account, include AWS anche un supporto integrato per consolidare e riportare i costi sull'intero set di account, nel caso in cui si decida di AWS Organizations utilizzarli in un determinato momento. Puoi anche utilizzare AWS Service Quotas per proteggerti da un approvvigionamento eccessivo e imprevisto di AWS risorse e da azioni dannose che potrebbero avere un impatto significativo sui costi. AWS
- Unità di isolamento: An Account AWS fornisce limiti di sicurezza, accesso e fatturazione per le AWS risorse che possono aiutarti a raggiungere l'autonomia e l'isolamento delle risorse. In base alla progettazione, tutte le risorse fornite all'interno di un account sono logicamente isolate dalle risorse fornite in altri account, anche all'interno del proprio ambiente. AWS Questo limite di isolamento consente di limitare i rischi di problemi relativi all'applicazione, di configurazioni errate o di azioni dannose. Se si verifica un problema all'interno di un account, è possibile ridurre o eliminare l'impatto sui carichi di lavoro contenuti in altri account.
- Rispecchia i carichi di lavoro aziendali: utilizza più account per raggruppare i carichi di lavoro con uno scopo aziendale comune in account distinti. Di conseguenza, puoi allineare la proprietà e il processo decisionale a tali account ed evitare dipendenze e conflitti con il modo in cui i carichi di lavoro in altri account sono protetti e gestiti. A seconda del modello aziendale generale, è possibile scegliere di isolare unità aziendali o filiali distinte in account diversi. Questo approccio potrebbe anche facilitare la cessione di tali unità nel tempo.

Sei un utente alle prime armi AWS ?

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

Per step-by-step istruzioni su come configurare un nuovo account, consulta. Iniziare con un Account AWS

AWS Servizi correlati

Account AWS funziona senza problemi con i seguenti servizi:

- IAM

  Your Account AWS è strettamente integrato con AWS Identity and Access Management (IAM). Puoi utilizzare IAM con il tuo account per garantire che le altre persone che lavorano nel tuo account abbiano tutto l'accesso di cui hanno bisogno per svolgere il proprio lavoro. Inoltre, utilizzi IAM per controllare l'accesso a tutte le tue AWS risorse, non solo alle informazioni specifiche dell'account. È importante acquisire familiarità con i concetti principali e le migliori pratiche di IAM prima di addentrarsi troppo nella configurazione della struttura del proprio. Account AWS Per ulteriori informazioni, consulta Best Practice di sicurezza in IAM nella Guida per l'utente di IAM.
- AWS Organizations

  Se la tua azienda è grande o è destinata a crescere, potresti voler creare più AWS account che riflettano la struttura specifica della tua azienda. AWS Organizations fornisce l'infrastruttura e le funzionalità di base per creare e gestire ambienti multi-account. È possibile combinare gli account esistenti in un'organizzazione che consente di gestire gli account centralmente. È possibile creare account che fanno automaticamente parte dell'organizzazione ed è possibile invitare altri account a far parte dell'organizzazione. È anche possibile collegare policy che interessano alcuni o tutti gli account. Per ulteriori informazioni, consulta Quando usare AWS Organizations.
- AWS Control Tower

  AWS Control Tower offre un modo semplificato per configurare e gestire un ambiente sicuro e con più account. AWS AWS Control Tower automatizza la creazione di un ambiente multi-account utilizzando AWS Organizations, istanziando, una serie di account iniziali e alcuni guardrail e configurazioni predefiniti per l'ambiente. È possibile eseguire il provisioning AWS Control Tower di nuovi account Account AWS in pochi passaggi, assicurando al contempo che gli account siano conformi alle politiche organizzative. Per ulteriori informazioni, consulta Quando usare AWS Control Tower.

Usando il Utente root dell'account AWS

Quando si crea una 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.

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 la pagina Root user best practices for your Account AWS.

> **Important**
>
> Chiunque disponga delle tue credenziali di utente root Account AWS ha accesso illimitato a tutte le risorse del tuo account, incluse le informazioni di fatturazione.

È possibile modificare o reimpostare la password dell'utente root e creare o eliminare chiavi di accesso (chiave di accesso IDs 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.

Support per la gestione degli AWS account

Puoi pubblicare commenti e domande utilizzando il forum di supporto per la gestione degli AWS account. Per informazioni generali sui AWS forum, consulta AWS re:Post.

Se non riesci a trovare le risposte che stai cercando AWS re:Post, puoi creare un account o una richiesta di supporto relativa alla fatturazione utilizzando il AWS Management Console. Per ulteriori informazioni, consulta Esempio: creazione di una richiesta di supporto per l'account e la fatturazione.

Altre risorse AWS

- AWS Formazione e corsi: collegamenti a corsi specializzati e basati su ruoli, nonché a laboratori di autoapprendimento per aiutarti ad affinare le tue abilità e acquisire esperienza pratica. AWS
- AWS Strumenti per sviluppatori: collegamenti a strumenti e risorse per sviluppatori che forniscono documentazione, esempi di codice, note di rilascio e altre informazioni con cui aiutarti a creare applicazioni innovative. AWS

- Supporto AWS Center: l'hub per la creazione e la gestione dei casi di AWS Support. Include anche collegamenti ad altre risorse utili, come forum, informazioni tecniche FAQs, stato di integrità del servizio e AWS Trusted Advisor.
- AWS Supporto: la pagina Web principale per informazioni su AWS Support one-on-one, un canale di supporto a risposta rapida per aiutarti a creare ed eseguire applicazioni nel cloud.
- Contattaci: un punto di contatto centrale per domande relative a AWS fatturazione, account, eventi, abusi e altre questioni.
- AWS Termini del sito: informazioni dettagliate sul nostro copyright e marchio, sull'account, sulla licenza e sull'accesso al sito dell'utente e su altri argomenti.

Iniziare con un Account AWS

Se sei nuovo AWS, il primo passo è iscriverti a un Account AWS. Quando lo AWS farai, creerà un account utilizzando i dettagli forniti e te lo assegnerà.

Gli argomenti di questa sezione ti aiuteranno a iniziare a conoscerne e configurarne uno nuovo Account AWS.

Argomenti

- Prerequisiti per la creazione di un nuovo Account AWS
- Crea un Account AWS
- Attiva l'MFA per il tuo utente root
- Creare un utente amministratore
- Accedere al tuo Account AWS

Prerequisiti per la creazione di un nuovo Account AWS

Per iscriverti a un Account AWS, devi fornire le seguenti informazioni:

- Indirizzo e-mail utente root Indirizzo : 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 e-mail 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.

- AWS nome dell'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

- Indirizzo: se il tuo indirizzo di contatto e di fatturazione si trova in India, il contratto d'uso per il tuo account è stipulato con Amazon Web Services India Private Limited (AWS India), 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. AWS L'India addebita al tuo metodo di pagamento 2 INR come parte del processo di verifica. AWS L'India rimborserà i 2 INR dopo il completamento della verifica.
- 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.

Crea un Account AWS

Questo argomento descrive come creare un file standalone Account AWS non gestito da AWS Organizations. Se desideri creare un account che faccia parte di un'organizzazione gestita da AWS Organizations, consulta Creazione di un account membro nella tua organizzazione nella Guida per l'AWS Organizations utente.

Queste istruzioni servono per creare un sito Account AWS al di fuori dell'India. Per creare un account in India, vediCrea un uomo Account AWS con AWS l'India.

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 a Account 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. AWS richiede 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 deve essere identica al tuo Account AWS nome o indirizzo email.
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 aziende Account 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 AWS cliente. 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 Supporto AWS piani disponibili. Per una descrizione dei piani di Support disponibili e dei relativi vantaggi, consulta Confronta Supporto 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.

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 AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo Account AWS indirizzo email. 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 AWS accesso.

2. Attiva l'MFA per il tuo utente root.

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

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.

Accedere al tuo Account AWS

Puoi accedere al tuo Account AWS in uno dei seguenti modi:

AWS Management Console

AWS Management ConsoleÈ un'interfaccia basata su browser che puoi utilizzare per gestire Account AWS le tue impostazioni e le tue risorse. AWS

AWS Strumenti da riga di comando

Con gli strumenti da riga di AWS comando, è possibile impartire comandi sulla riga di comando del sistema per eseguire AWS operazioni Account AWS e operazioni. L'utilizzo della riga di comando può essere più veloce e semplice rispetto all'uso della console. Gli strumenti da riga di comando sono utili anche se si desidera creare script che eseguano AWS attività. AWS fornisce due set di strumenti da riga di comando:

- AWS Command Line Interface(AWS CLI). Per informazioni sull'installazione e l'utilizzo di AWS CLI, consultate la Guida AWS Command Line Interface per l'utente.
- AWS Tools for Windows PowerShell. Per informazioni sull'installazione e l'utilizzo degli strumenti per Windows PowerShell, consulta la Guida per AWS Tools for Windows PowerShell l'utente.

AWS SDKs

AWS SDKs Sono costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (ad esempio, Java, Python, Ruby, .NET, iOS e Android). SDKs Si occupano di attività come la firma crittografica delle richieste, la gestione degli errori e il ritentativo automatico delle richieste. Per ulteriori informazioni AWS SDKs, incluso come scaricarli e installarli, consulta Tools for Amazon Web Services.

AWS API HTTPS Query per la gestione degli account

L'API HTTPS Query di AWS Account Management ti offre l'accesso programmatico a Account AWS e AWS. L'API della query HTTPS ti consente di eseguire richieste HTTPS direttamente al servizio. Quando utilizzi le API HTTPS, devi includere il codice per firmare in modo digitale le richieste utilizzando le tue credenziali. Per ulteriori informazioni, consulta Chiamare l'API effettuando richieste HTTP Query.

Pianifica la tua struttura di Account AWS governance

Sebbene tu abbia iniziato il AWS percorso con un solo account, ti AWS consiglia di configurare più account man mano che i carichi di lavoro aumentano in termini di dimensioni e complessità. Che tu sia una media impresa o una grande impresa, ti consigliamo di creare un piano di struttura di governance che garantisca il soddisfacimento delle esigenze relative ai dati e ai carichi di lavoro.

Questa sezione descrive i vantaggi e i servizi di governance disponibili AWS per aiutare a creare una struttura di governance multi-account.

Argomenti

- Vantaggi dell'utilizzo di più Account AWS
- Quando usare AWS Organizations
- Quando usare AWS Control Tower
- Comprensione delle modalità operative delle API

Vantaggi dell'utilizzo di più Account AWS

Account AWS costituiscono il limite di sicurezza fondamentale in. Cloud AWS Servono da contenitore per le risorse e forniscono un livello critico di isolamento essenziale per creare un ambiente sicuro e ben governato. Per ulteriori informazioni, consulta Che cos'è un Account AWS?.

La separazione delle risorse in risorse separate ti Account AWS aiuta a supportare i seguenti principi nel tuo ambiente cloud:

- Controllo della sicurezza: applicazioni diverse possono avere profili di sicurezza diversi, che richiedono politiche e meccanismi di controllo diversi. Ad esempio, è molto più semplice parlare con un revisore ed essere in grado di indicarne uno Account AWS che ospita tutti gli elementi del carico di lavoro soggetti agli standard di sicurezza PCI (Payment Card Industry).
- Isolamento: An Account AWS è un'unità di protezione di sicurezza. I potenziali rischi e le minacce alla sicurezza devono essere contenuti all'interno e Account AWS senza influire sugli altri. Potrebbero esserci esigenze di sicurezza diverse a causa dei diversi team o dei diversi profili di sicurezza.
- Molti team: team diversi hanno responsabilità e esigenze di risorse diverse. Puoi impedire ai team di interferire tra loro spostandoli in gruppi separati Account AWS.

- Isolamento dei dati: oltre a isolare i team, è importante isolare gli archivi dati in un account. Questo può aiutare a limitare il numero di persone che possono accedere e gestire quell'archivio dati. Ciò aiuta a contenere l'esposizione a dati altamente privati e quindi può contribuire a garantire la conformità con il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea.
- Processo aziendale: diverse unità aziendali o prodotti possono avere scopi e processi completamente diversi. Con più Account AWS opzioni, è possibile soddisfare le esigenze specifiche di un'unità aziendale.
- Fatturazione: un account è l'unico vero modo per separare gli articoli a livello di fatturazione. Gli account multipli consentono di separare gli articoli a livello di fatturazione tra unità aziendali, team funzionali o singoli utenti. Puoi comunque raggruppare tutte le tue fatture in un unico pagatore (utilizzando AWS Organizations la fatturazione consolidata) mantenendo le voci separate da Account AWS
- Assegnazione delle quote: le quote di AWS servizio vengono applicate separatamente per ciascuna di esse. Account AWS La suddivisione dei carichi di lavoro in diversi tipi Account AWS impedisce loro di consumare le quote l'uno per l'altro.

Tutte le raccomandazioni e le procedure descritte in questo documento sono conformi al AWS Well-Architected Framework. Questo framework ha lo scopo di aiutarti a progettare un'infrastruttura cloud flessibile, resiliente e scalabile. Anche quando inizi in piccolo, ti consigliamo di procedere in conformità con queste linee guida del framework. In questo modo potete scalare il vostro ambiente in modo sicuro e senza influire sulle operazioni in corso man mano che crescete.

Gestione di più Account AWS

Prima di iniziare ad aggiungere più account, ti consigliamo di sviluppare un piano per gestirli. Per questo, ti consigliamo di utilizzare AWS Organizations, che è un AWS servizio gratuito per gestire tutti i dati Account AWS della tua organizzazione.

AWS offre anche AWS Control Tower, che aggiunge livelli di automazione AWS gestita a Organizations e la integra automaticamente con altri AWS servizi come AWS CloudTrail Amazon CloudWatch e altri. AWS Config AWS Service Catalog Questi servizi possono comportare costi aggiuntivi. Per ulteriori informazioni, consulta Prezzi di AWS Control Tower.

Consulta anche

- Quando usare AWS Organizations
- Quando usare AWS Control Tower

Quando usare AWS Organizations

AWS Organizations è un AWS servizio che puoi utilizzare per gestire il tuo Account AWS gruppo. Ciò offre funzionalità come la fatturazione consolidata, in cui tutte le fatture dei tuoi 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 in merito AWS Organizations, consulta la Guida AWS Organizations per l'utente.

Accesso attendibile

Quando gestisci AWS Organizations gli account come gruppo, la maggior parte delle attività amministrative dell'organizzazione può essere eseguita solo dall'account di gestione dell'organizzazione. Per impostazione predefinita, sono incluse solo le operazioni relative alla gestione dell'organizzazione stessa. È possibile estendere questa funzionalità aggiuntiva ad altri AWS servizi abilitando l'accesso affidabile tra Organizations e quel servizio. L'accesso affidabile concede le autorizzazioni al AWS servizio specificato 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 a Organizations e al relativo account di gestione le autorizzazioni per accedere ai metadati, come le informazioni di contatto principali o alternative, per tutti gli account dei membri dell'organizzazione.

Per ulteriori informazioni, consulta Abilita l'accesso affidabile per la gestione AWS dell'account.

Amministratore delegato

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

Per ulteriori informazioni, consulta Abilita un account amministratore delegato per la gestione AWS degli account.

Policy di controllo dei servizi

Se l'utente Account AWS fa parte di un'organizzazione gestita da AWS Organizations, l'amministratore dell'organizzazione può applicare politiche di controllo del servizio (SCPs) che

possono limitare ciò che possono fare i responsabili degli account 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 (un principale) in un account membro può eseguire solo quelle operazioni che si trovano all'intersezione tra ciò SCPs che è consentito dalla normativa applicabile all'account e le politiche di autorizzazione IAM allegate all'account principale. Ad esempio, puoi utilizzare per impedire SCPs a qualsiasi titolare di un account di modificare i contatti alternativi del proprio account.

Ad esempio, SCPs ciò si applica a Account AWS, vedere. Limita l'accesso utilizzando le politiche AWS Organizations di controllo del servizio

Abilita l'accesso affidabile per la gestione AWS dell'account

L'abilitazione dell'accesso affidabile per la gestione dell' AWS account consente all'amministratore dell'account di gestione di modificare le informazioni e i metadati (ad esempio, i dettagli di contatto principali o alternativi) specifici di ciascun account membro in. AWS Organizations Per ulteriori informazioni, consulta Gestione AWS dell'account e AWS Organizations nella Guida per l'AWS Organizations utente. Per informazioni generali su come funziona l'accesso affidabile, consulta Utilizzo AWS Organizations con altri AWS servizi.

Dopo aver abilitato l'accesso affidabile, puoi utilizzare il `accountID` parametro nelle operazioni dell'API di gestione degli account che lo supportano. È possibile utilizzare correttamente questo parametro solo se si richiama l'operazione utilizzando le credenziali dell'account di gestione o dall'account amministratore delegato dell'organizzazione, se ne abiliti uno. Per ulteriori informazioni, consulta Abilita un account amministratore delegato per la gestione AWS degli account.

Utilizza la procedura seguente 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 AWS dell'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 Gestione AWS account 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 enable per confermarlo, quindi scegli Abilita accesso affidabile.

AWS CLI & SDKs

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

Dopo aver eseguito il comando seguente, è possibile utilizzare le credenziali dell'account di gestione dell'organizzazione per richiamare le operazioni dell'API Account Management 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.

Abilita un account amministratore delegato per la gestione AWS degli account

Si abilita un account amministratore delegato in modo da poter chiamare le operazioni dell'API di gestione degli AWS account per gli altri account membri in. AWS Organizations Dopo aver registrato

un account amministratore delegato per la tua organizzazione, gli utenti e i ruoli di quell'account possono chiamare le operazioni AWS CLI e AWS SDK nel `account` namespace che può funzionare in modalità Organizations supportando un parametro opzionale. `AccountId`

Per registrare un account membro nella tua organizzazione come account amministratore delegato, utilizza la seguente procedura.

AWS CLI & SDKs

Per registrare un account amministratore delegato per il servizio di gestione degli account

È possibile utilizzare i seguenti comandi per abilitare un amministratore delegato per il servizio di gestione dell'account.

> **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 aver abilitato l'accesso affidabile per la gestione degli account nella propria organizzazione.

È necessario specificare il seguente principale di servizio:

```
account.amazonaws.com
```

- AWS CLI: register-delegated-administrator

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

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

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

Dopo aver eseguito questo comando, puoi utilizzare le credenziali dell'account 123456789012 per richiamare le operazioni di Account Management AWS CLI e dell'API SDK che utilizzano il `--account-id` parametro per fare riferimento agli account dei membri di un'organizzazione.

AWS Management Console

Questa attività non è supportata nella console di gestione degli account. AWS È possibile eseguire questa attività solo utilizzando AWS CLI o un'operazione API da uno dei AWS SDKs.

Limita l'accesso utilizzando le politiche AWS Organizations di controllo del servizio

Questo argomento presenta esempi che mostrano come utilizzare le policy di controllo del servizio (SCPs) AWS Organizations per limitare ciò che gli utenti e i ruoli degli account dell'organizzazione possono fare. Per ulteriori informazioni sulle politiche di controllo del servizio, consulta i seguenti argomenti nella Guida AWS Organizations per l'utente:

- Creando SCPs
- Collegamento SCPs a OUs e account
- Strategie per SCPs
- Sintassi della politica SCP

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

L'esempio seguente nega che le operazioni `PutAlternateContact` e `DeleteAlternateContact` API vengano richiamate da qualsiasi account membro in modalità account autonomo. Ciò impedisce a qualsiasi titolare degli 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 di qualsiasi altro account membro dell'organizzazione

L'esempio seguente generalizza l'`Resource`elemento su «*», il che significa che si applica sia alle richieste in modalità autonoma che alle richieste in modalità organizzazione. Ciò significa che anche all'account amministratore delegato per Account Management, se si applica l'SCP, viene impedito di modificare qualsiasi contatto alternativo per qualsiasi account dell'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

L'esempio seguente SCP include una condizione che confronta il percorso dell'organizzazione dell'account con un elenco di due. OUs Ciò comporta l'impossibilità per un titolare di qualsiasi account nell'area specificata OUs 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/"
                    ]
                }
            }
    ]
}
```

Quando usare AWS Control Tower

AWS Organizations è il servizio fondamentale che consente di gestire e proteggere centralmente l'intero AWS ambiente. Un componente cruciale di questo approccio AWS Organizations incentrato è. AWS Control Tower AWS Control Tower funge da console di gestione all'interno di Organizations, fornendo un modo semplificato per configurare e gestire un AWS ambiente sicuro e multi-account applicando le migliori pratiche prescrittive.

Questo approccio basato sulle migliori pratiche di sicurezza fornito da AWS Control Tower estende le funzionalità principali di. AWS Organizations AWS Control Tower applica una serie di barriere preventive e investigative per garantire che l'organizzazione e gli account rimangano allineati agli standard di sicurezza e conformità consigliati.

Creando una AWS Organizations struttura ben architettata con AWS Control Tower, è possibile implementare rapidamente un ambiente scalabile, sicuro e conforme. AWS Questo approccio centralizzato alla gestione e alla governance del cloud è essenziale per le aziende che desiderano sfruttare tutta la potenza del cloud mantenendo al Cloud AWS contempo i più elevati standard di sicurezza e conformità.

Per ulteriori informazioni, consulta Che cos'è AWS Control Tower? nella Guida per l'utente AWS Control Tower .

Comprensione delle modalità operative delle API

Le operazioni API che funzionano con gli attributi Account AWS an's 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 dell'account nello stesso account. La modalità contestuale autonoma viene utilizzata automaticamente quando non si include il `AccountId` parametro quando si richiama una delle operazioni di Account Management AWS CLI o AWS SDK.
- Contesto delle organizzazioni: questa modalità viene utilizzata quando un utente o un ruolo in un account di un'organizzazione accede o modifica un attributo di account in un account membro diverso nella stessa organizzazione. La modalità contestuale dell'organizzazione viene utilizzata automaticamente quando si include il `AccountId` parametro quando si richiama una delle operazioni di Account Management AWS CLI o AWS SDK. È possibile richiamare le operazioni in questa modalità solo dall'account di gestione dell'organizzazione o dall'account amministratore delegato per Account Management.

Le operazioni AWS CLI e l' AWS SDK possono funzionare sia in contesti autonomi che in contesti organizzativi.

- Se non includi il `AccountId` parametro, l'operazione viene eseguita in un contesto autonomo e applica automaticamente la richiesta all'account utilizzato per effettuare la richiesta. Questo vale indipendentemente dal fatto che l'account sia membro di un'organizzazione.
- Se includi il `AccountId` parametro, l'operazione viene eseguita nel contesto delle organizzazioni 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 di gestione degli account, è possibile specificare qualsiasi account membro di tale organizzazione nel `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 account nel `AccountId` parametro è l'account specificato come account amministratore delegato per il servizio di gestione degli account. Qualsiasi altro account, incluso l'account di gestione, riceve un'`AccessDenied`eccezione.
- Se esegui un'operazione in modalità autonoma, devi avere il permesso di eseguire l'operazione con una policy IAM che includa `Resource` l'elemento Consenti tutte le risorse o un ARN che utilizzi la sintassi per un account autonomo. `"*"`

- Se esegui un'operazione in modalità organizzazione, devi avere il permesso di eseguire l'operazione con una policy IAM che includa un `Resource` elemento che `"*"` consenta tutte le risorse o un ARN che utilizzi la sintassi per un account membro in un'organizzazione.

Concessione delle autorizzazioni per aggiornare gli attributi dell'account

Come per la maggior parte AWS delle operazioni, concedi le autorizzazioni per aggiungere, aggiornare o eliminare gli attributi dell'account Account AWS utilizzando le politiche di autorizzazione IAM. Quando colleghi una policy di autorizzazione IAM a un principale IAM (un utente o un ruolo), specifichi quali azioni il principale può eseguire su quali risorse e in quali condizioni.

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

Formato Amazon Resource Name per Account AWS

- L'Amazon Resource Name (ARN) di un account Account AWS che puoi includere nell'`resource`elemento di una dichiarazione politica è costruito in modo diverso a seconda che l'account a cui desideri fare riferimento sia un account autonomo o un account appartenente a un'organizzazione. Vedi la sezione precedente su. Comprensione delle modalità operative delle API
  - Un ARN di account per un account indipendente:

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

    È necessario utilizzare questo formato quando si esegue un'operazione di attribuzione degli account in modalità autonoma senza includere il parametro. `AccountID`
  - Un ARN di account per un account membro in un'organizzazione:

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

    È necessario utilizzare questo formato quando si esegue un'operazione di attribuzione degli account in modalità organizzazioni includendo il `AccountID` parametro.

Chiavi contestuali per le politiche IAM

Il servizio Account Management fornisce anche diverse chiavi di condizione specifiche del servizio di Account Management che 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 un'unità organizzativa (OU) specifica. Solo gli account dei membri contenuti in quell'unità organizzativa soddisfano la condizione. Lo snippet di esempio seguente limita l'applicazione della politica ai soli account che rientrano in una delle due categorie specificate. OUs

Poiché `account:AccountResourceOrgPaths` si tratta di un tipo di stringa multivalore, è necessario utilizzare gli operatori di stringa o multivalore. `ForAnyValueForAllValues` Inoltre, tieni presente che il prefisso sulla chiave di condizione è`account`, anche se stai facendo riferimento ai percorsi di un'organizzazione. OUs

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

`account:AccountResourceOrgTags`

La chiave `account:AccountResourceOrgTags` di contesto 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 del tuo account. Per ulteriori informazioni sull'etichettatura, consulta Tag Editor nella Guida per l'utente.AWS Resource Groups Per informazioni sull'utilizzo dei tag come parte di una strategia di controllo degli accessi basata sugli attributi, consulta A cosa serve ABAC AWS nella IAM User Guide. Lo snippet di esempio seguente limita la politica da applicare solo agli account di un'organizzazione che hanno il tag con la chiave `project` e il valore o. `blue` `red`

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

che il prefisso sulla chiave di condizione è`account`, anche se stai facendo riferimento ai tag sull'account membro di un'organizzazione.

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

> **Note**
>
> Puoi allegare tag solo a un account di un'organizzazione. Non puoi allegare tag a un dispositivo standalone. Account AWS

Configura il tuo Account AWS

Questa sezione include argomenti che descrivono come gestire i tuoi Account AWS.

> **Note**
>
> Se il tuo Account AWS è stato creato in India utilizzando Amazon Web Services India Private Limited (AWS India), ci sono altre considerazioni. Per ulteriori informazioni, consulta Gestire gli account in India.

Argomenti

- Creare un Account AWS alias
- Abilita o disabilita Regioni AWS nel tuo account
- Aggiorna la fatturazione per il tuo Account AWS
- Aggiornare l'indirizzo e-mail dell'utente root (indirizzo)
- Aggiorna la password dell'utente root
- Aggiorna il tuo Account AWS nome
- Aggiorna i contatti alternativi per il Account AWS
- Aggiorna il contatto principale per il tuo Account AWS
- Visualizza gli Account AWS identificatori

Creare un 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 AWS ID, puoi creare un alias dell'account.

Per sapere come creare o aggiornare un alias di account, consulta Using an alias for your Account AWS ID nella IAM User Guide.

Abilita o disabilita Regioni AWS nel tuo account

An Regione AWSè una sede 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 EC2 istanze Amazon 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 del global AWS STS endpoint (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
- Abilita o disabilita una regione per gli account autonomi
- Abilita o disabilita una regione nella tua organizzazione

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 abilitate per impostazione predefinita.

Nome	Codice
Stati Uniti orientali (Virginia settentrionale)	`us-east-1`
Stati Uniti orientali (Ohio)	`us-east-2`
Stati Uniti occidentali (California settentrionale)	`us-west-1`
US West (Oregon)	`us-west-2`
Asia Pacifico (Tokyo)	`ap-northeast-1`
Asia Pacifico (Seoul)	`ap-northeast-2`
Asia Pacifico (Osaka-Locale)	`ap-northeast-3`
Asia Pacifico (Mumbai)	`ap-south-1`
Asia Pacifico (Singapore)	`ap-southeast-1`
Asia Pacifico (Sydney)	`ap-southeast-2`

Nome	Codice
Canada (Centrale)	`ca-central-1`
Europa (Francoforte)	`eu-central-1`
Europa (Stoccolma)	`eu-north-1`
Europa (Irlanda)	`eu-west-1`
Europe (London)	`eu-west-2`
Europa (Parigi)	`eu-west-3`
Sud America (San Paolo)	`sa-east-1`

- Puoi utilizzare tutte le regioni di destinazione in una geografia di inferenza interregionale indipendentemente dallo stato di regione-OPT: alcuni servizi di intelligenza artificiale AWS generativa, tra cui Amazon Bedrock (vedi Increase throughput with cross-region inference) e Amazon Q Developer (vedi Elaborazione interregionale in Amazon Q Developer) utilizzano l'inferenza interregionale. Se utilizzi questi servizi, essi selezionano automaticamente quella ottimale, Regione AWS comprese le regioni che non hai abilitato per le risorse e i dati IAM, all'interno della geografia prescelta. Ciò migliora l'esperienza del cliente massimizzando l'elaborazione disponibile e la disponibilità dei modelli.
- 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 EC2 istanza in una regione disabilitata.

- Gli addebiti per le risorse attive continuano se si disabilita una regione: se si disabilita 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 EC2 istanze Amazon, devi comunque pagare i costi per tali istanze anche se le istanze sono inaccessibili.
- 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 alla gestione dell' AWS account APIs 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, consultaAbilita l'accesso affidabile per la gestione AWS dell'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"
```

```
}
```

Aggiorna la fatturazione per il tuo Account AWS

Puoi aggiornare tutte le tue preferenze di Account AWS fatturazione utilizzando la console AWS Billing e la console di gestione dei costi. Per informazioni su come aggiornare le impostazioni relative alla fatturazione per il tuo account, consulta la Guida per l'AWS Billing and Cost Management utente:

Aggiornare l'indirizzo e-mail dell'utente root (indirizzo)

Esistono vari motivi aziendali per cui potresti dover aggiornare l'indirizzo e-mail dell'utente root (indirizzo e-mail) del tuo Account AWS. Ad esempio, sicurezza e resilienza amministrativa. Questo argomento illustra il processo di aggiornamento dell'indirizzo e-mail dell'utente root (indirizzo e-mail) sia per gli account autonomi che per quelli membri.

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

Puoi aggiornare l'e-mail dell'utente root 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 l'e-mail dell'utente root utilizzando la console di AWS gestione. Per informazioni su come eseguire questa operazione, consulta Aggiornare l'e-mail dell'utente root per una versione autonoma 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 l'e-mail dell'utente root (dell'account membro) dalla AWS Organizations console o programmaticamente tramite la AWS CLI &. SDKs Per informazioni su come eseguire questa operazione, consulta Aggiornare l'e-mail dell'utente root di per qualsiasi Account AWS utente dell'organizzazione.

Argomenti

- Aggiorna l'e-mail dell'utente root () per una versione autonoma. Account AWS
- Aggiorna l'e-mail dell'utente root (e-mail di) per qualsiasi Account AWS membro dell'organizzazione.

Aggiorna l'e-mail dell'utente root () per una versione autonoma. Account AWS

Per modificare l'indirizzo e-mail dell'utente root (indirizzo) per uno standalone Account AWS, esegui i passaggi indicati nella procedura seguente.

AWS Management Console

> **Note**
>
> Devi 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 Dettagli dell'account, scegli Azioni, quindi seleziona Aggiorna indirizzo email e password.
4. Nella pagina Dettagli dell'account, accanto a Indirizzo e-mail scegli Modifica.
5. Nella pagina Modifica indirizzo e-mail dell'account, compila i campi Nuovo indirizzo e-mail, Conferma nuovo indirizzo e-mail e conferma la password corrente. Quindi, scegli Salva e continua. Un codice di verifica viene inviato al tuo nuovo indirizzo email dano-`reply@verify.signin.aws`.
6. Nella pagina Modifica indirizzo e-mail dell'account, in Codice di verifica, inserisci il codice ricevuto tramite e-mail, quindi scegli Conferma aggiornamenti.

> **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.

AWS CLI & SDKs

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

Aggiorna l'e-mail dell'utente root (e-mail di) per qualsiasi Account AWS membro dell'organizzazione.

Per modificare l'indirizzo e-mail dell'utente root (indirizzo) per qualsiasi account membro dell'organizzazione utilizzando la AWS Organizations console, esegui i passaggi indicati nella procedura seguente.

> **Note**
>
> Prima di aggiornare l'indirizzo e-mail dell'utente root (indirizzo) per un account membro, ti consigliamo di comprendere l'impatto di questa operazione. Per ulteriori informazioni, consulta la sezione Aggiornamento dell'indirizzo e-mail dell'utente root dell' per un account membro AWS Organizations nella Guida per l'AWS Organizations utente.

Puoi anche aggiornare l'indirizzo e-mail dell'utente root (indirizzo per un account membro) direttamente dalla pagina Account AWS Management Console dopo aver effettuato l'accesso come utente root. Per step-by-step istruzioni, segui i passaggi indicati inAggiorna l'e-mail dell'utente root () per una versione autonoma. Account AWS.

AWS Management Console

> **Note**
>
> - Per eseguire questa procedura 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 di gestione degli account.
> - Non è possibile utilizzare questa procedura per accedere a un account in un'organizzazione diversa da quella utilizzata per chiamare l'operazione.

Per aggiornare l'indirizzo e-mail dell'utente root (indirizzo per un account membro utilizzando la AWS Organizations console):

1. Accedi alla AWS Organizations console . Devi accedere come utente IAM o accedere come utente root (scelta non consigliata) nell'account di gestione dell'organizzazione.
2. Account AWSNella pagina, scegli l'account membro per il quale desideri aggiornare l'indirizzo e-mail dell'utente root (indirizzo e-mail).
3. Nella sezione Dettagli dell'account, scegli il pulsante Azioni, quindi scegli Aggiorna indirizzo email.
4. In E-mail, inserisci il nuovo indirizzo e-mail per l'utente root, quindi scegli Salva. In questo modo viene inviata una password monouso (OTP) al nuovo indirizzo e-mail.

   > **Note**
   >
   > Se devi chiudere questa pagina nella console Organizations mentre aspetti il codice, puoi restituire e completare la procedura OTP entro 24 ore dall'invio del codice. A tale scopo, nella pagina dei dettagli dell'account, scegli il pulsante Azioni, quindi scegli Completa l'aggiornamento via email.

5. In Codice di verifica, inserisci il codice che è stato inviato al nuovo indirizzo e-mail nel passaggio precedente, quindi scegli Conferma. In questo modo l'aggiornamento viene inviato all'utente root dell'account.

AWS CLI & SDKs

Puoi recuperare o aggiornare l'indirizzo e-mail dell'utente root (noto anche come indirizzo e-mail principale) utilizzando i seguenti AWS CLI comandi o le relative operazioni equivalenti all' AWS SDK:

- GetPrimaryEmail
- StartPrimaryEmailUpdate
- AcceptPrimaryEmailUpdate

> **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 di gestione degli 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:GetPrimaryEmail`
> - `account:StartPrimaryEmailUpdate`
> - `account:AcceptPrimaryEmailUpdate`
>
> Se utilizzi queste autorizzazioni individuali, puoi concedere ad alcuni utenti la possibilità di leggere solo le informazioni sull'indirizzo e-mail dell'utente root e concedere ad altri la possibilità di leggere e scrivere.

Per completare la procedura relativa all'indirizzo e-mail dell'utente root di e-mail principale nell'ordine in cui sono mostrati negli esempi seguenti.

Example **`GetPrimaryEmail`**

L'esempio seguente recupera l'indirizzo e-mail dell'utente root (indirizzo) dall'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-primary-email --account-id 123456789012
```

Example **`StartPrimaryEmailUpdate`**

L'esempio seguente avvia il processo di aggiornamento dell'indirizzo e-mail dell'utente root dell', identifica il nuovo indirizzo e-mail e invia una password monouso (OTP) al nuovo indirizzo e-mail 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 start-primary-email-update --account-id 123456789012 --primary-email
 john@examplecorp.com
```

Example **`AcceptPrimaryEmailUpdate`**

L'esempio seguente accetta il codice OTP e imposta il nuovo indirizzo e-mail sull'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 accept-primary-email-update --account-id 123456789012 --otp 12345678
 --primary-email john@examplecorp.com
```

Aggiorna la password dell'utente root

Per modificare la Account AWS password dell'utente root, effettuate i passaggi indicati nella procedura seguente.

AWS Management Console

Per modificare la password dell'utente root

> **Note**
>
> 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 Dettagli dell'account, scegli Azioni, quindi seleziona Aggiorna indirizzo email e password.
4. Nella pagina Dettagli dell'account, accanto a Password scegli Modifica.
5. Nella pagina Modifica password, compila i campi Password attuale, Nuova password e Conferma nuova password. Quindi, scegli Aggiorna password. 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.

AWS CLI & SDKs

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

Aggiorna il tuo Account AWS nome

Quando ne gestite più di uno Account AWS, utilizzate convenzioni di denominazione chiare in linea con le unità aziendali e le applicazioni per l'identificazione e l'organizzazione. Durante le riorganizzazioni, le fusioni, le acquisizioni o gli aggiornamenti delle convenzioni di denominazione, potrebbe essere necessario rinominare gli account per mantenere standard di identificazione e amministrativi coerenti.

Il nome di un 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 metodo standard per assegnare un nome agli account in modo che i nomi degli account siano facili da riconoscere. Per gli account aziendali, prendi in considerazione l'utilizzo di uno standard di denominazione come organizzazione - scopo - ambiente (ad esempio, vendite - catalogo - produzione). Per motivi di privacy e sicurezza, evita di utilizzare nomi di account che riflettano informazioni di identificazione personale (PII).

- Autonomo Account AWS : Account AWS se non sei associato a un'organizzazione, puoi aggiornare il nome dell'account utilizzando il AWS Management Console, o e. AWS CLI SDKs Per informazioni su come effettuare questa operazione, consulta Aggiorna il nome del tuo account per renderlo indipendente Account AWS.
- Account AWS all'interno di un'organizzazione: per gli account membro che fanno parte di a AWS Organizations, un utente dell'account di gestione o dell'account amministratore delegato può aggiornare centralmente il nome dell'account di qualsiasi account membro dell'organizzazione dalla AWS Organizations console o a livello di codice tramite e. AWS CLI SDKs Per informazioni su come effettuare questa operazione, consulta Aggiorna il nome dell'account per qualsiasi Account AWS utente dell'organizzazione.

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

Argomenti

- Aggiorna il nome del tuo account per renderlo indipendente Account AWS
- Aggiorna il nome dell'account per qualsiasi Account AWS utente dell'organizzazione

Aggiorna il nome del tuo account per renderlo indipendente Account AWS

Per modificare il nome dell'account per uno standalone Account AWS, esegui i passaggi indicati nella procedura seguente.

AWS Management Console

> **Autorizzazioni minime**
>
> Puoi aggiornare il nome del tuo account utilizzando l'utente root, un utente IAM o un ruolo IAM. Se utilizzi l'utente root, non sono necessarie autorizzazioni IAM aggiuntive per aggiornare il nome di un account. Quando utilizzi un utente IAM o un ruolo IAM, devi disporre almeno delle seguenti autorizzazioni IAM:
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Per aggiornare il nome dell'account per un account autonomo

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 Dettagli dell'account, scegli Azioni, quindi seleziona Aggiorna nome account.
4. In Nome, inserisci il nuovo nome dell'account che desideri aggiornare, quindi scegli Salva.

AWS CLI & SDKs

> **Autorizzazioni minime**
>
> Puoi aggiornare il nome del tuo account utilizzando l'utente root, un utente IAM o un ruolo IAM. Per eseguire i seguenti passaggi, il tuo utente IAM o il tuo ruolo IAM deve disporre almeno delle seguenti autorizzazioni IAM:
>
> - `account:GetAccountInformation`
> - `account:PutAccountName`

Per aggiornare il nome dell'account per un account autonomo

È possibile utilizzare una delle seguenti operazioni:

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

Aggiorna il nome dell'account per qualsiasi Account AWS utente dell'organizzazione

In modalità AWS Organizations con tutte le funzionalità, gli utenti IAM autorizzati o i ruoli IAM negli account di gestione e amministratori delegati possono gestire centralmente i nomi degli account.

Per modificare il nome dell'account di qualsiasi account membro dell'organizzazione, esegui i passaggi indicati nella procedura seguente.

Requisiti

Per aggiornare il nome di un account 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 l'organizzazione è impostata solo sulla fatturazione consolidata e desideri abilitare tutte le funzionalità, vedi Abilitazione di tutte le funzionalità per un'organizzazione.
- È necessario abilitare l'accesso affidabile per il servizio di gestione degli AWS account. Per configurarlo, consultaAbilita l'accesso affidabile per la gestione AWS dell'account.

AWS Management Console

> **Autorizzazioni minime**
>
> Per aggiornare il nome dell'account di un account membro, il tuo utente IAM o il tuo ruolo IAM deve disporre delle seguenti autorizzazioni:
>
> - `organizations:DescribeOrganization` (solo console)

- `account:PutAccountName`

Per aggiornare il nome di un account membro

1. Apri la console Organizations all'indirizzo https://console.aws.amazon.com/organizations/.
2. Nel riquadro di navigazione a sinistra, scegliere Account AWS.
3. Account AWSNella pagina, scegli l'account membro che desideri aggiornare, scegli il menu a discesa Azioni, quindi scegli Aggiorna il nome dell'account.
4. In Nome, inserisci il nome aggiornato e scegli Salva.

AWS CLI & SDKs

> **Autorizzazioni minime**
>
> Per aggiornare il nome dell'account di un account membro, il tuo utente IAM o il tuo ruolo IAM deve disporre delle seguenti autorizzazioni:
>
> - `organizations:DescribeOrganization` (solo console)
> - `account:PutAccountName`

Per aggiornare il nome di un account membro

È possibile utilizzare una delle seguenti operazioni:

- AWS CLI: put-account-name

```
$ C:\> aws account put-account-name \
        --account-id 111111111111 \
        --account-name "New-Account-Name"
```

- AWS SDKs: PutAccountName

Aggiorna i contatti alternativi per il Account AWS

I contatti alternativi AWS consentono di 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 CLI & AWS . SDKs Per informazioni su come eseguire questa operazione, consulta Aggiornare i contatti alternativi per uno standalone. 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 a livello di codice tramite la AWS CLI &. SDKs Per informazioni su come eseguire questa operazione, consulta Aggiornare i contatti alternativi per tutti i membri dell'organizzazione. Account AWS

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 riportata di seguito 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 Console come 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 l'organizzazione è impostata solo sulla fatturazione consolidata e desideri abilitare tutte le funzionalità, vedi Abilitazione di tutte le funzionalità per un'organizzazione.
- È necessario abilitare l'accesso affidabile per il servizio di gestione degli AWS account. Per configurarlo, consultaAbilita l'accesso affidabile per la gestione AWS dell'account.

> **Note**
>
> Le politiche AWS Organizations `AWSOrganizationsReadOnlyAccess` gestite `AWSOrganizationsFullAccess` vengono aggiornate per consentire l'accesso alla gestione dell' AWS account APIs 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, il nome dell'azienda, 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 del tuo account principale utilizzando la console di AWS gestione o tramite AWS SDKs CLI &. Per informazioni su come eseguire questa operazione, consulta Aggiornare il contatto principale autonomo. 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 a livello di codice tramite la AWS CLI &. SDKs Per informazioni su come eseguire questa operazione, consulta Aggiornare il contatto Account AWS principale dell'organizzazione.

Argomenti

- Requisiti relativi al numero di telefono e all'indirizzo e-mail
- Aggiorna il contatto principale per uno standalone Account AWS
- Aggiorna il contatto principale per qualsiasi membro Account AWS della tua organizzazione

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 devono contenere solo numeri.
- I numeri di telefono devono iniziare con il 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 non devono includere trattini o spazi bianchi "`-`" tra il prefisso, il prefisso di scambio e il codice locale. Ad esempio, +12025550179.
- Per motivi di sicurezza, i numeri di telefono devono essere in grado di ricevere SMS da. AWS I numeri verdi non saranno accettati poiché la maggior parte non supporta gli SMS.
- 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. 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 indipendente Account 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' AWS SDK:

- 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 l'organizzazione è impostata solo sulla fatturazione consolidata e desideri abilitare tutte le funzionalità, vedi Abilitazione di tutte le funzionalità per un'organizzazione.
- È necessario abilitare l'accesso affidabile per il servizio di gestione degli AWS account. Per configurarlo, consultaAbilita l'accesso affidabile per la gestione AWS dell'account.

AWS Management Console

Per modificare il contatto principale di qualsiasi Account AWS membro 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 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' AWS SDK:

- 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.

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 AWS Molte AWS risorse includono l'ID dell'account nei rispettivi Amazon Resource Names (ARNs). 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 l'account IDs, come qualsiasi informazione identificativa, debba essere utilizzato e condiviso con attenzione, non è considerato un'informazione segreta, sensibile o riservata.

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 CLI L'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 gli elenchi di controllo degli accessi di Amazon S3 (). ACLs

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 AWS utenti IAM o i ruoli IAM.

Usa il comando list-buckets come segue.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --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 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 AWS utenti IAM o i ruoli IAM.

Usa il comando list-buckets come segue.

```
$ aws s3api list-buckets \
    --max-items 10 \
    --page-size 10 \
    --query Owner.ID \
    --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Sicurezza nella gestione degli AWS account

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

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

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per maggiori informazioni sui programmi di conformità che si applicano alla gestione degli account, consulta Servizi AWS Ambito per programma di conformitàServizi AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i tuoi requisiti aziendali e le leggi e le normative applicabili

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi AWS Account Management. Ti mostra come configurare la gestione degli account per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di gestione dell'account.

Argomenti

- Protezione dei dati nella gestione degli AWS account
- AWS PrivateLink per la gestione degli AWS account
- Identity and Access Management per la gestione degli AWS account
- AWS politiche gestite per la gestione degli AWS account
- Convalida della conformità per la gestione AWS degli account
- Resilienza nella gestione AWS degli account
- Sicurezza dell'infrastruttura in Gestione dell'account AWS

Protezione dei dati nella gestione degli AWS account

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

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Account Management o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

AWS PrivateLink per la gestione degli AWS account

Se utilizzi Amazon Virtual Private Cloud (Amazon VPC) per ospitare AWS le tue risorse, puoi accedere al servizio di gestione degli AWS account dall'interno del VPC senza dover attraversare la rete Internet pubblica.

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

Per connettere Amazon VPC a Account Management, devi prima definire un endpoint VPC di interfaccia, che ti permetta di connettere il tuo VPC ad altri servizi. AWS 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 un endpoint di gestione AWS dell'account nel tuo VPC utilizzando, AWS Management Console AWS Command Line Interface the AWS CLI(), AWS un SDK, l'API di gestione AWS dell'account oppure. AWS CloudFormation

Per informazioni sulla creazione e configurazione di un endpoint utilizzando la console Amazon VPC o la AWS CLI, consulta Creating an Interface Endpoint nella Amazon VPC User Guide.

> **Note**
>
> Quando crei un endpoint, specifica Account Management come servizio a cui desideri connettere il tuo VPC, utilizzando il seguente formato:
>
> ```
> com.amazonaws.us-east-1.account
> ```
>
> È necessario utilizzare la stringa esattamente come mostrato, specificando la regione. `us-east-1` In quanto servizio globale, la gestione degli account è ospitata solo in quella AWS regione.

Per informazioni sulla creazione e configurazione di un endpoint utilizzando AWS CloudFormation, consulta la VPCEndpoint risorsa AWS:::EC2: nella AWS CloudFormation User Guide.

Politiche degli endpoint Amazon VPC

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

- Policy degli endpoint di Amazon Virtual Private Cloud per la gestione degli account
- Controllo dell'accesso ai servizi con endpoint VPC nella guida.AWS PrivateLink

Policy degli endpoint di Amazon Virtual Private Cloud per la gestione degli account

Puoi creare una policy sugli endpoint Amazon VPC per la gestione degli account in cui specifichi quanto segue:

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

L'esempio seguente mostra una policy per gli endpoint di Amazon VPC che consente a un utente IAM di nome Alice nell'account 123456789012 di recuperare e modificare le informazioni di contatto alternative per qualsiasi account Account AWS, ma nega a tutti gli utenti IAM l'autorizzazione a 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 agli account che fanno parte di un' AWS organizzazione a un responsabile che si trova in uno degli account membri dell'organizzazione, l'elemento deve utilizzare il seguente formato: `Resource`

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

Per ulteriori informazioni sulla creazione di policy per gli endpoint, consulta Controllare l'accesso ai servizi con gli endpoint VPC nella Guida.AWS PrivateLink

Identity and Access Management per la gestione degli AWS account

AWS Identity and Access Management (IAM) è un Servizio AWS che consente agli amministratori a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può autenticarsi (eseguire l'accesso) ed è autorizzato (dispone di autorizzazioni) a utilizzare le risorse di Gestione degli account. IAM è un Servizio AWS che è possibile utilizzare senza alcun costo aggiuntivo.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come funziona la gestione degli AWS account con IAM
- Esempi di policy basate su identità per la gestione degli account AWS
- Utilizzo di policy basate su identità (policy IAM) per la gestione degli account AWS
- Risoluzione dei problemi relativi AWS all'identità e all'accesso alla gestione dell'account

Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in Gestione degli account.

Utente del servizio: se si utilizza il servizio Gestione account per eseguire la propria attività, l'amministratore fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità di gestione dell'account che utilizzi per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. 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 degli account, consultaRisoluzione dei problemi relativi AWS all'identità e all'accesso alla gestione dell'account.

Amministratore del servizio —Se sei il responsabile delle risorse di gestione degli account presso la tua azienda, probabilmente disponi dell'accesso completo alla Gestione degli account. Il tuo compito è determinare le funzionalità e le risorse di gestione degli account a cui gli utenti del servizio devono accedere. 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 ulteriori informazioni su come la tua azienda può utilizzare IAM con la gestione degli account, consultaCome funziona la gestione degli AWS account con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso ad Account Management. Per visualizzare policy basate su identità di esempio di Account Management che è possibile utilizzare in IAM, consultare. Esempi di policy basate su identità per la gestione degli account AWS

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWS utilizzando le credenziali di identità. È necessario essere autenticato (connesso a AWS) come utente Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

È possibile accedere ad AWS come identità federata utilizzando le credenziali fornite tramite un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWS tramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, è possibile accedere alla 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 ad in modo AWS programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi AWS gli strumenti, devi firmare le richieste personalmente. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

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

Account AWS Utente root

Quando 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 denominata utente Account AWS root 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 Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWS utilizzando credenziali temporanee.

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

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un

gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni Account AWS e gli. 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 all'interno dell'utente 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 IAMAdminse 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 Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

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

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

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

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

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso 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.
  - Forward access sessions (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. La tecnologia FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con la richiesta di un Servizio AWS per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che comporta interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
  - Ruolo collegato al servizio è un tipo di ruolo di servizio 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 ai servizi sono visualizzati nell'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: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza che eseguono richieste AWS API AWS CLI o. Ciò è preferibile all'archiviazione delle chiavi di accesso nell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le relative applicazioni, occorre creare un profilo dell'istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a AWS identità o risorse. Una policy è un oggetto in AWS che, quando associato a un'identità o risorsa, ne definisce le relative autorizzazioni. AWS Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene memorizzata in AWS sotto forma di 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 gli accessi ai diversi elementi. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

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

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

Policy basate sull'identità

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

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy standalone che possono essere collegate a più utenti, gruppi e ruoli in. Account AWS Le policy gestite includono le policy AWS gestite da e le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

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

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite da IAM in una policy basata su risorse.

Liste di controllo accessi di rete (ACLs)

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

Amazon S3 AWS WAF, e Amazon VPC sono esempi di servizi che supportano. ACLs Per maggiori informazioni ACLs, consulta Panoramica dell'elenco di controllo degli accessi nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy 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.
- Policy di controllo dei servizi (SCPs): SCPs sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o 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 si abilitano tutte le funzionalità in un'organizzazione, è possibile applicare le policy di controllo del servizio (SCPs) a uno o tutti i propri account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Policy di controllo delle risorse (RCPs): RCPs sono policy JSON che possono essere utilizzate per impostare il numero massimo di autorizzazioni disponibili per le risorse nei tuoi account senza aggiornare le policy IAM collegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account membri e può influire sulle autorizzazioni valide per le identità, tra cui Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno alla tua organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consultare Logica di valutazione delle policy nella Guida per l'utente di IAM.

Come funziona la gestione degli AWS account con IAM

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

Funzionalità IAM che è possibile utilizzare con la gestione degli AWS account

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
ACLs	No
ABAC (tag nelle policy)	No
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per ottenere un quadro generale del funzionamento di Account Management e altri AWS servizi con la maggior parte delle funzionalità di IAM, consulta AWS Servizi supportati da IAM nella Guida per l'utente IAM.

Policy basate su 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 operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

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

Esempi di policy basate su identità per la gestione degli account

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

Policy basate su risorse nell'ambito della gestione degli account

Supporta le policy basate su risorse: no

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

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account

attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per la gestione degli account

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare gli accessi ai diversi elementi. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

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

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

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

Le operazioni delle policy in Gestione degli account utilizzano il seguente prefisso prima dell'operazione:

```
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 operazioni che funzionano con i contatti alternativi Account AWS di un, includi la seguente operazione.

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

Per visualizzare esempi di policy basate su identità di Account Management, consulta. Esempi di policy basate su 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. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

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

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

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

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 relativi ARNs, consulta Risorse definite da AWS Account Management nel Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta la sezione Operazioni definite da Gestione AWS dell'account.

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

Chiavi di condizione delle policy 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. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

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

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

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

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

Il servizio di gestione degli account supporta le seguenti chiavi di condizione, utilizzabili per fornire filtri granulari per le tue policy 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 che consiste in un elenco di percorsi attraverso la gerarchia dell'organizzazione verso unità organizzative (OU) specifiche. Consente di filtrare la politica in modo da influire solo sugli account di destinazione in un'unità organizzativa corrispondente.

  ```
  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 informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta la sezione Operazioni definite da Gestione AWS dell'account.

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

Liste di controllo accessi in Gestione degli account

Supporti ACLs: No

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

Controllo dell'accesso basato su attributi con Access Management con Access Management

Supporta ABAC (tag nelle policy): No

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile collegare dei tag alle entità IAM (utenti o ruoli) e a numerose 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 la gestione degli AWS account, il controllo degli accessi basato su tag è supportato solo tramite la chiave di `account:AccountResourceOrgTags/key-name` condizione. La chiave di `aws:ResourceTag/key-name` condizione standard non è supportata APIs nello spazio dei nomi dell'account.

Esempio di policy JSON che utilizza la chiave di condizione supportata

La seguente politica di esempio consente l'accesso alla visualizzazione delle informazioni di contatto per gli account contrassegnati con la chiave "CostCenter" e il valore «12345" o «67890" nell'organizzazione.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "account:GetContactInformation",
            "account:GetAlternateContact"
         ],
         "Resource":"*",
```

```
            "Condition":{
               "ForAnyValue:StringEquals":{
                  "account:AccountResourceOrgTags/CostCenter":[
                     "12345",
                     "67890"
                  ]
               }
            }
         }
      ]
   }
```

Per ulteriori informazioni su ABAC, consulta Definizione delle autorizzazioni in base agli attributi con autorizzazione ABAC e tutorial IAM: Definisci le autorizzazioni per accedere alle AWS risorse in base ai tag nella IAM User Guide.

Utilizzo di credenziali temporanee con Account Management

Supporta le credenziali temporanee: sì

Alcuni Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i che Servizi AWS funzionano con le credenziali temporanee, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Console utilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi alla AWS utilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

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

Autorizzazioni del principale tra servizi per la gestione degli account

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando si utilizza un utente o un ruolo IAM per eseguire azioni in AWS, si viene considerati entità. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. La tecnologia FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con la richiesta di un Servizio AWS per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che comporta interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per 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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

Ruoli collegati ai servizi 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 ai servizi sono visualizzati nell'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 su identità per la gestione degli account AWS

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare 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 (console) nella Guida per l'utente IAM.

Per informazioni dettagliate sulle operazioni e sui tipi di risorse definiti da Account Management, incluso il formato di ARNs per ogni tipo di risorsa, consulta Operazioni, risorse e chiavi di condizione per AWS Account Management nella guida Informazioni di riferimento sull'autorizzazione del servizio.

Argomenti

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

Best practice per le policy

Le policy basate sulle identità determinano se qualcuno può creare, accedere o eliminare risorse di gestione dell'account nell'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:

- Nozioni di base sulle policy AWS gestite da e passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy AWS gestite da che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo. Account AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal AWS cliente specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. È possibile inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS

CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel Account AWS tuo, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

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

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 consentire 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 essere certi che gli utenti e i ruoli possano utilizzare la console di gestione account, puoi scegliere di collegare alle entità la policy `AWSAccountManagementReadOnlyAccess` o la policy `AWSAccountManagementFullAccess` AWS gestita da. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Non devi concedere le autorizzazioni minime per la console agli utenti che effettuano chiamate solo all'interfaccia a riga di comando o AWS all' AWS API. Al contrario, in molti casi puoi scegliere di concedere l'accesso solo alle operazioni che soddisfano le operazioni API che stai cercando di eseguire.

Fornire l'accesso in sola lettura alla pagina Account nella AWS Management Console

Nell'esempio seguente, desideri concedere a un utente IAM nel tuo 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, si desidera 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 policy basate su identità (policy IAM) per la gestione degli account AWS

Per informazioni complete sugli utenti IAM, vedi Che cos'è IAM? Account AWS nella Guida per l'utente IAM.

Per istruzioni su come aggiornare le policy gestite dai clienti, consulta Modifica le policy IAM nella IAM User Guide.

AWS Policy di azioni di gestione degli account

Questa tabella riepiloga le autorizzazioni che concedono l'accesso alle impostazioni dell'account. Per esempi di policy che utilizzano queste autorizzazioni, consulta Esempi di policy basate su identità per la gestione degli account AWS.

> **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 per elencare le regioni disponibili.
`account:GetAccount Information`	Lettura	Concede l'autorizzazione per recuperare le informazioni di un account.
`account:GetAlterna teContact`	Lettura	Concede l'autorizzazione per recuperare i contatti alternativi per un account.
`account:GetContact Information`	Lettura	Concede l'autorizzazione per recuperare le informazioni del contatto principale per un account.
`account:GetPrimary Email`	Lettura	Concede l'autorizzazione per recuperare l'indirizzo e-mail principale di un account.
`account:GetRegionO ptStatus`	Lettura	Concede l'autorizzazione per ottenere lo stato di attivazione di una regione.
`account:AcceptPrim aryEmailUpdate`	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 per chiudere un account. **Note** Questa autorizza zione vale solo per la

Nome autorizzazione	Livello di accesso	Descrizione
		console. Per questa autorizzazione non è disponibile alcun accesso API.
`account:DeleteAlternateContact`	Scrittura	Concede l'autorizzazione per eliminare i contatti alternativi per un account.
`account:DisableRegion`	Scrittura	Concede l'autorizzazione per disabilitare l'uso di una regione.
`account:EnableRegion`	Scrittura	Concede l'autorizzazione per abilitare l'uso di una regione.
`account:PutAccountName`	Scrittura	Concede l'autorizzazione per aggiornare il nome per un account.
`account:PutAlternateContact`	Scrittura	Concede l'autorizzazione per modificare i contatti alternativi per un account.
`account:PutContactInformation`	Scrittura	Concede l'autorizzazione per aggiornare le informazioni del contatto principale per un account.
`account:StartPrimaryEmailUpdate`	Scrittura	Concede l'autorizzazione ad avviare l'aggiornamento dell'indirizzo e-mail principal e dell'account membro in un'organizzazione. AWS

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

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di Account Management e IAM.

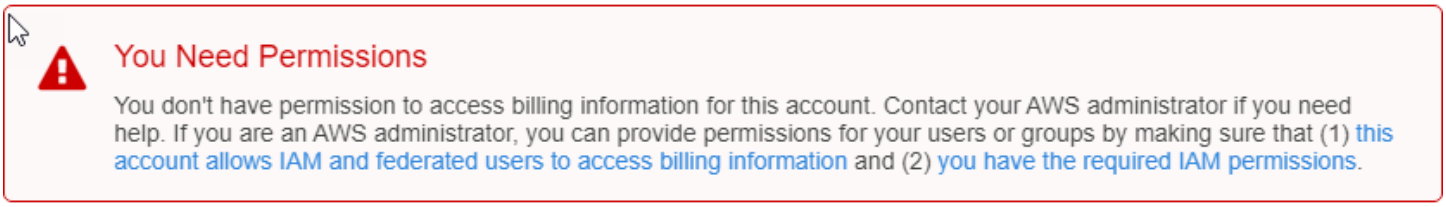
Argomenti

- Non sono autorizzato a eseguire un'operazione nella pagina Account
- Non sono autorizzato a eseguire iam:PassRole
- Voglio consentire alle persone esterne al mio di accedere Account AWS ai dettagli del mio account

Non sono autorizzato a eseguire un'operazione nella pagina Account

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

L'errore di esempio seguente si verifica quando l'utente `mateojackson` IAM tenta di utilizzare la console per visualizzare i dettagli relativi al suo 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 errore che indica che non sei autorizzato a eseguire l'`iam:PassRole`operazione, le tue policy devono essere aggiornate per poter passare un ruolo a Gestione account.

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

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in Gestione account. 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`.

Per ulteriore assistenza, contatta AWS l'amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire alle persone esterne al mio 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 accessi, puoi utilizzare tali policy per concedere alle persone l'accesso alle tue risorse. ACLs

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se la gestione degli account supporta queste funzionalità, consultaCome funziona la gestione degli AWS account con IAM.
- Per capire come garantire l'accesso alle risorse negli Account AWS che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS che si possiede nella Guida per l'utente di IAM.
- Per capire come fornire l'accesso alle risorse ad di terze parti Account AWS, consulta Concessione dell'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente di IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

AWS politiche gestite per la gestione degli AWS account

AWS Attualmente Account Management offre due policy AWS gestite disponibili per l'uso:

- AWS politica gestita: AWSAccount ManagementReadOnlyAccess
- AWS politica gestita: AWSAccount ManagementFullAccess
- Gestione degli account: aggiornamenti alle politiche AWS gestite

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

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti 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 politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consulta Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AWSAccount ManagementReadOnlyAccess

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 tuo Account AWS
- I quali sono abilitati o disabilitati per Account AWS (puoi visualizzare lo stato delle regioni nel tuo account solo utilizzando la AWS console) Regioni AWS

Lo fa concedendo l'autorizzazione a eseguire una qualsiasi delle `List*` operazioni `Get*` o. Non offre alcuna possibilità di modificare i metadati dell'account o di abilitare o disabilitare Regioni AWS l'account.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `account`— Consente ai responsabili di recuperare le informazioni sui metadati relativi a. Account AWS Consente inoltre ai mandanti di elencare le Regioni AWS funzionalità abilitate per l'account in. AWS Management Console

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

AWS politica gestita: AWSAccount ManagementFullAccess

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 Account AWS
- I quali sono abilitati o disabilitati per Account AWS (puoi visualizzare lo stato o abilitare o disabilitare le regioni per il tuo account solo utilizzando la AWS console) Regioni AWS

Lo fa concedendo l'autorizzazione a eseguire qualsiasi `account` operazione.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `account`— Consente ai responsabili di visualizzare o modificare le informazioni sui metadati relativi a. Account AWS Consente inoltre ai mandanti di elencare i dispositivi abilitati per Regioni AWS l'account e di abilitarli o disabilitarli in. AWS Management Console

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

Gestione degli account: aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Account Management da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di gestione degli account.

Modifica	Descrizione	Data
AWS Account Management è stato lanciato con nuove politiche AWS gestite e ha iniziato a tenere traccia delle modifiche	Account Management è stato inizialmente lanciato con le seguenti politiche AWS gestite: • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess	30 settembre 2021

Convalida della conformità per la gestione AWS degli account

I revisori di terze parti valutano la sicurezza e la conformità dei AWS servizi che possono essere eseguiti all'interno dell'azienda nell' Account AWS ambito di più programmi di AWS conformità. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco dei AWS servizi che rientrano nell'ambito di specifici programmi di conformità, vedere Servizi AWS Ambito per programma di conformitàServizi AWS . Per informazioni generali, vedere Programmi di AWS conformità Programmi di di .

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

La vostra responsabilità in materia di conformità nell'utilizzo dei servizi offerti da voi Account AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- Valutazione delle risorse con le regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza dell'utente, AWS che consente di verificare la conformità agli standard e alle best practice del settore della sicurezza.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza nella gestione AWS degli account

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS 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 tradizionali.

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

Sicurezza dell'infrastruttura in Gestione dell'account AWS

In quanto servizi gestiti, AWS i servizi in esecuzione all'interno dell'utente Account AWS sono protetti dalla sicurezza della rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Si utilizzano chiamate API AWS pubblicate per accedere alle impostazioni dell'account attraverso la rete. I client devono supportare quanto segue:

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

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

Monitora il tuo Account AWS

Il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità e delle prestazioni di AWS Account Management e delle altre AWS soluzioni. AWS fornisce 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 registro in un bucket Amazon Simple Storage Service (Amazon S3) da te specificato. Ciò consente di identificare gli utenti e gli account chiamati AWS, 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 delle chiamate API di gestione dell' AWS account tramite AWS CloudTrail

La gestione degli AWS APIs account è integrata con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente, da un ruolo o da un AWS servizio che richiama un'operazione di gestione dell'account. CloudTrailacquisisce tutte le chiamate API di Account Management come eventi. Le chiamate acquisite includono tutte le chiamate alle operazioni di gestione dell'account. Se crei un trail, puoi attivare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per le operazioni di gestione degli account. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che ha richiesto un'operazione di gestione dell'account, l'indirizzo IP utilizzato per effettuare la richiesta, chi ha effettuato la richiesta e quando, e ulteriori dettagli.

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

Informazioni sulla gestione dell'account in CloudTrail

CloudTrail è attivata nel tuo Account AWS quando crei l'account. Quando si verifica un'attività con un'operazione di gestione dell'account, CloudTrail registra tale attività in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo account Account AWS, compresi gli eventi relativi alle operazioni di gestione dell'account, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso in AWS Management Console, il percorso si applica a tutti. Regioni AWS Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. È possibile configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni
- Ricezione di file di CloudTrail registro da più account

AWS CloudTrail registra tutte le operazioni dell'API di gestione dell'account riportate nella sezione API Reference di questa guida. Ad esempio, le chiamate alle `PutAlternateContact` operazioni `CreateAccountDeleteAlternateContact`, e generano voci nei file di CloudTrail registro.

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

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

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Comprensione delle voci del registro di Account Management

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

Esempio 1: L'esempio seguente mostra una voce di CloudTrail registro per una chiamata all'`GetAlternateContact`operazione di recupero del contatto `OPERATIONS` alternativo corrente 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 CloudTrail registro per una chiamata all'`PutAlternateContact`operazione per aggiungere un nuovo contatto `BILLING` 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 CloudTrail registro per una chiamata all'`DeleteAlternateContact`operazione di eliminazione del contatto `OPERATIONS` alternativo corrente.

```
{
  "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 alle 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 Account Management.

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 da and: `GetRegionOptStatus` `ListRegions` APIs

- `ENABLED`— La regione è stata abilitata con successo per quanto indicato `accountId`
- `ENABLING`— La Regione è in fase di attivazione 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"
      ]
   }
}
```

Risolvi i tuoi problemi Account AWS

Utilizza le informazioni contenute nei seguenti argomenti per aiutarti a diagnosticare e risolvere i problemi relativi a. Account AWS Per assistenza con l'utente root, consulta Risoluzione dei problemi con l'utente root nella Guida per l'utente IAM. Per assistenza sulla procedura di accesso, consulta Risoluzione dei problemi di Account AWS accesso nella Guida per l'utente di AWS accesso.

Argomenti sulla risoluzione dei problemi

- Risoluzione dei problemi relativi alla Account AWS creazione
- Risoluzione dei problemi relativi alla Account AWS chiusura
- Risoluzione di altri problemi con Account 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 un 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 cerco di verificarlo Account AWS telefonicamente?	https://repost. aws/knowledge-center/maximum-tentativi falliti	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-i ssues .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 Supporto AWS.

Risoluzione dei problemi relativi alla 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, consultaChiudere 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 inChiudere 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, all'indirizzo 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 di AWS 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 dispone di 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 Guida AWS 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 Organizations nella 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 di altri problemi con Account AWS

Utilizza le informazioni qui per aiutarti a risolvere i problemi relativi al tuo. Account AWS

Problemi

- Devo cambiare la mia carta di credito Account AWS
- Devo segnalare attività fraudolente Account AWS
- Devo chiudere il mio Account AWS

Devo cambiare la mia carta di credito Account AWS

Per cambiare la tua carta di credito Account AWS, devi essere in grado di accedere. AWS dispone di protezioni che richiedono che tu dimostri di essere il proprietario dell'account. Per istruzioni, consulta Gestione dei metodi di pagamento con carta di credito nella Guida per l'AWS Billing utente.

Devo segnalare attività fraudolente Account AWS

Se sospetti un'attività fraudolenta che utilizza il tuo Account AWS e desideri effettuare una segnalazione, consulta Come posso segnalare un abuso di AWS risorse.

Se riscontri problemi con un acquisto effettuato su Amazon.com, consulta il Servizio clienti Amazon.

Devo chiudere il mio Account AWS

Per assistenza nella risoluzione dei problemi relativi alla chiusura del tuo Account AWS, consultaChiudere un Account AWS.

Chiudere 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. Supporto AWS
- 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. Per ulteriori informazioni, consulta Aggiornare l'indirizzo e-mail dell'utente root (indirizzo).
- 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 del 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.
- Dopo la chiusura di un account, AWS invieremo e-mail giornaliere per un massimo di cinque giorni prima di sospendere il dominio. Dopo la sospensione del dominio, e a seconda del registrar del dominio, elimineremo il dominio entro 30 giorni o lo rilasceremo al suo registrar. Per ulteriori informazioni, vedi My Account AWS è chiuso o permanentemente chiuso e il mio dominio è registrato con Route 53.

- AWS CloudTrail è un servizio di sicurezza fondamentale. Ciò significa che i percorsi creati dagli utenti possono continuare a esistere e fornire eventi anche dopo la chiusura, a meno che un utente non li elimini esplicitamente Account AWS prima di chiuderli. Account AWS Per ulteriori informazioni su come richiedere l'eliminazione di un Account AWS percorso dopo la chiusura, consulta la sezione Account AWS Chiusura e percorsi nella Guida per l'CloudTrail utente.

Come chiudere il tuo 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 relativi alla 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 dei AWS SDKs. È possibile eseguire questa operazione 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. Questa opzione è disponibile solo quando un' AWS organizzazione è in modalità Tutte le funzionalità.

   > **Note**
   >
   > Se l'organizzazione utilizza la modalità di fatturazione consolidata, non sarà possibile visualizzare il pulsante Chiudi nella console. Per chiudere un account in modalità di fatturazione consolidata, accedi all'account che desideri chiudere come utente root. Nella pagina Account, scegli il pulsante Chiudi account, inserisci l'ID dell'account, quindi scegli il pulsante Chiudi account.

4. Leggi e assicurati di aver compreso le istruzioni per la chiusura dell'account.
5. Inserisci l'ID dell'account membro, quindi scegli Chiudi account per avviare il processo di chiusura dell'account.

> **Note**
>
> Qualsiasi account membro che chiudi mostrerà un'`SUSPENDED`etichetta accanto al nome dell'account nella AWS Organizations console per un massimo di 90 giorni dopo la data

di chiusura originale. Dopo 90 giorni, l'account del membro non verrà più visualizzato nel AWS Organizations.

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 AWS CLI e SDKs

Per istruzioni su come chiudere un account membro utilizzando il AWS CLI and SDKs, 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 dei AWS SDKs. È possibile eseguire questa operazione 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 relativi alla Account AWS chiusura.
- Qualsiasi account membro che chiudi mostrerà un'`SUSPENDED`etichetta accanto al nome dell'account nella AWS Organizations console per un massimo di 90 giorni dopo la data di chiusura originale. Dopo 90 giorni, l'account del membro non verrà più visualizzato 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.

La chiusura dell'account potrebbe non avvenire immediatamente in tutte le regioni e i servizi e il completamento può richiedere diverse ore.

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 anche contenuti e risorse dal tuo account (ad eccezione CloudTrail dei percorsi). Dopo che un account è stato chiuso definitivamente, il suo Account AWS ID non può più essere riutilizzato.

Riapertura del 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 Supporto AWSpossibile 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.

Documentazione di riferimento API

Le operazioni API nello spazio dei nomi Account Management (`account`) consentono di modificare le proprie. Account AWS

Every Account AWS supporta metadati con informazioni sull'account, incluse informazioni su un massimo di tre contatti alternativi associati all'account. Questi si aggiungono all'indirizzo e-mail associato all'utente root dell'account. È possibile specificare solo uno dei seguenti tipi di contatto associati a un account.

- Contatto di fatturazione
- Contatto operativo
- Contatto di sicurezza

Per impostazione predefinita, le operazioni API illustrate in questa guida si applicano direttamente all'account che chiama l'operazione. L'identità dell'account che chiama l'operazione è in genere un ruolo IAM o un utente IAM e deve avere l'autorizzazione applicata da una policy IAM per richiamare l'operazione API. In alternativa, puoi richiamare queste operazioni API da un'identità in un account di AWS Organizations gestione e specificare il numero ID dell'account per qualsiasi Account AWS membro dell'organizzazione.

Versione dell'API

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

> **Note**
>
> In alternativa all'utilizzo diretto dell'API, puoi utilizzarne una AWS SDKs, che consiste in librerie e codice di esempio per vari linguaggi e piattaforme di programmazione (Java, Ruby, .NET, iOS, Android e altri). SDKs Forniscono un modo conveniente per creare un accesso programmatico alle AWS Organizzazioni. Ad esempio, SDKs si occupano di firmare crittograficamente le richieste, gestire gli errori e riprovare automaticamente le richieste. Per ulteriori informazioni su AWS SDKs, incluso come scaricarli e installarli, consulta Tools for Amazon Web Services.

Ti consigliamo di utilizzare il AWS SDKs per effettuare chiamate API programmatiche al servizio di gestione degli account. 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, consulta Chiamata dell'API tramite richieste di query HTTP la Guida per l'utente di Account Management. Organizations supporta 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 le operazioni che richiedono dimensioni maggiori, utilizzate una richiesta POST.

Firma delle richieste

Quando invii richieste HTTP a AWS, devi firmare le richieste in modo da AWS poter identificare chi le ha inviate. Le richieste vengono firmate con la chiave di AWS 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, usa AWS Security Token Service per generare credenziali di sicurezza temporanee e usa tali credenziali per firmare le richieste.

Per firmare le richieste, ti consigliamo di utilizzare la versione 4 di Signature. Se disponi di un'applicazione esistente che utilizza Signature Version 2, non è necessario aggiornarla per utilizzare Signature Version 4. Tuttavia, alcune operazioni ora richiedono Signature Version 4. La documentazione per le operazioni che richiedono la versione 4 indica questo requisito. Per ulteriori informazioni, consulta Signing AWS API request nella IAM User Guide.

Quando utilizzi l'interfaccia a riga di AWS comando (AWS CLI) o una delle altre AWS SDKs per effettuare richieste AWS, questi strumenti firmano automaticamente le richieste per te con la chiave di accesso specificata durante la configurazione degli strumenti.

Support e feedback per la gestione degli account

Apprezziamo il tuo feedback. Invia i tuoi commenti a feedback-awsaccounts@amazon.com o pubblica commenti e domande nel forum di supporto per la gestione degli account. Per ulteriori informazioni sui forum di AWS supporto, consulta la sezione Aiuto dei forum.

Come vengono presentati gli esempi

Il codice JSON restituito dalla gestione dell'account come risposta alle richieste viene restituito come una singola 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 alcuni parametri di input 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

Supporta Account Management CloudTrail, un servizio che registra le chiamate AWS API per te Account AWS e invia i file di log a un bucket Amazon S3. Utilizzando le informazioni raccolte da CloudTrail, 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 relativo supporto CloudTrail, vedereRegistrazione delle chiamate API di gestione dell' AWS account tramite AWS CloudTrail. Per ulteriori informazioni CloudTrail, incluso come attivarlo e trovare i file di registro, consulta la Guida per l'AWS CloudTrail utente.

Azioni

Sono supportate le operazioni seguenti:

- AcceptPrimaryEmailUpdate
- DeleteAlternateContact
- DisableRegion
- EnableRegion
- GetAccountInformation
- GetAlternateContact
- GetContactInformation
- GetPrimaryEmail
- GetRegionOptStatus
- ListRegions
- PutAccountName
- 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 una delle lingue specifiche AWS SDKs, 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 Kotlin
- 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 dettagli completi su come utilizzare le operazioni relative ai contatti alternativi, vedi Aggiornare i contatti alternativi per il tuo. Account AWS

> **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, consulta Abilitare l'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

Specificare il numero di ID dell'account di 12 cifre dell' AWS account a cui si desidera 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. Riprova l'operazione in un secondo momento.

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 di sicurezza alternativo per l'account le cui credenziali vengono utilizzate per chiamare l'operazione.

Richiesta di esempio

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

{
   "AccountName":"MyAccount"
}
```

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 una delle lingue specifiche AWS SDKs, 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 Kotlin
- AWS SDK for PHP V3
- AWS SDK per Python
- AWS SDK for 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 una delle lingue specifiche AWS SDKs, 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 Kotlin
- 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 una delle lingue specifiche AWS SDKs, 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 Kotlin

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

GetAccountInformation

Recupera informazioni sull'account specificato, tra cui il nome dell'account, l'ID dell'account e la data e l'ora di creazione dell'account. Per utilizzare questa API, un utente o un ruolo IAM deve disporre dell'autorizzazione `account:GetAccountInformation` IAM.

Sintassi della richiesta

```
POST /getAccountInformation 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 di ID dell'account di 12 cifre dell' AWS account a cui desideri 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

Sintassi della risposta

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

{
   "AccountCreatedDate": "string",
   "AccountId": "string",
   "AccountName": "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.

AccountCreatedDate

La data e l'ora di creazione dell'account.

Tipo: Timestamp

AccountId

Specificare il numero di ID dell'account di 12 cifre dell'account a Account AWS cui si desidera accedere o modificare con questa 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.

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}$`

AccountName

Il nome dell'account.

Tipo: stringa

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

Modello: `^[ -;=?-~]+$`

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. Riprovare 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

Nell'esempio seguente vengono recuperate le informazioni sull'account le cui credenziali vengono utilizzate per chiamare l'operazione.

Richiesta di esempio

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

{}
```

Risposta di esempio

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

{
   "AccountId": "123456789012",
   "AccountName": "MyAccount",
   "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

Esempio 2

L'esempio seguente recupera le informazioni sull'account dell'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.GetAccountInformation

{
   "AccountId": "123456789012"
}
```

Risposta di esempio

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

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount",
   "AccountCreatedDate": "2020-11-30T17:44:37Z"
}
```

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in una delle lingue specifiche AWS SDKs, consulta le risorse seguenti:

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

GetAlternateContact

Recupera il contatto alternativo specificato collegato a un. Account AWS

Per dettagli completi su come utilizzare le operazioni relative ai contatti alternativi, vedi Aggiornare i contatti alternativi per il tuo. Account AWS

> **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, consulta Abilitare l'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

Specificare il numero di ID dell'account di 12 cifre dell' AWS account a cui si desidera 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

Specificare il contatto alternativo da 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 contenente 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. Riprovare 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

Nell'esempio seguente viene recuperato il contatto di sicurezza alternativo 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 dei linguaggi specifici AWS SDKs, consulta le risorse seguenti:

- 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 Kotlin
- 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 dettagli completi su come utilizzare le operazioni di contatto principale, vedi Aggiornare il contatto principale per il tuo Account AWS.

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

Specifichi il numero di ID dell'account di gestione dell'account a Account AWS cui si desidera accedere o modificare con questa operazione. Se non si specifica questo parametro, per l'account Amazon Web Services utilizzata per la chiamata dell'operazione viene ripristinata l'impostazione predefinita. 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. Riprovare l'operazione in un secondo momento.

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 una delle lingue specifiche AWS SDKs, 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 Kotlin
- AWS SDK for PHP V3
- AWS SDK per Python
- AWS SDK for 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 una delle lingue specifiche AWS SDKs, 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 Kotlin
- 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 una delle lingue specifiche AWS SDKs, 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 Kotlin
- 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, se si trasmette il valore ENABLING, verrà restituito 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. 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 una delle lingue specifiche AWS SDKs, 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 Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python

- AWS SDK per Ruby V3

PutAccountName

Aggiorna il nome dell'account dell'account specificato. Per utilizzare questa API, i responsabili IAM devono disporre dell'autorizzazione `account:PutAccountName` IAM.

Sintassi della richiesta

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

{
   "AccountId": "string",
   "AccountName": "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 di ID dell' AWS account di gestione a cui si desidera 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

AccountName

Il nome dell'account.

Tipo: stringa

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

Modello: `^[ -;=?-~]+$`

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. Riprovare l'operazione in un secondo momento.

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

Nell'esempio seguente viene aggiornato il nome dell'account le cui credenziali vengono utilizzate per chiamare l'operazione.

Richiesta di esempio

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

{
   "AccountName":"MyAccount"
}
```

Risposta di esempio

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

Esempio 2

L'esempio seguente aggiorna il nome dell'account dell'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.PutAccountName

{
   "AccountId": "123456789012",
   "AccountName": "MyMemberAccount"
}
```

Risposta di esempio

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

Vedi anche

Per ulteriori informazioni sull'utilizzo di questa API in uno dei linguaggi specifici AWS SDKs, consulta le risorse seguenti:

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

PutAlternateContact

Modifica il contatto alternativo specificato collegato a un. Account AWS

Per dettagli completi su come utilizzare le operazioni relative ai contatti alternativi, vedi Aggiornare i contatti alternativi per il tuo. Account AWS

> **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, consulta Abilitare l'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

Specificare il numero di ID dell'account di 12 cifre dell' AWS account a cui si desidera 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 il contatto alternativo che 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. Riprovare l'operazione in un secondo momento.

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

Nell'esempio seguente viene impostato il contatto di fatturazione alternativo 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 dei linguaggi specifici AWS SDKs, consulta le risorse seguenti:

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

PutContactInformation

Aggiorna le informazioni di contatto principali di un Account AWS.

Per dettagli completi su come utilizzare le operazioni di contatto principale, vedi Aggiornare il contatto principale per il tuo Account AWS.

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

Specifichi il numero di ID dell'account di gestione di Account AWS cui si desidera accedere o modificare con questa operazione. Se non si specifichi questo parametro, per l'identità utilizzata per chiamare l'operazione viene ripristinata l'impostazione predefinita Amazon Web Services.

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. Riprovare l'operazione in un secondo momento.

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 una delle lingue specifiche AWS SDKs, 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 Kotlin
- AWS SDK for PHP V3

- AWS SDK per Python
- AWS SDK for 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 una delle lingue specifiche AWS SDKs, 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 Kotlin
- AWS SDK per PHP V3
- AWS SDK per Python
- AWS SDK per Ruby V3

Azioni correlate in altri AWS servizi

Le seguenti operazioni sono correlate Gestione dell'account AWS ma fanno parte del AWS Organizations namespace:

- CreateAccount
- CreateGovCloudAccount
- DescribeAccount

CreateAccount

L'operazione `CreateAccount` API può essere utilizzata solo nel contesto di un'organizzazione gestita dal AWS Organizations servizio. L'operazione API è definita nello spazio dei nomi di quel servizio.

Per ulteriori informazioni, consulta CreateAccount nella documentazione di riferimento dell'API AWS Organizations .

CreateGovCloudAccount

L'operazione `CreateGovCloudAccount` API può essere utilizzata solo nel contesto di un'organizzazione gestita dal AWS Organizations servizio. L'operazione API è definita nello spazio dei nomi di quel servizio.

Per ulteriori informazioni, consulta CreateGovCloudAccount nella documentazione di riferimento dell'API AWS Organizations .

DescribeAccount

L'operazione `DescribeAccount` API può essere utilizzata solo nel contesto di un'organizzazione gestita dal AWS Organizations servizio. L'operazione API è definita nello spazio dei nomi di quel servizio.

Per ulteriori informazioni, consulta DescribeAccount nella documentazione di riferimento dell'API AWS Organizations .

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 una delle lingue specifiche AWS SDKs, 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 d'America (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`, `CA``GB`,`DE`, `JP``IN`, 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 una delle lingue specifiche AWS SDKs, 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 una delle lingue specifiche, consulta quanto segue: AWS SDKs

- 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 una delle lingue specifiche AWS SDKs, 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 sulla versione 4 di Signature, consulta Signing AWS API requests nella IAM User Guide.

Action

azione da eseguire.

Tipo: stringa

Campo obbligatorio: sì

Version

La versione dell'API per cui è scritta la richiesta, espressa nel formato YYYY-MM-DD.

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 Creare una richiesta AWS API firmata nella Guida per l'utente 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'). Per esempio, la data e l'ora seguenti è un X-Amz-Date valore valido:`20120325T120000Z`.

Condizione: X-Amz-Date è facoltativa per tutte le richieste; può essere utilizzata per sovrascrivere la data utilizzata per firmare le richieste. Se l'intestazione Date è specificata nel formato base ISO 8601, non X-Amz-Date è obbligatoria. Quando X-Amz-Date viene utilizzata, sovrascrive sempre il valore dell'intestazione Date. Per ulteriori informazioni, consulta Elementi di una firma di richiesta AWS API nella Guida per l'utente IAM.

Tipo: stringa

Obbligatorio: condizionale

X-Amz-Security-Token

Il token di sicurezza temporaneo ottenuto tramite una chiamata a 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 credenziali di sicurezza temporanee di 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 specificazione delle intestazioni firmate, consulta Creare una richiesta AWS API firmata nella Guida per l'utente 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

Questa sezione elenca gli errori comuni alle azioni API di tutti i AWS servizi. 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 AWS standard.

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 AWS l'ID della chiave di accesso fornito non esiste nei nostri archivi.

Codice di stato HTTP: 403

NotAuthorized

Non disponi delle autorizzazioni per eseguire questa azione.

Codice di stato HTTP: 400

OptInRequired

L'ID della chiave di AWS accesso richiede un abbonamento al servizio.

Codice di stato HTTP: 403

RequestExpired

La richiesta ha raggiunto il servizio più di 15 minuti dopo la data indicata sulla richiesta o più di 15 minuti dopo la data di scadenza della richiesta (ad esempio nel caso di pre-firmata URLs), oppure la data indicata sulla richiesta è tra più di 15 minuti.

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 soddisfa 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 per la gestione degli AWS account. Per ulteriori informazioni sulle operazioni delle API e sugli errori, consulta la Documentazione di riferimento API.

> **Note**
>
> Invece di effettuare chiamate dirette all'API AWS Account Management Query, puoi utilizzare una delle AWS SDKs. AWS SDKs Sono costituiti da librerie e codice di esempio

per vari linguaggi e piattaforme di programmazione (Java, Ruby, .NET, iOS, Android e altri). SDKs Forniscono un modo conveniente per creare un accesso programmatico alla gestione degli AWS account e. AWS Ad esempio, SDKs si occupano di attività come la firma crittografica delle richieste, la gestione degli errori e il ritentativo automatico delle richieste. Per informazioni su AWS SDKs, incluso come scaricarli e installarli, consulta Tools for Amazon Web Services.

Con l'API Query per la gestione degli AWS account, puoi richiamare azioni di servizio. Le richieste Query API sono richieste HTTPS che devono contenere un `Action` parametro per indicare l'operazione da eseguire. AWS Supporti `GET` e `POST` richieste di Account Management per tutte le operazioni. Cioè, l'API non richiede l'utilizzo `GET` per alcune azioni e `POST` per altre. 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 Query API che richiedono dimensioni maggiori, è necessario utilizzare una richiesta. `POST`

La risposta è un documento XML. Per ulteriori informazioni sulla risposta, consultare le singole pagine delle operazioni nella Documentazione di riferimento API.

Argomenti

- Endpoints
- HTTPS obbligatorio
- Richieste API per la gestione AWS degli account di firma

Endpoints

AWS Account Management dispone di un unico endpoint API globale ospitato negli Stati Uniti orientali (Virginia settentrionale). Regione AWS

Per ulteriori informazioni sugli AWS endpoint e sulle regioni per tutti i servizi, consulta Regioni ed endpoint nel. 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.

Richieste API per la gestione AWS degli account di firma

Le richieste devono essere firmate usando un ID chiave di accesso e una Secret Access Key. Ti consigliamo vivamente di non utilizzare le credenziali dell'account AWS root per il lavoro quotidiano con AWS Account Management. Puoi utilizzare le credenziali di un utente AWS Identity and Access Management (IAM) o credenziali temporanee come quelle che usi con un ruolo IAM.

Per firmare le tue richieste API, devi utilizzare AWS Signature Version 4. Per informazioni sull'utilizzo della versione 4 di Signature, consulta Signing AWS API requests nella IAM User Guide.

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
- Best practice di sicurezza in IAM: offre suggerimenti per l'utilizzo del servizio IAM per proteggere le AWS risorse, comprese quelle di AWS Account Management.
- Credenziali di sicurezza temporanee in IAM: descrive come creare e usare credenziali di sicurezza temporanee.

Quote per Gestione dell'account AWS

Your Account AWS dispone di quote predefinite, precedentemente denominate limiti, per ogni servizio. AWS Salvo diversa indicazione, ogni quota è specifica. Regione AWS

Ciascuna Account AWS ha le seguenti quote relative alla gestione dell'account.

Risorsa	Quota
Numero massimo di `StartPrimaryEmailUpdate` richieste per account di destinazione	3 ogni 30 secondi
Numero di contatti alternativi in un Account AWS	3: uno ciascuno per `BILLING``SECURITY`, e `OPERATIONS`
Numero di richieste region-opt simultanee per account	6
Numero di richieste region-opt simultanee per organizzazione	50
Tasso di `AcceptPrimaryEmailUpdate` richieste per account chiamante	1 al secondo, raffica a 1 al secondo
Tasso di `DeleteAlternateContact` richieste per account	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
Frequenza di `GetAccountInformation` richieste per account chiamante	3 al secondo, raffica a 3 al secondo
Tasso di `GetAlternateContact` richieste per account	10 al secondo, raffica a 15 al secondo

Risorsa	Quota
Tasso di `GetContactInformation` richieste per account	10 al secondo, raffica a 15 al secondo
Tasso di `GetPrimaryEmail` richieste per account chiamante	3 al secondo, raffica a 3 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
Frequenza di `PutAccountName` richieste per account chiamante	1 al secondo, raffica a 1 al secondo
Tasso 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
Tasso di `StartPrimaryEmailUpdate` richieste per account chiamante	1 al secondo, raffica a 1 al secondo

Gestire gli account in India

Se ti registri a un nuovo account Account AWS e scegli l'India come indirizzo di contatto e fatturazione, il contratto utente è stipulato con Amazon Web Services India Private Limited (AWS India), un AWS venditore locale in India. AWS L'India gestisce la fatturazione e il totale della fattura è indicato in rupie indiane (INR) anziché in dollari USA (USD). Per informazioni sulla gestione di un, consulta. Account AWSConfigura il tuo Account AWS

Se il tuo account è AWS in India, segui le procedure riportate in questo argomento per gestire il tuo account. Questo argomento spiega come creare un account AWS in India, modificare le informazioni sull'account AWS in India, gestire la verifica dei clienti e aggiungere o modificare il numero di conto permanente (PAN).

Come parte della verifica della carta di credito durante l'iscrizione, AWS l'India addebita sulla carta di credito 2 INR. AWS L'India rimborserà i 2 INR dopo la verifica. La verifica potrebbe includere il reindirizzamento al sito della tua banca.

Argomenti

- Crea un uomo Account AWS con AWS l'India
- Gestisci le informazioni di verifica dei clienti

Crea un uomo Account AWS con AWS l'India

AWS L'India è un venditore locale AWS in India. Se il tuo indirizzo di contatto e di fatturazione si trova in India e desideri creare un account, utilizza la seguente procedura per registrare un account AWS in India.

Per creare un account AWS in India

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. Se l'opzione Crea un nuovo account non

è Account AWS ancora visibile, scegli Accedi a un altro account, quindi scegli Crea un nuovo Account AWS.

3. Inserisci le informazioni del tuo account, verifica il tuo indirizzo email e scegli una password sicura per il tuo account.
4. Scegli Business o Personal. Gli account personali e gli account aziendali hanno le stesse caratteristiche e funzioni.
5. Inserisci le tue informazioni di contatto aziendali o personali. Se il tuo indirizzo di contatto o di fatturazione ha sede in India, in conformità con le normative dell'Indian Computer Emergency Response Team (Cert-in), AWS è necessario raccogliere e convalidare le informazioni sulla tua identità prima di concederti l'accesso ai servizi. AWS

   Il nome che hai scelto tra le informazioni di contatto o di fatturazione deve corrispondere esattamente al nome che appare sul documento che intendi utilizzare per la verifica del cliente. Ad esempio, se intendi verificare un account aziendale utilizzando un certificato di incorporazione, devi fornire il nome dell'azienda che appare sul documento. Per un elenco dei tipi di documenti accettati, consulta the section called “Documenti indiani accettati per la verifica del cliente”.
6. Dopo aver letto il contratto con il cliente, seleziona la casella di controllo Termini e condizioni, quindi scegli Continua.
7. Nella pagina Informazioni di fatturazione, inserisci il metodo di pagamento che intendi utilizzare. È necessario fornire il CVV come parte del processo di verifica.
8. In Hai un PAN? , scegli Sì se disponi di un numero di conto permanente (PAN) che desideri venga visualizzato nelle fatture fiscali, quindi inserisci il PAN. Se non disponi di un PAN o desideri aggiungerlo dopo la registrazione, scegli No.
9. Scegli Verifica e continua. AWS L'India addebita sulla tua carta 2 INR come parte del processo di verifica. AWS L'India rimborserà i 2 INR dopo la verifica.
10. Nella pagina Conferma la tua identità, seleziona lo scopo principale della registrazione dell'account.
11. Scegli il tipo di proprietà che meglio rappresenta il proprietario dell'account. Se scegli una società, un'organizzazione o una partnership come tipo di proprietà, inserisci il nome di un dirigente chiave. La persona manageriale chiave può essere un direttore, un responsabile delle operazioni o una persona responsabile delle operazioni della vostra azienda.
12. A seconda del tipo di proprietà scelto, scegli un tipo di documento accettato in India da utilizzare per la verifica e digita le informazioni del documento.

> **Note**
>
> Se disponi di un account personale e intendi utilizzare una patente di guida non rilasciata dall'Unione dell'India, ti consigliamo di utilizzare un tipo di documento personale diverso per la verifica.

13. Scegli il nome che desideri utilizzare per la verifica del cliente.

    I nomi indicati nelle informazioni di fatturazione e di contatto verranno visualizzati per la selezione se sono associati a un indirizzo indiano. Assicurati che il nome scelto corrisponda al nome sul tipo di documento che intendi utilizzare per la verifica del cliente. Se devi apportare modifiche al nome associato al tuo indirizzo di fatturazione o di contatto, puoi farlo dopo aver completato la registrazione dell'account.
14. Fornisci il tuo consenso a inviare le informazioni per la verifica, quindi scegli Continua.

    Riceverai una notifica del risultato della verifica del cliente via e-mail dopo aver completato la registrazione dell'account. Puoi anche controllare lo stato nella pagina di verifica del cliente nelle impostazioni del tuo account o nella AWS Health Dashboard in un secondo momento. È necessario superare la verifica del cliente per accedere ai AWS servizi.
15. Scegli se verificare il tuo numero di cellulare tramite SMS o chiamata vocale.
16. Seleziona il codice del paese o dell'area geografica, quindi inserisci il numero di cellulare.
17. Completa il controllo di sicurezza.
18. Scegli Send SMS (Invia SMS) o Call Me Now (Chiamami ora). Dopo alcuni istanti, riceverai un PIN a quattro cifre in un SMS o una chiamata automatica sul tuo telefono cellulare.
19. Nella pagina Conferma la tua identità, inserisci il PIN che hai ricevuto e scegli Continua.
20. Nella pagina Seleziona un piano di supporto, seleziona il tuo piano di supporto, quindi scegli Completa l'iscrizione. Dopo la verifica del metodo di pagamento e la verifica da parte del cliente, l'account verrà attivato e riceverai un'e-mail di conferma dell'attivazione dell'account.

> **Note**
>
> Se hai completato la verifica come cliente e hai modificato il nome, l'indirizzo o il documento precedentemente utilizzato per verificare la tua identità, potrebbe essere necessario aggiornare e completare nuovamente la verifica come cliente. Per ulteriori informazioni, consulta the section called “Modifica le informazioni di verifica del cliente”.

Gestisci le informazioni di verifica dei clienti

In conformità con le normative dell'Indian Computer Emergency Response Team (Cert-in), AWS è necessario raccogliere e convalidare le informazioni sulla tua identità prima di concederti un accesso nuovo o continuo ai servizi. AWS La tua identità deve essere verificata utilizzando il nome dell'indirizzo di fatturazione o di contatto in India che hai fornito. Durante la verifica, AWS controllerà se il numero del documento è valido e se il nome fornito corrisponde al nome associato al documento utilizzato per la verifica del cliente. Il nome che scegli tra le informazioni di contatto o di fatturazione deve corrispondere esattamente al nome che appare sul documento.

Per aggiornare il nome e l'indirizzo di fatturazione, consulta la pagina delle preferenze di pagamento. Per aggiornare il nome e l'indirizzo del contatto, consulta the section called “Aggiorna il contatto principale per il tuo Account AWS”. Se modifichi le informazioni che hai utilizzato in precedenza per la verifica del cliente, ad esempio il nome o l'indirizzo con sede in India nelle informazioni di fatturazione o di contatto, potresti dover aggiornare e inviare nuovamente le informazioni di verifica del cliente.

Controlla lo stato della verifica del cliente

Puoi visualizzare lo stato della verifica del cliente in qualsiasi momento nella pagina di verifica del cliente. Se lo stato della verifica è Verifica obbligatoria o Verifica fallita, crea o aggiorna le informazioni di verifica del cliente e inviale per la verifica.

Crea le informazioni di verifica del cliente

Per completare la verifica del cliente, dovrai fornire le informazioni contenute in un documento indiano accettato. Per un elenco dei tipi di documenti accettati, consulta the section called “Documenti indiani accettati per la verifica del cliente”.

1. Accedi alla AWS Management Console.
2. Nella barra di navigazione, nell'angolo in alto a destra, scegli il nome (o alias) del tuo account, quindi scegli Account.
3. In Altre impostazioni, scegli Verifica del cliente.

   Se non hai ancora fornito le informazioni di verifica del cliente in precedenza, vedrai la pagina Crea verifica cliente.
4. Scegli il nome che corrisponde esattamente al nome sul documento che intendi utilizzare per la verifica del cliente. Ad esempio, se intendi verificare un account aziendale utilizzando un certificato di incorporazione, devi fornire il nome dell'azienda che appare sul documento.

5. Fornisci le informazioni rimanenti richieste nella pagina. A seconda del tipo di documento scelto, potrebbe essere necessario caricare una copia della parte anteriore e posteriore del documento. Se carichi un file di immagine, assicurati che tutte le informazioni nel documento siano visibili e leggibili.
6. Scegli Invia.

   Riceverai una notifica del risultato della verifica del cliente e di eventuali passaggi successivi via e-mail o sulla AWS Health Dashboard.

Modifica le informazioni di verifica del cliente

Puoi modificare le informazioni di verifica del cliente, ad esempio lo scopo principale della registrazione dell'account, il tipo di organizzazione e il nome, il tipo di documento, il caricamento del documento o le informazioni sul documento che desideri utilizzare per la verifica.

Se modifichi il nome o il tipo di documento da utilizzare per la verifica del cliente o aggiorni qualsiasi informazione del documento, il salvataggio delle modifiche richiederà una nuova verifica della tua identità.

1. Accedi alla AWS Management Console.
2. Nella barra di navigazione, nell'angolo in alto a destra, scegli il nome (o alias) del tuo account, quindi scegli Account.
3. In Altre impostazioni, scegli Verifica del cliente.
4. Scegli Modifica, quindi aggiorna le informazioni che desideri modificare.

   Mentre aggiorni le informazioni, tieni presente le seguenti indicazioni:

   - Se scegli un nome diverso, il nome deve corrispondere esattamente al nome sul documento che intendi utilizzare per la verifica da parte del cliente. Ad esempio, se intendi verificare un account aziendale utilizzando un certificato di incorporazione, devi fornire il nome dell'azienda che appare sul documento.
   - Se scegli un tipo di documento diverso, dovrai caricare una copia del fronte e del retro (se applicabile) del documento. Tutte le informazioni contenute nel documento caricato devono essere visibili e leggibili.
   - Se disponi di un account personale e intendi utilizzare una patente di guida non rilasciata dall'Unione dell'India, ti consigliamo di utilizzare un tipo di documento personale diverso per la verifica.

Per un elenco dei tipi di documenti accettati, consulta the section called “Documenti indiani accettati per la verifica del cliente”.

5. Scegli Invia.

   Se la tua identità deve essere nuovamente verificata a causa del tipo di modifiche salvate, riceverai una notifica via e-mail del risultato della verifica da parte del cliente e di eventuali passaggi successivi. Puoi anche visualizzare i risultati tornando alla pagina di verifica del cliente o nella AWS Health Dashboard.

Documenti indiani accettati per la verifica del cliente

I seguenti tipi di documenti rilasciati dalla pubblica amministrazione indiana sono accettati per la verifica del cliente.

> **Note**
>
> I link condivisi di seguito sono soggetti a modifiche da parte del governo.

- Carta PAN - Disponibile sia in formato digitale che fisico, la carta Permanent Account Number (PAN) contiene un identificatore alfanumerico univoco rilasciato dal Dipartimento delle imposte sul reddito dell'India a individui, società ed entità. Un PAN è composto da dieci caratteri, tra cui lettere e numeri, nel formato **`AAAAA1111A`**. Per utilizzare questo documento per la verifica, è necessario fornire anche la data di nascita (individuale) o la data di costituzione (aziendale) che appare sul documento PAN e caricare il lato anteriore della carta. Puoi visitare il sito web ufficiale del Dipartimento delle imposte sul reddito per verificare la validità del tuo PAN.
- Carta d'identità elettore/EPIC - La carta d'identità dell'elettore, nota anche come Electors Photo Identity Card (EPIC), contiene un numero di identificazione univoco rilasciato dalla Commissione elettorale dell'India agli elettori idonei in India. Un numero ID/EPIC dell'elettore è composto da dieci caratteri, inclusi lettere e numeri. Puoi visitare il sito web ufficiale della Commissione elettorale dell'India per verificare la validità del tuo ID elettorale. Per utilizzare questo documento per la verifica, devi caricare sia il lato anteriore che quello posteriore della carta.
- Patente di guida - Se la tua patente di guida non è stata rilasciata dall'Unione dell'India, ti consigliamo di utilizzare un tipo di documento diverso per la verifica. Il numero della patente di guida è composto da 12-16 caratteri, inclusi lettere, numeri e uno spazio o un trattino. Per utilizzare questo documento per la verifica, devi fornire la tua data di nascita e caricare sia la parte anteriore

che quella posteriore della carta. Puoi visitare il sito Parivahan Sewa del Ministero dei Trasporti Stradali e delle Autostrade per verificare la validità della tua patente di guida.

- Passaporto - Il passaporto serve come prova della cittadinanza indiana e può essere utilizzato come forma di identificazione per i viaggi internazionali. Nei passaporti emessi dal Passport Seva Kendra (PSK), il numero del fascicolo del passaporto è un identificatore alfanumerico univoco associato al passaporto di una persona. Il numero del file del passaporto è composto da quindici caratteri, inclusi lettere e numeri. A differenza del numero del passaporto, il numero del file del passaporto si trova in una delle ultime pagine del passaporto indiano. Per utilizzare questo documento per la verifica, è necessario fornire la data di nascita e caricare sia la prima che l'ultima pagina (contenente il numero del file del passaporto) del passaporto. Puoi visitare il sito Passport Seva Kendra del Ministero degli Affari Esteri per verificare la validità del numero del tuo passaporto.

> **Note**
>
> Ai fini della verifica da parte del cliente, è accettato solo il numero di un passaporto indiano emesso in India. Se il tuo passaporto indiano è stato rilasciato in un altro paese, devi utilizzare un altro documento indiano per la verifica del cliente.

- Certificato di incorporazione - Un certificato di incorporazione è un documento rilasciato dal Ministero degli Affari Societari (MCA) che data la registrazione di un'azienda come entità legale. Il certificato viene utilizzato per identificare e tracciare in modo univoco le società registrate in India. Ogni certificato contiene un numero di identificazione aziendale (CIN), che è un identificatore alfanumerico unico composto da 21 caratteri, inclusi lettere e numeri. Per utilizzare questo documento per la verifica, è necessario caricare il documento del certificato di incorporazione. Puoi visitare il portale del Ministero degli Affari Societari per verificare la validità del tuo CIN.

Per gli account personali e aziendali sono accettati diversi tipi di documenti indiani:

- Per gli account personali: carta PAN, carta d'identità elettorale/EPIC, patente di guida e passaporto.
- Per account aziendali: carta PAN e certificato di incorporazione.

Gestisci il tuo account AWS in India

Ad eccezione delle seguenti attività, le procedure per la gestione dell'account sono le stesse degli account creati al di fuori dell'India. Per informazioni generali sulla gestione dell'account, consultaConfigura il tuo account.

Utilizzare il AWS Management Console per eseguire le seguenti attività:

- Aggiungere o modificare un numero di conto permanente
- Modifica di più numeri di conto permanenti
- the section called “Gestisci le informazioni di verifica dei clienti”
- Modifica più codici fiscali per beni e servizi (GSTs)
- Visualizza una fattura fiscale

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
Nuovo nome di account APIs	Support per `GetAccountInformation` la creazione e `PutAccountName` APIs la visualizzazione o modifica di un nome di account.	22 aprile 2025
Fine del supporto per la modifica delle domande relative alle sfide di sicurezza	L'argomento Modifica le domande relative alla sfida di sicurezza è stato rimosso dalla guida dopo la fine del supporto.	6 gennaio 2025
Nuova email principale APIs	Support per il nuovo `GetPrimaryEmail` e `AcceptPrimaryEmailUpdate` APIs l'aggiornamento centralizzato dell'indirizzo e-mail dell'utente root (indirizzo per qualsiasi account membro in) AWS Organizations. `StartPrimaryEmailUpdate` Per ulteriori informazioni, consulta la sezione Aggiornamento dell'indirizzo e-mail dell'utente root dell'indirizzo per un account membro nella Guida	6 giugno 2024

	per l'AWS Organizations utente.	
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 alla sicurezza	È stato aggiunto un nuovo contenuto in cui si segnala che l'opzione per aggiunger e nuove domande di sfida è stata rimossa dalla pagina Account.	5 gennaio 2024
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 informazioni di contatto APIs	Support per nuovi `GetContactInformation` e `PutContactInformation` APIs.	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

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.